Company - MAYKIT WRIGHT LTD
Facility - Tool room - East Factory.
Date - 8/29/95
Operator profile - Apprentice/Fully skilled.

Equipment Identity & Date	Directive Conformity	Risk Assessment Report Number	Accident History	Notes	Hazard Identity	Hazard Type	Action Required	Implemented and Inspected - Reference
Bloggs center lathe. Serial no. 8390726 Installed 1978	None claimed	RA302	None	Electrical equipment complies with BS EN 60204 E-Stops fitted (replaced 1989)	Chuck rotation with guard open	Mechanical Entanglement Cutting	Fit guard interlock switch	11/25/94 J Kershaw Report no 9567
					Cutting fluid	Toxic	Change to non toxic type	11/30/94 J Kershaw Report no 9714
					Swarf cleaning	Cutting	Supply gloves	11/30/94 J Kershaw Report no 9715
Bloggs turret head milling m/c Serial no 17304294 Manuf 1995 Installed May 95	M/c Dir. EMC Dir	RA416	None		Movement of bed (towards wall)	Crushing	Move machine to give enough clearance	4/13/95 J Kershaw Report no 10064

Figure 31

Systèmes de commande relatifs à la sécurité

Qu'entend-on exactement par système de commande relatif à la sécurité ? (ou SCRS) ?
Il s'agit de la partie d'un système de commande d'une machine ayant pour fonction de prévenir l'apparition d'une situation de danger. Il peut s'agir d'un système externe ou intégré au système normal de commande de la machine.

Sa complexité peut varier d'un système simple (par exemple une porte de protecteur avec interrupteur de sécurité et arrêts d'urgence câblés en série à la bobine de commande d'un contacteur de puissance) à un système combiné constitué à la fois de dispositifs simples et de dispositifs complexes (avec communication par logiciel ou par matériel).

Afin d'assurer la fonction de sécurité, le système doit continuer à fonctionner correctement dans toutes les conditions prévisibles.

Ainsi, comment s'y prendre pour concevoir un système capable de cela, et lorsque c'est fait, comment le démontrer ?

La norme ISO 13849-1 « Parties des systèmes de commande relatives à la sécurité » traite de tous ces aspects. Par convention, elle définit cinq catégories pour référencer et décrire le fonctionnement des SRCS (*voir Figure 32* pour le résumé de ces catégories).

Remarque 1 : la catégorie B ne prescrit aucune mesure particulière en elle-même, mais constitue la Contact des autres catégories.

Remarque 2 : une série de plusieurs pannes dues à une cause commune ou aux conséquences inévitables de la première panne, doit être considérée comme une panne unique.

Remarque 3 : la comptabilisation des pannes peut se limiter à deux défaillances combinées si cela peut être justifié, mais pour les circuits complexes (microprocesseurs par exemple), il peut être nécessaire de prendre en compte un plus grand nombre de défaillances combinées.

Comment donc définir la catégorie nécessaire ? Pour pouvoir traduire ces impératifs en un système de spécifications de conception, il faut se livrer à une interprétation des impératifs de Contact.

Une idée fausse très répandue veut que la catégorie 1 fournisse la protection minimale et la catégorie 4 la meilleure protection. *Ce n'est pourtant pas le raisonnement à adopter pour ces catégories.* Elles sont sensées être des points de référence permettant de décrire la performance fonctionnelle des différentes méthodes de commande associée à la sécurité et leurs constituants.

La catégorie 1 vise la PREVENTION des défaillances, laquelle est atteinte par l'utilisation de principes, de composants, de constituants, et de matériaux, adaptés. Les facteurs-clés de cette catégorie sont d'une part la simplicité du principe et de la conception, et d'autre part la stabilité et le choix des matériaux.

Les catégories 2, 3 et 4 ont été conçues pour détecter des pannes dans le cas ou il n'est pas possible de s'en prémunir (et de déclencher les actions appropriées). Les facteurs-clés de ces catégories sont la surveillance et le contrôle. La méthode habituelle (qui n'est pas la seule) de surveillance consiste à dupliquer les fonctions critiques de sécurité (on parle de redondance) et à en comparer les fonctionnements respectifs.

