EN ISO 13849-1

Allen-Bradley

Guardmaster®

Indices de performance de sécurité

Transition de EN 954-1 à EN ISO 13849-1

LISTEN. THINK. SOLVE.SM

Rockwell Automation

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

INTRODUCTION

Cette publication est destinée à clarifier les récents changements ainsi que ceux à venir dans la législation et les normes relatives à la sécurité des machines. Elle concerne principalement les exigences européennes mais, en raison de la globalisation croissante des normes de sécurité des machines, une grande partie du contenu est valable sur le plan mondial.

Les machines et les traitements deviennent de plus en plus rapides, flexibles et performants. Afin de pouvoir offrir un niveau de sécurité constant pour les opérateurs et les techniciens, les mesures de protection ont à leur tour été adaptées de sorte à répondre à la complexité croissance de l'automatisation. Les systèmes de sécurité ont généralement été implémentés séparément des systèmes d'automatisation, exploités indépendamment et souvent parallèlement au système d'automatisation. En effet, le système de sécurité doit toujours être disponible. Un défaut ou une occurrence inattendue dans le fonctionnement « normal » de la machine ne doit pas entraver ou compromettre les mesures protectives de sécurité.

Il est cependant indéniable que le niveau d'intelligence du système de sécurité doit évoluer parallèlement à celui du système d'automatisation. Les conditions requises en vue d'une fonctionnalité plus sûre dépendent de plus en plus de la fonction ou du mode de la machine. Cela signifie que la « sécurité » doit, en quelque sorte, communiquer avec le système de commande « normal ». Nous devons donc reconsidérer la manière dont nous pouvons établir l'indépendance et l'intégrité du système de sécurité. Cela se manifeste principalement dans la nouvelle génération de normes généralement appelés les Normes en vigueur pour la sécurité fonctionnelle. Cette publication traite de l'une des plus significatives de ces normes : EN ISO 13849-1. Il existe parallèlement une nouvelle Directive Machines européenne qui concerne la législation relative à l'environnement industriel contemporain.

Il est important que toutes les personnes fournissant ou utilisant des machines se tiennent informées des normes en vigueur ainsi que des exigences légales. C'est l'objet de cette publication, qui traite notamment des aspects relatifs au système de commande. Elle ne remplace pas une étude exhaustive des dispositions spécifiques détaillées dans les normes et la législation. Elle a seulement pour objectif de fournir une vue d'ensemble et, nous l'espérons, de clarifier les conditions nécessaires.

Passage de EN 954-1 à EN ISO 13849-1

Il y plusieurs années, la méthode la plus utilisée pour classifier les systèmes de sécurité consistait à employer les différentes catégories de EN 954-1 [ou son équivalent ISO 13849-1:1999]. La norme EN 954-1 [son équivalent, la norme ISO 13849-1:1999, quant à elle, a déjà été supprimée] sera supprimée à la fin du mois de décembre 2012. La principale conséquence est le fait que, après cette date, cette norme ne pourra plus être utilisée pour attester de la conformité avec la Directive Machines.

Une nouvelle norme destinée à remplacer EN 954-1 à d'ores et déjà été publiée. Il s'agit de la norme EN ISO 13849-1:2008. « Sécurité des machines – Parties des systèmes de commande relatives à la sécurité ». Une norme alternative peut également être utilisée : EN/IEC 62061 « Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables ». Il est possible d'utiliser l'une ou l'autre de ces normes pour attester de la conformité avec la Directive Machines. Dans cette publication, nous présenterons la relation entre les deux normes le cas échéant. Il revient à l'utilisateur de choisir entre les deux normes, mais nous traiterons principalement de la norme EN ISO 13849-1:2008. Elle a été établie spécialement afin de permettre une transition aux concepteurs de systèmes qui utilisaient les catégories, c'est pourquoi elle est en passe de devenir la norme la plus utilisée pour les systèmes de sécurité des machines. Elle peut aussi bien être utilisée pour les systèmes complets ainsi que pour les sous-systèmes.

Différences de base entre EN 954-1 et EN ISO 13849-1

Considérons tout d'abord les différences de base entre l'ancienne norme EN 954-1 et la nouvelle norme EN ISO 13849-1. Les sorties de l'ancienne norme étaient les Catégories [B, 1, 2, 3 ou 4]. Celles de la nouvelle norme sont les Indices de performance [PL a, b, c, d ou e]. Le concept de catégorie est conservé mais il existe des exigences supplémentaires qui doivent être satisfaites avant qu'un indice de performance ne puisse être revendiqué pour un système.

Ces exigences peuvent être listées de la manière suivante :

- L'architecture du système. Désigne essentiellement les éléments utilisés comme catégories.
- Les données de fiabilité sont nécessaires pour les parties constituantes du système.
- Le taux de couverture des tests de diagnostic [DC] du système est nécessaire. Il représente la quantité effective de surveillance des défauts dans le système.
- Protection contre la défaillance de cause commune.
- Protection contre les défauts systématiques.
- Le cas échéant, exigences spécifiques pour le logiciel.

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

Nous présenterons ces différents facteurs de manière plus détaillée par la suite, mais, dans un premier temps, il est utile de considérer le principe et l'intention de base de la norme dans son ensemble. A ce niveau, il est clair que de nouvelles notions doivent être apprises, mais il sera plus facile de comprendre les détails lorsque nous en connaîtrons les objectifs et les raisons.

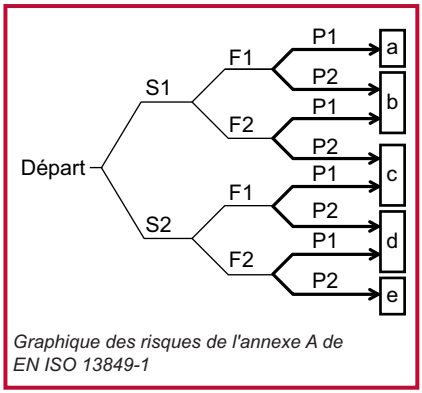
La première question à sa poser est la suivante : pourquoi avons-nous besoin d'une nouvelle norme ? Il est évident que la technologie utilisée dans les systèmes de sécurité des machines a considérablement progressé et changé au cours des dix dernières années. Jusqu'à récemment, les systèmes de sécurité dépendaient d'un équipement « simple » avec des modes de défaillance parfaitement prévisibles. Cependant, des dispositifs électroniques et programmables plus complexes sont actuellement de plus en plus utilisés dans les systèmes de sécurité. Cela a certes des avantages en termes de coûts, de flexibilité et de compatibilité, mais cela signifie également que les normes pré-existantes ne sont désormais plus appropriées. Pour savoir si un système de sécurité est suffisamment bon, nous devons disposer de plus de renseignements sur ce dernier. C'est pourquoi la nouvelle norme exige des informations plus détaillées. Les systèmes de sécurité commençant à utiliser une approche de type « boîte noire », nous pouvons de plus en plus nous fier à leur conformité avec les normes. Cependant, ces normes doivent être en mesure d'interroger correctement la technologie. Pour cela, elles doivent se baser sur les facteurs de base que sont la fiabilité, la détection des défauts, l'intégralité architecturale et systématique. Il s'agit là de l'objectif de la norme EN ISO 13849-1.

Pour établir un tracé logique dans la norme, il est important de réaliser qu'il existe deux types d'utilisateurs radicalement différents : les concepteurs des sous-systèmes relatifs à la sécurité et les concepteurs des systèmes relatifs à la sécurité. En règle générale, le concepteur de sous-systèmes [généralement un fabricant de composants de sécurité] est soumis à un niveau de complexité plus élevé. Il est alors nécessaire de fournir les données requises de sorte que le concepteur du système puisse garantir l'intégrité adéquate du système. Cela exige généralement des tests, des analyses et des calculs. Les résultats sont exprimés sous la forme des données requises par la norme.

