SAFEBOOK 3

Allen-Bradley

Guardmaster®

Systèmes de commande de sécurité pour machines

Principes, normes et intégration

LISTEN. THINK. SOLVE.℠

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

Table des matières

Directives et législation UE

La présente section a pour vocation de servir de guide général aux personnels concernés par la sécurité des machines, notamment en ce qui concerne les installations de protection et les systèmes d'interrupteur de sécurité dans l'Union Européenne. Elle s'adresse aussi bien aux concepteurs qu'aux utilisateurs d'équipements industriels.

Afin de promouvoir le concept d'un marché ouvert au sein de l'Espace Economique Européen (EEE) (qui inclut tous les états membres de l'UE et 3 autres pays), tous les états membres ont l'obligation d'édicter des lois qui définissent les exigences essentielles de sécurité pour les machines et leur utilisation.

Les machines qui ne répondent pas à ces prescriptions sont interdites dans les pays de l'EEE.

Il existe plusieurs directives européennes qui concernent la sécurité des machines et les équipements industriels, mais les deux d'entre elles les plus pertinentes sont :

1 La Directive Machines

2 Les prescriptions minimales de sécurité et de santé pour l'utilisation par les employés d'équipements de travail

Ces deux directives sont directement liées étant donné que les exigences essentielles de santé et de sécurité (EESS) de la Directive Machines peuvent servir à confirmer la sécurité des équipements dans les prescriptions minimales pour l'utilisation d'équipements de travail.

La présente section expose certains aspects des deux directives ; il est très vivement conseillé à quiconque concerné par la conception, la fourniture, l'achat ou l'utilisation d'un équipement industriel dans les pays de l'EEE et dans certains autres pays de se familiariser avec leurs critères. La plupart des fournisseurs et utilisateurs de machines ne sont tout simplement pas autorisés à fourni ou à opérer des équipements dans ces pays s'ils ne se conforment pas à ces directives.

Il existe d'autres directives européennes pertinentes pour la sécurité industrielle. Elles sont pour la plupart relativement spécialisées dans leur domaine d'application et n'entrent par conséquent pas dans le champ d'étude de la présente section ; il est toutefois important de remarquer que, le cas échéant, leurs impératifs doivent également être respectés. Par exemple, la directive basse tension, la directive ATEX.

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

La Directive Machines

Cette directive (98/37/CEI) réglemente la fourniture des machines neuves, ainsi que des autres équipements incorporant des composants de sécurité. Il est interdit de fournir des machines qui ne sont pas conformes à cette directive. Il faut donc qu'elles satisfassent à l'essentiel des normes de sécurité stipulées à l'Annexe I de la directive, qu'une évaluation correcte de la conformité soit effectuée, qu'une « Déclaration de conformité » soit émise et que le marquage CE soit apposé.

Marquage CE sur la machine

Les prescriptions essentielles de la directive sont entrées en vigueur pour les machines le 1er janvier 1995 et pour les composants de sécurité le 1er janvier 1997. Une période de transition de deux ans a été accordée. Pendant cette période de transition, il était possible d'utiliser les réglementations nationales en vigueur ou la nouvelle directive. Il est de la responsabilité du fabricant, de l'importateur ou du fournisseur final des équipements de s'assurer que les machines fournies sont conformes à la directive.

Une nouvelle version de la Directive Machines a été publiée sous la référence 2006/42/CE en 2006. Cette nouvelle directive ne remplacera pas les prescriptions de la directive en vigueur avant 2009 et dans l'intervalle, la Directive Machines existante reste en vigueur. Le texte suivant traite de la directive 98/37/CE en vigueur, mais il y aura très peu de changements en ce qui concerne les exigences essentielles pour la plupart des machines dans la nouvelle directive.

Exigences essentielles de santé et de sécurité

La machine doit être conforme aux EESS

La directive donne une liste d'exigences essentielles de santé et de sécurité (EESS) auxquelles les machines doivent se conformer. Cette liste a pour objet de faire en sorte que la machine présente toutes les garanties de sécurité et que sa conception et sa fabrication soient telles qu'elle puisse être utilisée, réglée et entretenue à toutes les phases de sa vie sans porter atteinte à la sécurité des personnes.

La directive fournit également une liste hiérarchique des mesures à prendre pour éliminer les risques :

(1) Sécurité à la conception – Chaque fois que possible, la prévention des risques est assurée par la conception elle-même de la machine.

Si cela n'est pas possible, des **(2) Equipements de protection supplémentaires**, comme des protections munies d'interrupteurs de sécurité, des barrières immatérielles comme les barrières photoélectriques, des tapis de détection, etc., doivent être utilisés.

Tout risque résiduel ne pouvant être géré par l'une des méthodes évoquées doit être limité par **(3) Equipement de protection individuelle et/ou formation**. Le fournisseur de la machine doit alors spécifier ce qui est approprié.