Résumé des prescriptions	Comportement du système	Principe
CATEGORIE B (voir remarque 1) - Les parties des systèmes de commande relatives à la sécurité et leur équipement de protection, ainsi que leurs composants, doivent être conçus en conformité avec les normes en vigueur afin de pouvoir résister aux influences prévues.	Toute panne risque de conduire à la perte de la fonction de sécurité.	Sélection des composants (axée sur la PREVENTION des pannes)
CATEGORIE 1 - Les prescriptions de la catégorie B s'appliquent avec utilisation de principes et de composants de sécurité dûment éprouvés.	Comme pour la catégorie B mais avec un niveau relevé de fiabilité de la fonction relative à la sécurité. (plus la fiabilité est élevée, moindre est la probabilité d'un défaut	
CATEGORIE 2 - Les prescriptions de la catégorie B et l'utilisation d'un principe de sécurité dûment éprouvé s'appliquent. - La ou les fonction(s) de sécurité sont contrôlées au démarrage de la machine et périodiquement par le système de commande. Si un défaut est détecté, la machine doit être rétablie à un état de sécurité et en cas d'impossibilité, une alarme doit être déclenchée.	La perte de la fonction de sécurité est détectée par le contrôle. Toute panne peut conduire à la perte de la fonction de sécurité entre deux contrôles périodiques.	Structure (axée sur la DETECTION des défauts)
CATEGORIE 3 (voir remarques 2 et 3) - Les prescriptions de la catégorie B et l'utilisation d'un principe de sécurité dûment éprouvé s'appliquent. - Le système doit être conçu de sorte qu'aucun défaut dans l'une des parties ne conduise à la perte des fonctions de sécurité.	Un seul défaut ne suffit pas à faire perdre la fonction de sécurité. Certains défauts, mais pas tous, sont détectés. Une accumulation de défauts non détectés peut conduire à la perte de la fonction de sécurité.	
CATEGORIE 4 (voir remarques 2 et 3) - Les prescriptions de la catégorie B et l'utilisation d'un principe de sécurité dûment éprouvé s'appliquent. - Le système doit être conçu de sorte qu'aucun défaut dans l'une des parties ne conduise à la perte des fonctions de sécurité. - La panne simple est détectée pendant ou avant la sollicitation suivante de la fonction de sécurité. Si la détection est impossible, une accumulation de défauts ne doit pas conduire à la perte de la fonction de sécurité.	La fonction de sécurité est toujours maintenue même en cas de défauts multiples. Les défauts sont détectés à temps pour prévenir la perte des fonctions de sécurité.	

Figure 32

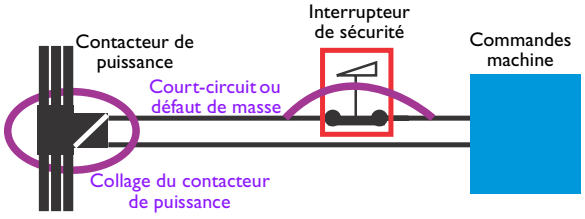

Figure 33

La *Figure 33* montre en exemple un interrupteur de sécurité d'accès à une machine, câblé en série avec la bobine de commande d'un contacteur de puissance.

En prenant pour objectif la fiabilité totale sans aucune possibilité de défaillance en cas de situation dangereuse, laquelle des différentes catégories est la plus appropriée ?

Si l'on se réfère à la *Figure 32*, quelle catégorie est-elle la plus appropriée ? La prévention des défauts ou leur détection ?

Systèmes de commande relatifs à la sécurité

La première étape consiste à décomposer le système en ses principaux constituants, puis à examiner leurs modes de défaillance potentielle.

Dans cet exemple, les constituants sont les suivants :

1. Interrupteur de sécurité.
2. Contacteur.
3. Câblage électrique.

L'interrupteur de sécurité est un dispositif mécanique.Sa tâche est simple : ouvrir les contacts lorsqu'une porte de protecteur est ouverte. Il répond aux critères de la catégorie 1 et, par l'utilisation de principes de conception conformes et de matériaux adéquats, il peut être prouvé que, utilisé dans les limites de ses paramètres de fonctionnement spécifiés, il n'aura pas de défaillances dans une situation à risque. Cela est rendu possible, car le dispositif est relativement simple et ses caractéristiques sont définies d'avance et démontrables.

Le contacteur est un dispositif légèrement plus complexe, avec des caractéristiques de pannes théoriques. Les contacteurs des fabricants réputés sont extrêmement fiables. Les statistiques montrent que les défaillances sont rares et sont généralement imputables à une mauvaise installation ou maintenance.

Les contacteurs doivent toujours avoir leurs contacts d'alimentation protégés par dispositif d'écrêtage des surintensités pour empêcher qu'ils ne se soudent (arc dû aux surintensités).

Les contacteurs doivent faire l'objet d'un programme de contrôle régulier pour détecter une usure excessive des contacts ou des connexions lâches, qui peuvent provoquer une surchauffe et des déformations.