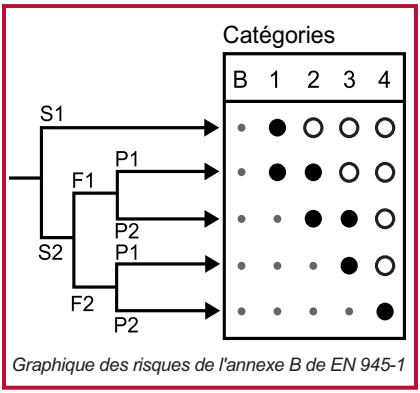
Le concepteur du système [généralement un concepteur ou intégrateur de machine] utilise ces données pour réaliser des calculs relativement simples afin de déterminer l'indice de performance global du système.

Pour déterminer l'indice de performance requis [PLr], la norme fournit un graphique des risques représentant les facteurs d'application tels que la gravité des blessures, la fréquence d'exposition et la possibilité d'évitement.

La sortie est l'indice de performance requis. Les utilisateurs de l'ancienne norme EN 954-1 utilisent couramment cette approche. Il convient cependant de noter que la ligne S1 est à présent divisée, ce qui n'était pas le cas pour l'ancien graphique des risques. Cela indique une possible reconsidération de l'intégrité des mesures de sécurité nécessaires pour des niveaux de risques plus bas.



Graphique des risques de l'annexe A de EN ISO 13849-1



Graphique des risques de l'annexe B de EN 945-1

Nous pouvons maintenant voir la relation directe entre le PLr du système [graphique des risques] et le PL obtenu par le système [calculé].

Cependant, une partie très importante doit toujours être couverte. Nous savons maintenant, grâce à la norme, quelle doit être la qualité du système et comment déterminer cette dernière, mais nous ne savons pas ce qui doit être fait. Nous devons préciser ce qu'est une fonction de sécurité. Il est clair que la fonction de sécurité doit être adaptée à l'opération concernée, mais comment peut-elle être établie ? En quoi la norme peut-elle nous aider ?

Il est important de comprendre que la fonctionnalité requise peut uniquement être déterminée en prenant en compte les caractéristiques actuelles dans l'application considérée. Il est possible pour cela de considérer la phase de conception du concept de sécurité. Cette phase ne peut pas être totalement couverte par la norme car cette dernière ne dispose pas de toutes les caractéristiques d'une application spécifique. Cela s'applique donc souvent aux constructeurs de machines qui produisent la machine mais ne connaissent pas nécessairement les conditions exactes dans lesquelles cette dernière sera utilisée.

La norme fournit une aide en listant de nombreuses fonctions de sécurité couramment utilisées et en indiquant certaines exigences généralement associées. D'autres normes telles que **EN ISO 12100 : Principes généraux de conception et EN ISO 14121 : Appréciation du risque**, sont vivement recommandées à ce niveau. Il existe donc une grande série de normes spécifiques aux machines capables de fournir des solutions pour des machines spécifiques. Elles sont appelées les normes de type C au sein des normes EN européennes ; la plupart d'entre elles ont des équivalents exacts parmi les normes ISO.

Nous pouvons donc maintenant voir que la phase de conception du concept de sécurité dépend donc du type de machine ainsi que des caractéristiques de l'application et de l'environnement dans lequel elle est utilisée. Le constructeur de machines anticipe ces facteurs pour pouvoir concevoir le concept de sécurité. Les conditions d'utilisation prévues

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

[c'est-à-dire anticipées] doivent être indiquées dans le manuel de l'utilisateur. L'utilisateur de la machine est tenu de vérifier que ces conditions correspondent bien aux conditions d'utilisation réelles.

Nous disposons maintenant d'une description de la fonctionnalité de sécurité. L'annexe A de la norme indique également l'indice de performance requis [PLr] pour les pièces de sécurité du système de commande [SRP/CS] utilisé pour implémenter cette fonctionnalité. Nous devons maintenant concevoir le système et s'assurer qu'il est bien conforme au PLr.

L'un des facteurs décisifs dans le choix de la norme à utiliser [EN ISO 13849-1 ou EN/IEC 62061] est la complexité de la fonction de sécurité. Dans la plupart des cas, pour les machines, la fonction de sécurité est relativement simple et la norme EN ISO 13849-1 est la plus appropriée. Pour évaluer le PL, elle utilise les facteurs déjà mentionnés que sont les données de fiabilité, le taux de couverture des tests de diagnostic [DC], l'architecture du système [catégorie] et les exigences concernant le logiciel le cas échéant.

Il s'agit-là d'une description simplifiée uniquement destinée à donner une vue d'ensemble. Il est important de comprendre que toutes les dispositions indiquées dans la norme doivent être appliquées. Une aide est cependant disponible. Il existe en effet un excellent logiciel capable de fournir une aide précieuse concernant tout ce qui touche au calcul. Il s'agit du logiciel SISTEMA, produit par BGIA en Allemagne. Il peut être utilisé gratuitement, vous trouverez tous les détails concernant le téléchargement sous :

www.dguv.de/bgia/en/pra/softwa/sistema

Au moment de l'impression de cette publication il est disponible en allemand et en anglais, d'autres langues étant ensuite prévues. Cet outil n'est pas commercialisé. BGIA, le concepteur du logiciel SISTEMA, est une institution de recherche et de tests reconnue, établie en Allemagne. Elle est notamment impliquée dans la résolution de problèmes scientifiques et techniques relatifs à la sécurité dans le contexte des assurances statutaires contre les accidents ainsi que dans la prévention en Allemagne. Elle travaille en étroite coopération avec des agences professionnelles de santé et de sécurité dans plus de vingt pays. Les spécialistes de BGIA, assistés de leurs collègues BG, ont contribué de manière significative à l'élaboration des normes EN ISO 13849-1 et IEC/EN 62061.

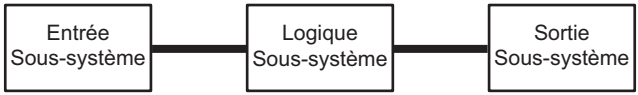
Données Rockwell Automation® pour l'utilisation avec SISTEMA

Un « catalogue » Rockwell Automation de ces dispositifs de sécurité est disponible et peut être utilisé avec l'outil de calcul de l'indice de performance SISTEMA. Pour obtenir ce catalogue, veuillez vous inscrire sous :

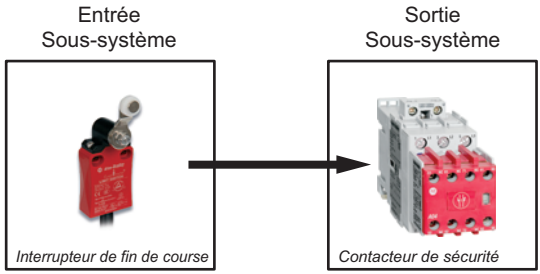
www.discoverrockwellautomation.com/safety

Quel que que soit le mode de calcul de l'indice de performance utilisé, il est important de partir des bases correctes. Nous devons visualiser notre système de la même manière que la norme, alors allons-y.

STRUCTURE DU SYSTEME

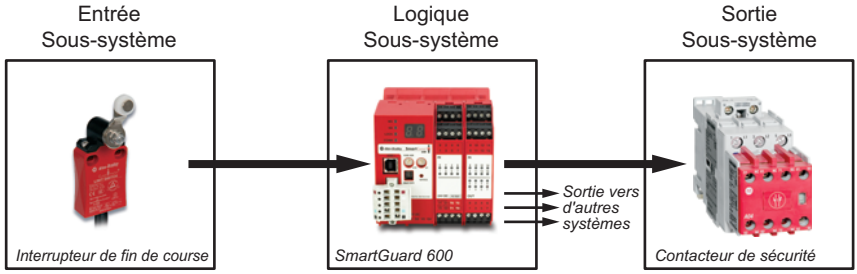


Tout système peut être divisé en composants de base du système ou « sous-systèmes ». Chaque sous-système possède sa propre fonction discrète. La plupart des systèmes peuvent être divisés en trois fonctions de base ; entrée, solution logique et actionneur [certains systèmes simples peuvent ne pas avoir de solution logique]. Les groupes de composants qui implémentent ces fonctions sont les sous-systèmes.



Interrupteur de sécurité et contacteur de sécurité

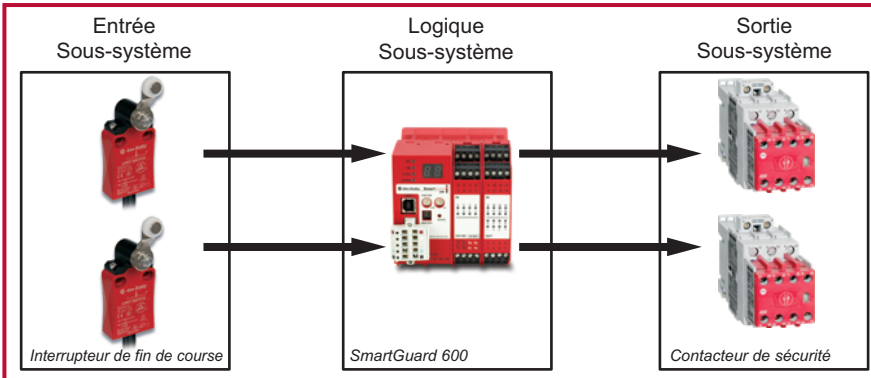
Un système électrique simple à voie unique est représenté ci-dessus à titre d'exemple. Il contient uniquement des sous-systèmes d'entrée et de sortie.



Interrupteur de sécurité, automate de sécurité et contacteur de sécurité

Le système est un peu plus complexe car une certaine logique est également nécessaire. L'automate de sécurité lui-même tolère les défauts (double voie par exemple) internes mais le système global est toujours limité au statut voie unique en raison de l'interrupteur de fin de course et du contacteur uniques.

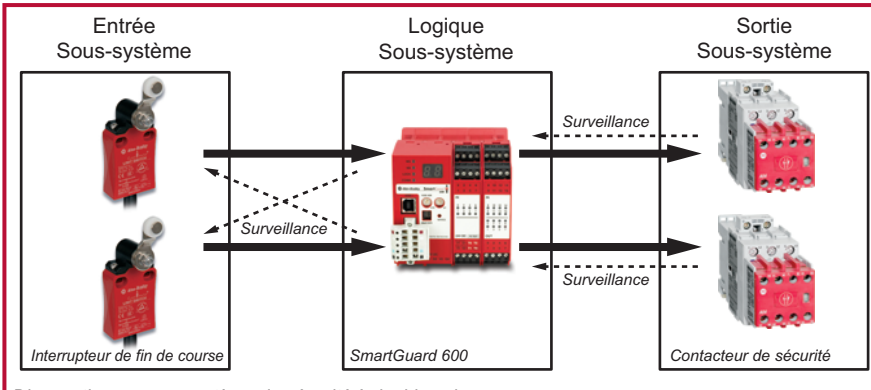
AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr



Système de sécurité à double voie

A partir de l'architecture de base du diagramme précédent, d'autres éléments doivent également être pris en compte. D'abord, combien de « voies » doit avoir le système ? Un système à voie unique tombe en panne en cas de défaut de l'un de ses sous-systèmes. Un système à voir double [également appelé système redondant] a besoin de deux défaillances, une dans chaque voie, avant de tomber en panne. Grâce aux deux voies, il peut tolérer un défaut unique tout en continuant de fonctionner. Le diagramme ci-dessus illustre un système à voie double.

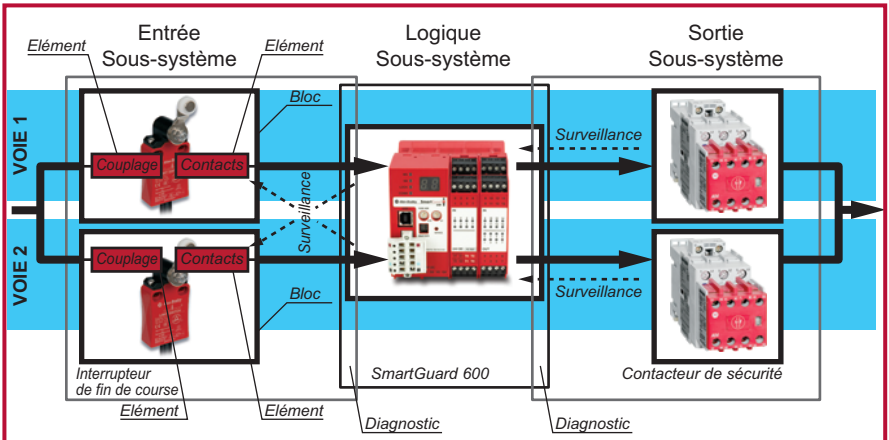
Il est clair qu'un système à double voie est moins sensible aux pannes qu'un système à voie unique. Mais nous pouvons encore augmenter sa fiabilité [en ce qui concerne sa fonction du sécurité] si nous y incluons des mesures de diagnostic pour la détection des défauts. Il va de soi que, lorsqu'un défaut a été détecté, nous devons alors y réagir et ramener le système dans un état sûr. Le diagramme suivant montre l'intégration de mesures de diagnostic grâce à des techniques de surveillance.



Diagnostics avec un système de sécurité à double voie

Il arrive fréquemment [mais ce n'est pas toujours le cas] que le système comprenne deux voies dans tous ses sous-systèmes. Par conséquent, nous pouvons voir que, dans ce cas, chaque sous-système possède deux « sous-voies ». Ces dernières sont décrites dans la norme en tant que « blocs ». Un sous-système à voie double possède au minimum deux blocs tandis qu'un sous-système à voie unique possède au minimum un bloc. Il est possible que certains systèmes comprennent une combinaison de blocs à voie unique et à double voie.

Si nous voulons étudier de manière plus détaillée le système, nous devons considérer les pièces constitutives des blocs. L'outil SISTEMA utilise le terme « éléments » pour désigner ces pièces constitutives.



Système subdivisé avec diagnostics avec un système de sécurité à double voie

Le sous-système fins de course est représenté divisé en ses éléments. Le sous-système contacteur de sortie est divisé au niveau des blocs et le sous-système logique n'est pas divisé du tout. La fonction de surveillance des fins de course et des contacteurs est réalisée au niveau de l'automate logique. Par conséquent, les cadres représentant les sous-systèmes interrupteur de fin de course et contacteur recoupent légèrement celui représentant le sous-système logique.

Ce principe de sous-division du système peut être reconnu dans la méthodologie indiquée dans EN ISO 13849-1 et dans le principe de la structure de base du système pour l'outil SISTEMA. Cependant il est important de remarquer qu'il existe quelques différences subtiles. La norme ne présente pas de méthodologie restrictive mais, pour la méthode simplifiée d'estimation de l'indice de performance, la première étape consiste généralement à diviser la structure du système en voies puis en blocs au sein de chaque voie. Avec SISTEMA, le système est généralement d'abord divisé en sous-systèmes. La norme ne

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

décrit pas explicitement un concept de sous-système mais son utilisation telle qu'elle est indiquée dans SISTEMA permet une approche plus intuitive et plus simple à comprendre. Cela n'a naturellement aucun effet sur le calcul final. SISTEMA et la norme utilisent tous deux les mêmes principes et formules. Il est intéressant de remarquer que l'approche sous-système est également utilisée dans EN/IEC 62061.

Le système qui nous a servi d'exemple est simplement l'un des cinq types de base des architectures des systèmes mentionnés dans les normes. Toutes les personnes familiarisées avec le système des catégories reconnaîtra que notre exemple est représentatif des catégories 3 ou 4.