On doit veiller à la conformité du contacteur avec les normes applicables aux caractéristiques et conditions d'utilisation requises.

En respectant ces facteurs, on réduit les possibilités de défaillance au minimum possible. Pourtant, il existe des situations où ceci est encore inacceptable et, pour améliorer le niveau de sécurité, il faut recourir à la duplication et à la surveillance.

Le câblage de raccordement des constituants doit être également pris en considération. Un court-circuit non détecté et des défauts de mise à la terre peuvent provoquer une situation dangereuse, alors que s'il est convenablement conçu et installé conformément aux normes telles que la CEI/EN 60204, les risques de défaillance sont considérablement réduits.

Ce système est en mesure de fournir un bon niveau de sécurité, suffisant dans bien des situations. On n'aura pas manqué de remarquer que le contacteur et le câblage ne laissent place qu'à des pannes théoriquement enviseageables mais très improbables. Dans certains cas, il est même possible, au prix de certaines précautions (par exemple concernant le cheminement et la protection des câbles), d'éliminer tout risque de panne. Si cela n'est pas faisable, alors les techniques se rapportant aux catégories 2, 3 et 4, telles que duplication et surveillance, sont généralement plus pratiques et économiques.

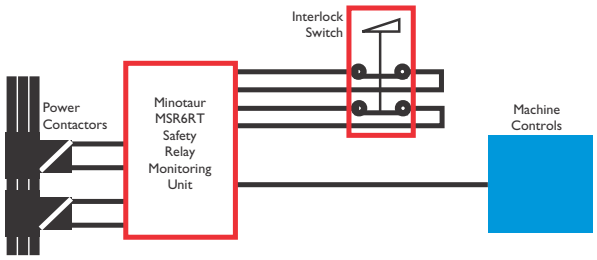

Figure 34

La Figure 34 illustre un système conforme aux prescriptions de la catégorie 3. Le MINOTAUR MSR6RT de Guardmaster est une unité de surveillance doté de deux voies d'entrée pour surveiller un circuit de commande. Avec ce système, le moindre défaut de câblage ou de contacteur est détecté par le Minotaur à la prochaine sollicitation de la fonction de sécurité. **REMARQUE :** Bien que l'interrupteur de sécurité soit ici bipolaire, il constitue toujours un **dispositif** conforme aux critères de la catégorie 1, puisqu'il fait partie d'un **système** qui répond aux critères de la catégorie 3.

La question suivante est de savoir quand, et jusqu'à quel point, nous avons besoin de prendre de telles mesures.

On peut répondre simplement que cela dépend des résultats de l'appréciation du risque. C'est la bonne approche, mais il faut comprendre qu'elle englobe tous les facteurs et non pas simplement le niveau de risque au poste dangereux. Par exemple, on pourrait penser que si l'estimation révèle un haut niveau de risque, l'interrupteur de sécurité devrait être doublé et surveillé. Or, dans bien des circonstances, ce dispositif de protection, du fait de son application, de sa conception et de sa simplicité, réagira systématiquement comme prévu et il n'y aura pas de défaillance non détectée à surveiller.

En conséquence, **le type de catégorie utilisé dépend à la fois de l'appréciation du risque et de la nature et de la complexité du dispositif ou du système**. Il apparaît également clairement que lorsqu'un système complet est conforme aux critères de la catégorie 3, par exemple, il peut incorporer des dispositifs de la catégorie 1.

S'il existe une possibilité de défaut, plus le degré du risque, calculé lors de l'appréciation, est élevé, et plus les mesures prises pour les éviter ou les détecter sont justifiées. Le type de catégorie doit être choisi pour fournir la méthode la plus adaptée et la plus efficace pour y parvenir. Il faut bien se rappeler que l'estimation du risque est un facteur, mais il faut également prendre en compte la nature du dispositif ou système de protection ainsi que les caractéristiques de fonctionnement de la machine.

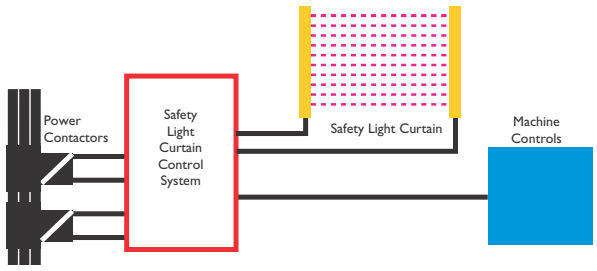

Figure 35