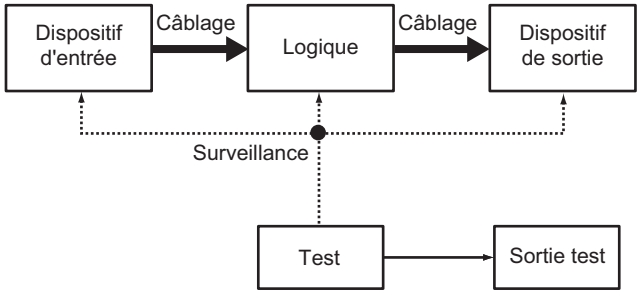
La norme utilise les catégories d'origine EN 954-1 comme ses cinq types de base pour les architectures mentionnées du système. Il s'agit des catégories d'architecture désignées. Les exigences concernant les catégories sont pratiquement [mais pas totalement] identiques à celles indiquées dans EN 954-1. Les catégories d'architecture désignées sont représentées par les figures suivantes. Il est important de remarquer qu'elles peuvent être appliquées à un système complet aussi bien qu'à un sous-système. Les diagrammes ne doivent pas être considérés comme une structure physique pure, ils sont bien plus destinés à représenter graphiquement les exigences conceptuelles.

Catégorie d'architecture désignée B

La catégorie d'architecture désignée B doit utiliser les principes de sécurité de base [voir annexe de la norme EN ISO 13849-2]. Le système ou le sous-système peut tomber en panne en cas de défaut unique. Cf. EN ISO 13849-1 pour connaître la totalité des exigences.

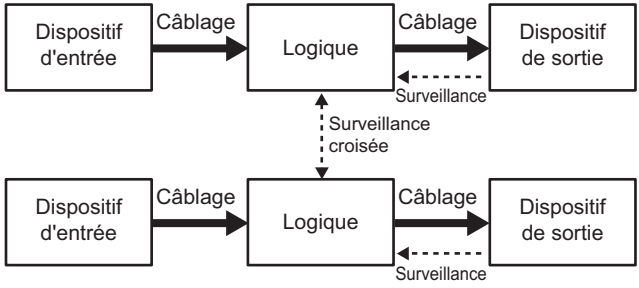
Catégorie d'architecture désignée 1

La catégorie d'architecture désignée 1 possède la même structure que la catégorie B et peut également tomber en panne en cas de défaut unique. Cela est cependant moins probable que pour la catégorie B car elle doit également utiliser des principes de sécurité largement éprouvés [cf. annexe de EN ISO 13849-2]. Cf. EN ISO 13849-1 pour connaître la totalité des exigences.



Catégorie d'architecture désignée 2

La catégorie d'architecture désignée 2 doit appliquer les principes de sécurité de base [voir annexe de la norme EN ISO 13849-2]. Une surveillance de diagnostic sous la forme d'un test fonctionnel du système ou du sous-système doit donc également exister. Cette surveillance doit intervenir lors du démarrage, puis régulièrement, avec une fréquence équivalente à au moins cent tests pour chaque demande au niveau de la fonction de sécurité. Le système ou le sous-système peut toujours tomber en panne si un défaut unique se produit entre les tests fonctionnels, mais cela est généralement moins probable que pour la catégorie 1. Cf. EN ISO 13849-1 pour connaître la totalité des exigences.

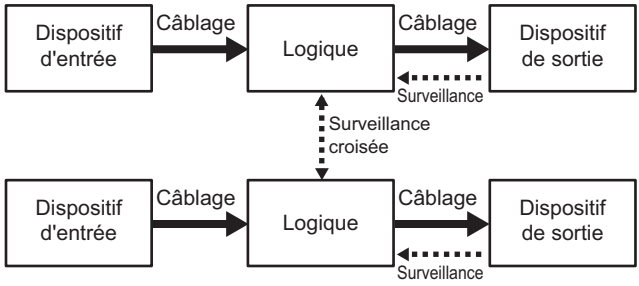


Catégorie d'architecture désignée 3

La catégorie d'architecture désignée 3 doit appliquer les principes de sécurité de base [voir annexe de la norme EN ISO 13849-2]. Il existe également une condition selon laquelle le système/sous-système ne doit pas tomber en panne en cas de défaut unique. Cela signifie que le système doit présenter une tolérance pour les défauts uniques au niveau de sa fonction de sécurité. La manière la plus simple de satisfaire à cette condition est de recourir à une architecture à double voie comme cela est représenté ci-dessus. De plus, il est également nécessaire que le défaut unique soit détecté chaque fois que cela est possible. Cette condition est la même que la condition d'origine pour la catégorie 3 de la norme EN 954-1. Dans ce contexte, la signification de la mention « chaque fois que cela est possible » s'avère quelque peu problématique. Elle indique que la catégorie 3 pourrait

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

couvrir la totalité d'une plage allant d'un système avec redondance mais sans détection des défauts [souvent désignée de manière descriptive et appropriée par le terme « redondance stupide »] à un système redondant dans lequel tous les défauts uniques sont détectés. Ce problème est traité dans la norme EN ISO 13849-1 par la condition d'estimation de la qualité du taux de couverture des tests de diagnostic. Nous pouvons voir que plus la fiabilité [MTTFd] du système est élevée, moins le taux de couverture des tests de diagnostic nécessaire est élevé. Cependant, il est également clair que le taux de couverture des tests de diagnostic doit être d'au moins 60 % pour l'architecture de la catégorie 3.



Catégorie d'architecture désignée 4

La catégorie d'architecture désignée 4 doit appliquer les principes de sécurité de base [voir annexe de la norme EN ISO 13849-2]. Le diagramme des conditions est similaire à celui de la catégorie 3 mais il demande une surveillance plus importante, c'est-à-dire un taux de couverture des tests de diagnostic plus élevé. Cela est indiqué par les lignes pointillées plus épaisses qui représentent les fonctions de surveillance. La différence essentielle entre les catégories 3 et 4 est que, pour la catégorie 3, la plupart des défauts doivent être détectés tandis que pour la catégorie 4, tous les défauts uniques doivent être détectés. Le taux de couverture des tests de diagnostic doit ainsi être d'au moins 99 %. Même les combinaisons de défauts ne doivent pas provoquer de défaillance dangereuse.

DONNEES DE FIABILITE

La norme EN ISO 13849-1 utilise des données de fiabilité quantitatives dans le calcul de l'indice de performance atteint par les pièces de sécurité d'un système de commande. Il s'agit là d'un départ significatif de EN 954-1. La première question qui vient à l'esprit est « d'où proviennent ces données ? » Il est possible d'utiliser les données des manuels de fiabilité reconnus mais la norme utilise préférentiellement le fabricant comme source de ces données. A cette fin, Rockwell Automation met à disposition les informations nécessaires sous la forme d'un catalogue de données pour SISTEMA. La société publiera également en temps voulu les données sous d'autres formes. Mais avant de poursuivre, nous devons considérer quels sont les types de données nécessaires et comprendre la manière dont elles sont produites.

Le dernier type de données nécessaires pour la détermination de l'indice de performance dans la norme [et SISTEMA] est le PFH [probabilité de défaillance dangereuse pendant une heure]. Il s'agit des mêmes données que celles représentées par l'abréviation PFHd utilisée dans IEC/EN 62061.

PL (Indice de performance)	PFH_D (Probabilité de défaillance dangereuse par heure)	SIL (Niveau d'intégrité de sécurité)
A	$\geq 10^{-5}$ à $<10^{-4}$	aucun
B	$\geq 3 \times 10^{-6}$ à $<10^{-5}$	1
C	$\geq 10^{-6}$ à $<3 \times 10^{-6}$	1
D	$\geq 10^{-7}$ à $<10^{-6}$	2
E	$\geq 10^{-8}$ à $<10^{-7}$	3

Le tableau ci-dessus montre la relation entre PFH, PL et SIL. Pour certains sous-systèmes, le PFH peut être obtenu auprès du fabricant. Cela facilite d'autant plus le calcul.
Le fabricant réalise généralement des calculs et/ou tests relativement complexes sur son sous-système afin de fournir ces données. Lorsque ces données ne sont pas disponibles, la norme EN ISO 13849-1 nous indique une approche alternative simplifiée basée sur MTTFd moyen [durée moyenne d'une défaillance dangereuse] d'une voie unique. Le PL [et donc le PFH] d'un système ou d'un sous-système peut être calculé à l'aide de la méthodologie et des formules de la norme. Il est plus facile d'utiliser SISTEMA.

MTTFd

Cette donnée représente la durée moyenne avant une défaillance pouvant conduire à une défaillance de la fonction de sécurité. Elle s'exprime en années. Il s'agit d'une valeur moyenne des MTTFd des « blocs » de chaque voie qui peut s'appliquer à un système ou à un sous-système. La norme indique la formule suivante qui est utilisée pour calculer la moyenne de tous les MTTFd de chaque élément utilisé dans une voie unique ou dans un sous-système.

A ce niveau, la valeur de SISTEMA devient évidente. Les utilisateurs gagnent du temps lorsqu'ils consultent les tableaux et calculent les formules, ces opérations étant effectuées par le logiciel. Les résultats finaux peuvent être imprimés sous la forme d'un rapport de plusieurs pages.

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}} \quad (D.1)$$

où

$MTTF_d$
correspond à la voie complète ;

$MTTF_{di}$, $MTTF_{dj}$
est le MTTFd de chaque composant contribuant à la fonction de sécurité.

La première somme concerne chaque composant séparément ; la deuxième somme est une forme équivalente, simplifiée, dans laquelle tous les composants *nj* identiques avec le même MTTFdi sont regroupés.

Dans la plupart des systèmes à double voie, les deux voies sont identiques, c'est pourquoi le résultat de la formule représente chaque voie. Si les voies du système/sous-système sont différentes, la norme fournit une formule adéquate.

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right] \quad (D.2)$$

où **$MTTF_{dc1}$** et **$MTTF_{dc2}$** sont les valeurs pour deux voies redondantes différentes.

Il s'agit, en fait, de la moyenne de deux moyennes. Pour des raisons liées à la simplification, il est également permis d'utiliser simplement la valeur de la voie correspondant au cas le moins avantageux.

La norme regroupe les MTTFd en trois plages de la façon suivante :

de 3 à < 10 ans = basse

de 10 à < 30 ans = moyenne

de 30 à 100 ans = élevée

Comme nous le verrons plus tard, la plage obtenue de MTTFd moyen est ensuite combinée à la catégorie d'architecture désignée et au taux de couverture des tests de diagnostic pour fournir un indice de performance nominal préliminaire. Le terme préliminaire est utilisé ici car d'autres conditions, notamment l'intégrité systématique et des mesures contre la défaillance de cause commune doivent toujours être remplies le cas échéant.

Méthodes de détermination des données

Nous devons maintenant aller un cran plus loin dans la manière dont un fabricant détermine les données, soit sous forme de PFHd soit de MTTFd. Il est primordial de comprendre ceci lors du traitement des données des fabricants. Les composants peuvent être regroupés en trois types de base :

- mécaniste (électro-mécanique, mécanique, pneumatique, hydraulique etc.)
- électronique (c'est-à-dire état solide)
- logiciel

Il existe une différence primordiale entre les mécanismes de défaillance commune de ces trois types de technologies. Cette dernière peut être résumée de la manière suivante, sous forme basique :

TECHNOLOGIE MECANISTE

La défaillance est proportionnelle à la fiabilité inhérente et au taux d'utilisation. Plus le taux d'utilisation est élevé, plus la probabilité que l'une des pièces constitutives soit dégradée et tombe en panne est élevée. Remarquez qu'il ne s'agit pas là de la seule cause de défaillance, mais il s'agit de la cause prédominante, sauf si nous limitons la durée/les cycles de fonctionnement. Il est bien évident qu'un contacteur ayant un cycle de commutation de 10 secondes fonctionnera de manière fiable pendant une durée plus courte qu'un contacteur identique qui fonctionne une fois par jour. Les dispositifs de la technologie mécaniste comprennent généralement des composants conçus individuellement pour leur utilisation spécifique. Les composants sont profilés, moulés, coulés, usinés etc. Ils sont combinés avec des couplages, des ressorts, des aimants, des enroulements électriques etc. pour former un mécanisme. Les pièces constitutives des composants n'ayant pas, en général, d'historique d'utilisation dans d'autres applications, il n'est pas possible de trouver de données de fiabilité pré-existantes pour ces derniers. L'estimation de PFHd ou de MTTFd pour le mécanisme est normalement basée sur les essais. Les deux normes EN/IEC 62061 et EN ISO 13849-1 préconisent toutes deux une procédure d'essai connue sous le nom de « test B10d ».

Dans le test B10d, différents échantillons de dispositifs [au moins dix généralement] sont testés dans des conditions représentatives. Le nombre moyen de cycles de fonctionnement effectués avant que 10 % des échantillons ne présentent de défaillance dangereuse correspond à ce qu'on appelle la valeur B10d. En pratique, il est fréquent que tous les échantillons présentent une défaillance dans l'état sûr mais, dans ce cas, il est établi dans la norme que la valeur B10d[dangereuse] peut être choisie comme le double de la valeur B10[sûre].

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

TECHNOLOGIE ELECTRONIQUE

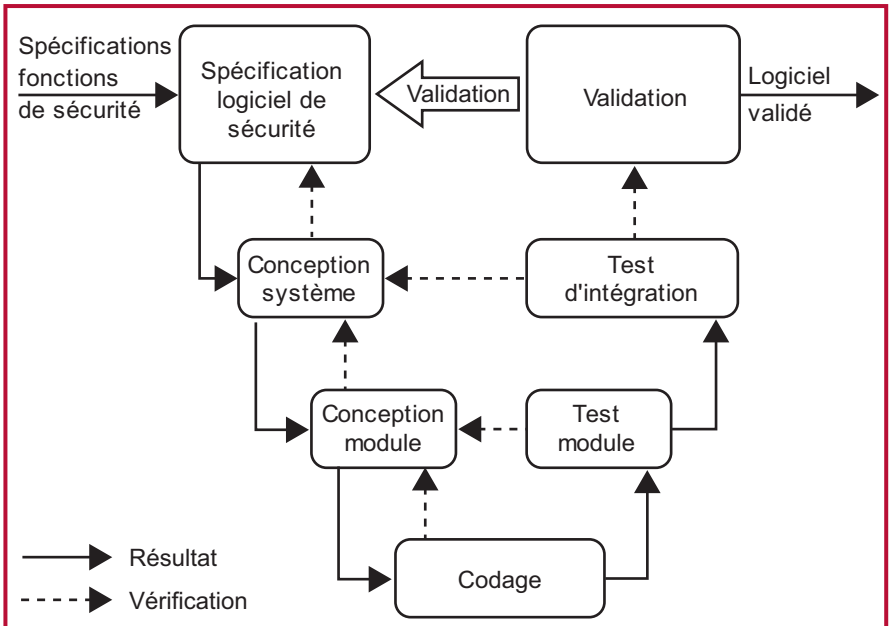
Il n'y a pas d'usure physique relative aux pièces mobiles. En admettant que l'environnement d'utilisation soit proportionnel aux caractéristiques électriques, de température [etc.] spécifiées, la défaillance prédominante d'un circuit électronique est proportionnelle à la fiabilité inhérente de ses composants constitutifs [ou à l'absence de cette dernière]. Il existe de nombreuses raisons pouvant conduire à la défaillance d'un composant individuel, notamment des imperfections liées à la fabrication, des sautes de puissance excessives, des problèmes de connexion mécanique etc.
En règle générale, les défauts des composants électroniques sont difficiles à prévoir grâce à l'analyse, ils semblent être plutôt de nature aléatoire. C'est pourquoi tester un dispositif électronique dans des conditions d'un laboratoire d'essais ne permet pas nécessairement de révéler des configurations de défaillances types à long terme.

Pout déterminer la fiabilité des dispositifs électroniques, il est d'usage d'avoir recours à l'analyse et au calcul. Nous pouvons trouver des données de bonne qualité pour les composants individuels dans les manuels de données de fiabilité. Une analyse peut permettre de déterminer les modes de défaillance dangereux pour les composants. On fait généralement la moyenne des modes de défaillance des composants comme 50 % des cas sûrs et 50 % des cas dangereux. Cela permet normalement d'obtenir des données relativement stables.

La norme IEC 61508 fournit des formules pouvant être utilisées pour calculer la probabilité globale de défaillance dangereuse [PFH ou PFD] du dispositif, c'est-à-dire du sous-système. Ces formules sont relativement complexes et prennent en compte [le cas échéant] la fiabilité du composant, le potentiel de défaillance de cause commune [facteur béta], le taux de couverture des tests de diagnostic [DC], l'intervalle entre tests fonctionnels et l'intervalle entre tests périodiques. La bonne nouvelle est que ce calcul complexe est normalement réalisé par le fabricant du dispositif. Les normes EN/IEC 62061 et EN ISO 13849-1 acceptent toutes deux un sous-système calculé de cette manière pour IEC 61508. Le PFHd obtenu peut être utilisé directement soit dans l'annexe K de EN ISO 13849-1 soit dans l'outil de calcul SISTEMA.

LOGICIEL

Les défaillances du logiciel sont toujours de nature inhérente. Toutes les défaillances sont dues à la manière dont le logiciel est conçu, écrit ou compilé. C'est pourquoi les défaillances sont toutes causées par le système sur lequel le logiciel est produit, et non celui sur lequel il est utilisé. Nous devons donc, pour contrôler les défaillances, contrôler ce système. Les deux normes IEC 61508 et EN ISO 13849-1 fournissent pour cela des conditions et des méthodologies. Il n'est pas nécessaire à ce stade de traiter ce point de manière plus détaillée, et nous nous limiterons à dire que ces conditions et méthodologies font appel au modèle V classique.



Modèle V de développement logiciel

Les logiciels intégrés sont un problème pour le concepteur du dispositif. L'approche classique consiste à développer un logiciel intégré conformément aux méthodes formelles présentées dans la norme IEC 61508 partie 3. En ce qui concerne le code d'application du logiciel servant d'interface avec l'utilisateur, la plupart des dispositifs de sécurité programmables sont livrés avec des blocs fonctionnels ou des routines « certifié(e)s ». Cela simplifie l'opération de validation pour le code d'application mais il est nécessaire de se rappeler que le programme d'application complet doit encore être validé. La manière dont les blocs sont reliés et paramétrés doit être correcte et valable pour l'opération souhaitée. Les normes EN ISO 13849-1 et IEC/EN 62061 fournissent toutes deux des directives pour ce procédé.

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

Taux de couverture des tests de diagnostic

Nous avons déjà abordé ce sujet dans le point consacré aux catégories 2, 3 et 4 de l'architecture désignée. Ces catégories nécessitent une certaine forme de test de diagnostic afin de vérifier si la fonction de sécurité est toujours active. Le terme « taux de couverture des tests de diagnostic » [généralement abrégé DC] est utilisé pour caractériser l'efficacité de ce test. Il est important de réaliser que le DC n'est pas uniquement basé sur le nombre de composants pouvant faire l'objet d'une défaillance dangereuse. Il prend également en compte le taux de défaillance dangereuse total. Le symbole λ représente le « taux de défaillance ». DC exprime la relation entre les taux d'occurrence des deux types de défaillance dangereuse suivants :

Défaillance dangereuse détectée [λdd] c'est-à-dire les défaillances qui causent ou peuvent causer une perte de la fonction de sécurité, mais qui sont détectées. Après la détection, une fonction de réaction de défaut fait passer le dispositif ou le système dans un état sûr.

Défaillance dangereuse [λd] c'est-à-dire les défaillances qui peuvent potentiellement causer ou entraîner une perte de la fonction de sécurité. Cela comprend les défaillances détectées et celles qui ne le sont pas. Il va de soi que les défaillances qui sont vraiment dangereuses sont celles qui ne sont pas détectées [indiquées par λdu]

DC est exprimé par la formule :

DC = λdd/λd sous forme de pourcentage.

Cette signification du terme DC est commune aux normes EN ISO 13849-1 et EN/IEC 62061. Cependant, sa provenance est différente. La norme EN/IEC 62061 propose d'utiliser le calcul basé sur l'analyse du mode de défaillance tandis que la norme EN ISO 13849-1 fournit une méthode simplifiée sous la forme de tables de conversion. Différentes techniques de diagnostic types sont listées avec le pourcentage DC que leur utilisation doit permettre d'obtenir. Dans certains cas, un jugement rationnel est toujours nécessaire, par exemple, dans certaines techniques, le DC obtenu est proportionnel à la fréquence de réalisation du test. D'aucuns prétendent parfois que cette approche est trop vague. Cependant, l'estimation de DC peut dépendre de plusieurs variables différentes et, quelle que soit la technique utilisée, le résultat peut généralement uniquement être décrit comme approximatif.

Il est également important de comprendre que les tables de la norme EN ISO 13849-1 sont basées sur une recherche approfondie menée par la société BGIA sur les résultats obtenus par les techniques de diagnostic connues actuellement et utilisées dans les applications réelles. A des fins de simplification, la norme divise le taux de couverture des tests de diagnostic entre quatre plages de base.

< 60 % = aucune

de 60 % à < 90 % = basse

de 90 % à < 99 % = moyenne

≥ 99 % = élevée

Cette approche consistant à traiter des plages plutôt que des valeurs de pourcentages individuelles peut également être considérée comme plus réaliste en termes de précision des résultats. L'outil SISTEMA utilise les mêmes tables de conversion que la norme.
Des systèmes électroniques complexes étant de plus en plus utilisés dans les dispositifs relatifs à la sécurité, le taux de couverture des tests de diagnostic revêt une importance croissante. Il est probable que les travaux futurs sur les normes permettront de clarifier plus précisément cette problématique. Dans l'intervalle, le recours aux connaissances de l'ingénierie et au bon sens doit être suffisant pour permettre de choisir la plage DC correcte.

Défaillance de cause commune

Dans la plupart des systèmes ou sous-systèmes à double voie [c'est-à-dire dans lesquels un défaut unique est toléré], le principe de diagnostic est basé sur une supposition selon laquelle il n'y a pas de défaillance dangereuse sur les deux voies simultanément. Le terme « simultanément » peut être exprimé de manière plus précise par « dans l'intervalle du test de diagnostic ». Si l'intervalle du test de diagnostic est raisonnablement court [par exemple moins de huit heures], on peut raisonnablement supposer qu'il est très peu probable que deux défauts séparés et indépendants l'un de l'autre se produisent pendant cette période. Cependant, la norme établit clairement que nous devons rester prudents lorsque nous décidons si les possibilités de défaut sont vraiment séparées et indépendantes l'une de l'autre ou non. Par exemple, s'il est prévisible qu'un défaut dans un composant puisse conduire à des défaillances d'autres composants, alors les défauts résultants sont considérés comme une défaillance unique.

Il est également possible qu'un événement causant la panne d'un composant puisse également provoquer la défaillance d'autres composants. Cela se traduit par la « défaillance de cause commune », généralement abrégée par CCF. Le degré de propension de CCF est normalement décrit par le facteur béta (ß). Il est très important que les concepteurs des systèmes et des sous-systèmes soient conscients des possibilités de défaillance de cause commune. Il existe de nombreux types différents de défaillances de cause commune et,

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

par conséquent, autant de manières de les éviter. La norme EN ISO 13849-1 trace un chemin rationnel entre la complication extrême et la simplification à outrance. Comme la norme EN/IEC 62061, elle adopte une approche essentiellement qualitative. Elle fournit une liste de mesures connues pour éviter avec efficacité la CCF. Ces mesures doivent être implémentées en nombre suffisant dans la conception d'un système ou d'un sous-système. Il serait possible de prétendre, avec justification, que l'utilisation de cette liste seule ne peut pas éviter de manière appropriée toutes les possibilités de CCF. Cependant, si l'intention de la liste est considérée correctement, il est clair que le rôle de ces exigences est de faire analyser au concepteur les possibilités de CCF et d'implémenter des mesures de prévention adaptées, basées sur le type de technologie et les caractéristiques de l'application prévue. L'utilisation de la liste permet d'appliquer certaines des techniques les plus efficaces et fondamentales telles que la diversité des modes de défaillance et les compétences de conception. L'outil BGIA SISTEMA implique également l'implémentation des tables de conversion CCF de la norme et garantit leur disponibilité sous une forme adaptée.

Défauts systématiques

Nous avons déjà présenté les données de fiabilité de sécurité quantifiées sous la forme de MTTFd ainsi que la probabilité de défaillances dangereuses. Mais ce n'est pas tout. Lorsque nous avons fait référence à ces termes, nous avions déjà à l'esprit les défaillances qui semblent être de nature aléatoire. En effet, la norme IEC/EN 62061 fait spécifiquement référence à l'abréviation PFHd comme étant la probabilité de défaillance matérielle aléatoire. Il existe cependant certains types de défaillances connues sous le nom de « défaillance systématique » pouvant être attribuées aux erreurs commises au cours des phases de conception ou de fabrication. L'exemple classique est une erreur dans le code logiciel. La norme indique, dans l'annexe G, des mesures permettant d'éviter ces erreurs [et donc les défaillances]. Ces mesures incluent des dispositions telles que l'utilisation de matériaux et de techniques de fabrication adaptés, de révisions, d'analyses et de simulation sur ordinateur. Il existe également des événements et caractéristiques prévisibles pouvant se produire dans l'environnement d'utilisation et susceptibles de causer des défaillances si leur effet n'est pas contrôlé. L'annexe G présente également des mesures dans ce cas. Il est par exemple facile de prévoir des pertes de puissance occasionnelles. C'est pourquoi la mise hors tension des composants doit se produire lorsque le système se trouve dans un état sûr. Ces mesures peuvent sembler relever uniquement du bon sens, et c'est en effet le cas, mais elles ne sont pas moins primordiales. Toutes les autres exigences spécifiées dans la norme n'auraient aucun sens sans la prise en compte du contrôle et de la prévention des défaillances systématiques. Cela nécessite également parfois le même type de mesures que celles utilisées pour le contrôle des défaillances matérielles aléatoires [afin de parvenir au PFHd requis] telles que le test de diagnostic automatique et le matériel redondant.

Rockwell Automation

Les sociétés sont concernées de différentes manières par la sécurité des machines. Les fabricants/fournisseurs de machines, généralement désignés par OEM (Original Equipment Manufacturers, équipementiers), doivent se conformer à la législation en vigueur relative à la sécurité des machines (en Europe, la Directive Machines par exemple), mais ils veulent également améliorer le rendement des machines tout en fournissant des produits de valeur à leurs clients. Les utilisateurs finaux de ces machines veulent améliorer le taux de rendement synthétique. La baisse du temps moyen de réparation, la réduction des déchets et la prévention des arrêts non nécessaires peuvent contribuer à remplir ces objectifs, améliorant ainsi la sécurité sur le poste de travail productif tout en garantissant le respect des réglementations de sécurité.

On sait bien que la législation a pour but de garantir un environnement de fabrication plus sûr ; travailler dans le respect des normes telles que EN ISO 13849-1 est une bonne méthode pour illustrer la conformité vis-à-vis de l'arsenal législatif. Mais cela peut impliquer de relever des défis auxquels vous n'étiez pas préparé…

- Y a-t-il des répercussions sur les performances de votre équipement ?
  Des arrêts alors qu'il devrait fonctionner ? Des déclenchements nuisibles ?
- Est-ce que cela ne vous coûte pas trop cher ?
  Avez-vous implémenté un niveau de sécurité excessif ?
  Est-ce que vous implémentez une solution de sécurité de manière inappropriée, donnant ainsi lieu à des problèmes ?
  La gestion de fournisseurs de sécurité supplémentaires est coûteuse pour votre société
- Est-ce que la sécurité limite votre capacité à :
  faire fonctionner votre machine de manière productive et efficace ?
  effectuer les opérations de maintenance rapidement et facilement ?
  livrer rapidement vos machines à votre client ?
- Des incidents se sont-ils produits plus fréquemment dans votre installation ?
  Vos mesures de sécurité sont-elles appliquées correctement ?
  Les remboursements d'invalidité et suite à des accidents du personnel sont-ils importants ?

La majorité de ces problèmes ne sont pas pris en compte lors de l'application de la sécurité des machines. Cependant, maintenant, avec les normes de sécurité fonctionnelle telles que EN ISO 13849-1 et IEC 62061, la méthodologie de l'application de sécurité est guidée vers la recherche de l'ensemble des caractéristiques de fonctionnement de votre machine dans tous ses modes de fonctionnement (production, maintenance, démarrage, déclassement etc.) et vers l'application du niveau correct d'automatisation de la sécurité afin de permettre un TRS maximal (taux de rendement synthétique).

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

Cela donne lieu à une question concernant la capacité d'un fournisseur de sécurité. Historiquement, la sécurité est appliquée pour protéger une machine en l'arrêtant, supprimant ainsi le danger. Grâce à cette méthodologie, la fabrication se fait désormais conformément à la législation. Mais qu'en est-il de la productivité et de l'efficacité ?

C'est là que l'expérience de Rockwell Automation dans l'automatisation et la sécurité fait la différence par rapport à de nombreuses sociétés qui se limitent à livrer des solutions de sécurité. En tant que fournisseur de pointe de solutions d'automatisation qui intègre la sécurité dans ses solutions d'automatisation globales, vous êtes en mesure de voir pourquoi les clients estiment un fournisseur qui leur permet d'obtenir la productivité et la flexibilité dont ils ont besoin. Chez Rockwell Automation, nous croyons fermement en la fourniture de solutions d'automatisation présentant une sécurité fonctionnelle accrue grâce à l'adoption de normes de sécurité fonctionnelle. Vous pouvez ainsi clairement voir quel est le rôle des normes de sécurité fonctionnelle telles que EN ISO 13849-1 dans la fabrication.

Rockwell Automation est une société d'automatisation qui sait de quoi il retourne en matière de sécurité. Il est possible de concevoir une solution unique pour la commande, le déplacement et le traitement de la machine et la sécurité est intégrée dans cette plateforme de commande individuelle.

Travailler avec Rockwell Automation

Un fournisseur de solutions d'automatisation maîtrisant à la fois l'automatisation et la sécurité… et pas seulement la sécurité.

- Vous aide à obtenir les **performances** souhaitées… en toute sécurité
- **Coûts** – vous aide à rentabiliser au maximum votre investissement
- Exigences légales – vous garantit la **conformité**

Toute une série de services et de solutions pour une automatisation plus sûre

- Une palette complète de produits (entrée/logique/actionnement)
- Normes et sécurité dans un réseau (CIP Safety)
- Services de sécurité (estimations, validation, formation etc.)

Intégration des fonctions de sécurité dans des solutions standard d'automatisation

- Variateurs, automates programmables, E/S, déplacement, réseaux, logiciel de programmation…
- Simplification de votre architecture
- Réduction des coûts
- Augmentation des performances

Rockwell Automation, leader global des solutions de sécurité – si vous souhaitez de plus amples informations, veuillez contacter votre bureau local.

Dispositifs d'entrée

Interrupteurs de sécurité

Ces dispositifs sont conçus pour l'interverrouillage physique des grilles de protection et de l'équipement, permettant ainsi l'accès à une zone potentiellement dangereuse uniquement lorsque le danger est neutralisé. Les dispositifs disponibles comprennent des interrupteurs de sécurité avec et sans gâche de sécurité conditionnelle, des systèmes de clés guidés et des interrupteurs de fin de course de sécurité.

Dispositifs de détection de présence

Ces dispositifs sont conçus pour détecter la présence d'une personne ou d'un objet dans ou à proximité d'une zone dangereuse. Ils n'offrent aucune barrière physique et constituent ainsi une solution idéale dans les applications nécessitant un accès fréquent dans des conditions sûres. Les dispositifs disponibles comprennent une barrière immatérielle de sécurité, des scrutateurs laser de sécurité, des matelas de protection sensibles à la pression et des bandes de chant.

Logique

Relais de sécurité

Ces dispositifs sont conçus pour surveiller l'état d'un circuit de sécurité et offrent une variété de configurations. Ils sont disponibles comme relais à fonction simple ou comme relais multifonctions matériels programmables.

Automates à sécurité programmable

Ces dispositifs sont conçus pour surveiller l'état d'un circuit de sécurité et leur logiciel peut être configuré pour des fonctionnalités spécifiques. Il s'agit d'automates de sécurité dédiés spécialement conçus pour la commande du circuit de sécurité.

Dispositifs de sortie

Contacteurs de sécurité

Les contacteurs de sécurité sont utilisés pour supprimer l'alimentation électrique de l'actionneur. Des caractéristiques spéciales sont ajoutées aux contacteurs pour obtenir les caractéristiques de sécurité.
Des contacts normalement fermés et raccordés mécaniquement sont utilisés pour renvoyer l'état des contacteurs au dispositif logique, garantissant ainsi la fonction de sécurité.

Variateurs c.a. PowerFlex® avec sécurité intégrée

Une série de variateurs c.a. PowerFlex dispose d'une fonctionnalité de sécurité intégrée en option, comprenant un arrêt de couple de sécurité, une commande de vitesse de sécurité et une commande de gâches de sécurité conditionnelle. Les PowerFlex 40P, 70, 700S et 700H proposent généralement un arrêt de couple de sécurité tandis que la nouvelle série des variateurs PowerFlex 750 propose toutes les fonctionnalités de sécurité mentionnées précédemment.

Dispositifs de déclenchement et d'arrêt d'urgence

Ces dispositifs sont conçus pour offrir une fonction d'arrêt d'urgence sur les machines et sont utilisés dans des positions permettant un accès facile pour l'opérateur. Les dispositifs comprennent des boutons d'arrêt d'urgence, des dispositifs d'arrêt d'urgence à commande par câble et des poignées de sécurité « homme mort » avec fonctionnalité arrêt d'urgence.

Interface opérateur

Ces dispositifs sont conçus pour offrir aux opérateurs une interaction sûre pour la commande de la machine et comprennent des dispositifs tels que des poignées de sécurité « homme mort » 3 positions et des dispositifs permettant la commande bimanuelle.

Automates à sécurité intégrée

Ces dispositifs sont conçus pour offrir une commande standard d'automatisation ainsi qu'une commande de sécurité sur une seule plateforme. Ils peuvent être programmés par logiciel et permettent la configuration de fonctionnalités standard et de sécurité dans le même environnement de programmation.

E/S de sécurité

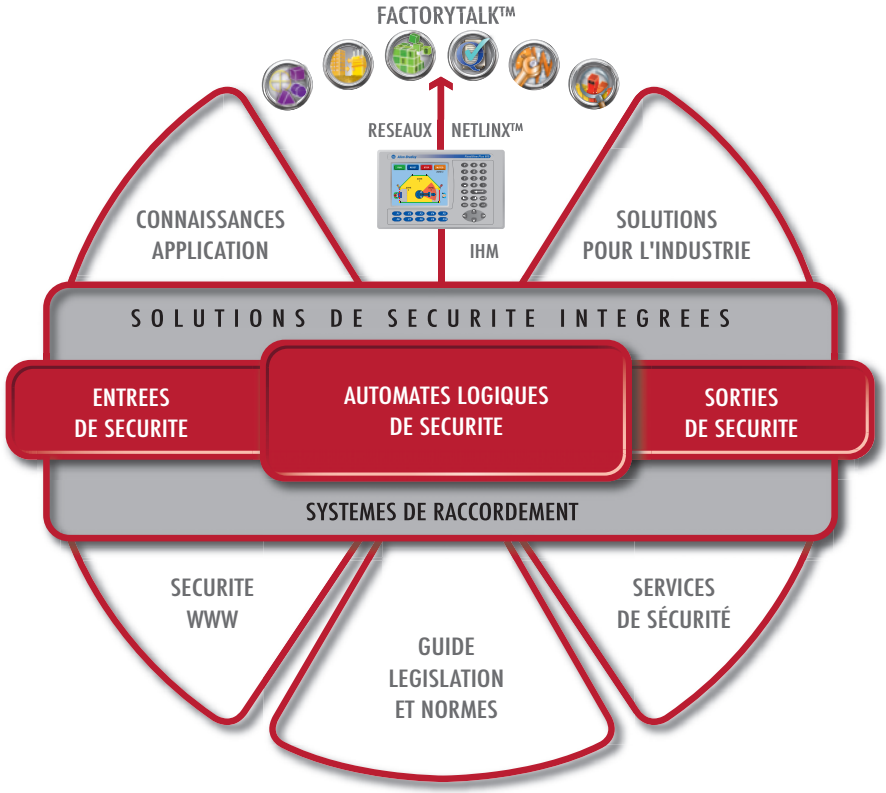
Ces dispositifs offrent des solutions E/S de sécurité pour une grande flexibilité d'application. Ils sont disponibles avec une grande série de solutions de communication de CIP Safety via DeviceNet ou EtherNet/IP. La famille comprend les produits CompactBlock Guard I/O, ArmourBlock Guard I/O et POINT Guard I/O.

Servo-variateurs Kinetix® avec sécurité intégrée

Les servo-variateurs Kinetix 6000 sont dotés de la fonctionnalité de sécurité intégrée en option avec arrêt de couple de sécurité et, dans la prochaine version, également du contrôle de la vitesse de sécurité et de la commande de gâche de sécurité conditionnelle.

Rockwell Automation

Les produits, les connaissances et l'infrastructure globale pour vous assister dans vos besoins d'automatisation et de sécurité.



www.discoverrockwellautomation.com/safety

www.rockwellautomation.com

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

www.rockwellautomation.com

Siège des activités "Power, Control and Information Solutions"

Amériques : Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 Etats-Unis, Tél. : +1 414 382 2000, Fax : +1 414 382 4444
Europe / Moyen-Orient / Afrique : Rockwell Automation, Vorstlaan/Boulevard du Souverain 36, B-1170 Bruxelles, Tél. : +32 2 663 0600, Fax : +32 2 663 0640

Belgique : Rockwell Automation, Nijverheidslaan 1, B-1853 Strombeek-Bever, Tél. : +32 2 716 84 11, Fax : +32 2 725 07 24, www.rockwellautomation.be
Canada : Rockwell Automation, 135 Dundas Street, Cambridge, Ontario, N1R 5X1, Tél. : +1 519 623 1810, Fax : +1 519 623 8930, www.rockwellautomation.ca
France : Rockwell Automation S.A.S., 2, rue René Caudron - Bât. A, F-78960 Voisins-le-Bretonneux, Tél. : +33 1 61 08 77 00, Fax : +33 1 30 44 03 09, www.rockwellautomation.fr
Suisse : Rockwell Automation, Gewerbepark, Postfach 64, CH-5506 Mägenwil, Tél. : +41 (062) 889 77 77, Fax : +41 (062) 889 77 66, www.rockwellautomation.ch

Publication : SAFETY-RM004A-FR-P — April 2009