La fabrication et le fonctionnement doivent faire appel à des matériaux appropriés. Un éclairage confortable et une facilité de manipulation doivent être assurés. Les commandes et systèmes de commande doivent présenter toutes les garanties de sécurité et de fiabilité. Les machines ne doivent pas pouvoir démarrer intempestivement et doivent être munies d'un ou plusieurs dispositif(s) d'arrêt d'urgence. Il doit être tenu compte des installations complexes dont les procédures en amont ou en aval peuvent nuire à la sécurité d'une machine. La défaillance d'une source d'alimentation ou d'un circuit de commande ne doit pas entraîner une situation de danger. Les machines doivent être stables et capables de supporter des efforts prévisibles. Elles ne doivent pas comporter de parties saillantes ni de surfaces susceptibles de causer une blessure corporelle.

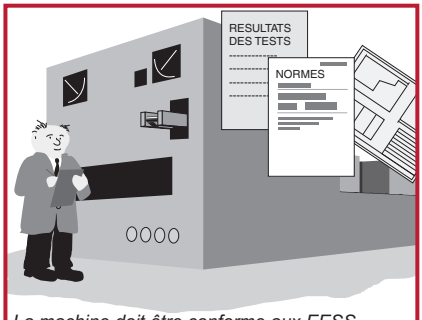
Des barrières ou des équipement de protection doivent être utilisés pour se prémunir des risques dus aux parties en mouvement. Ces dispositifs doivent être de construction robuste et difficiles à neutraliser. Les dispositifs de protection fixes doivent être montés de telle manière qu'ils ne puissent être démontés qu'avec des outils. Les dispositifs de protection amovibles doivent être munis d'interrupteurs de sécurité. Les dispositifs de protection réglables doivent pouvoir être réglés immédiatement, sans nécessiter d'outils.

Les risques liés à la source d'alimentation électrique et à d'autres sources d'énergie doivent également faire l'objet d'une prévention. Le risque de blessure corporelle dû à la température, à une explosion, au bruit, aux vibrations, aux poussières, aux gaz ou aux radiations, doit être minimal. Des dispositions adaptées doivent être prises pour la maintenance et le temps de service. Une signalisation suffisante et des systèmes d'alarme doivent être prévus. Les machines doivent être livrées avec les instructions permettant en toute sécurité l'installation, l'utilisation, le réglage, etc.

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

Evaluation de conformité

Le concepteur ou tout autre organisme responsable doit être en mesure d'apporter la preuve de la conformité aux EESS. Ce dossier doit contenir toutes les informations nécessaires : résultats d'essais, plans, caractéristiques, etc.



La machine doit être conforme aux EESS

Une norme européenne (EN) harmonisée publiée au Journal Officiel (JO) de l'Union européenne sous la rubrique de la Directive Machines et dont la date de fin de présomption de conformité n'a pas expiré, donne une présomption de conformité à certaines des EESS. (De nombreuses normes publiées au JO incluent une référence croisée qui indiquent les EESS couvertes par la norme.)

Par conséquent, lorsque l'équipement est conforme à de telles normes européennes harmonisées en vigueur, la démonstration de la conformité avec les EESS est grandement simplifiée et le fabricant bénéficie également d'une meilleure certitude quant à la conformité à la légalité. Ces normes ne sont pas légalement exigées ; toutefois, il est vivement conseillé de les utiliser, car il peut être extrêmement complexe de démontrer la conformité par d'autres moyens. Ces normes, émises par le CEN (Comité Européen de Normalisation) en collaboration avec l'ISO et le CENELEC (Comité Européen de Normalisation Electrotechnique) en collaboration avec la CEI, viennent en complément de la Directive Machines.

Une évaluation approfondie et documentée des risques doit être effectuée pour s'assurer que tous les risques potentiels liés aux machines ont été identifiés. Par ailleurs, il est de la responsabilité du fabricant des machines de s'assurer du respect de toutes les EESS, même celles qui ne sont pas couvertes par les normes EN harmonisées.

Dossier technique

La personne responsable des déclarations de conformité doit veiller à ce que la documentation suivante soit consultable sur site, en cas d'inspection.

Un dossier technique comprenant :

1 Plans d'ensemble de l'équipement, avec schémas des circuits de commande.

2 Plans de détail, méthodes de calcul, etc., nécessaires au contrôle de la conformité de la machine aux EESS.

3. Une liste comprenant :
   - EESS applicables à l'équipement.
   - Normes européennes harmonisées en vigueur.
   - Autres normes en vigueur.
   - Spécifications techniques pour la conception.

4 Un descriptif des méthodes adoptées pour éliminer les risques présentés par les machines.

5 Si nécessaire, tout rapport technique ou certificat obtenu auprès d'un organisme (centre d'essai) ou laboratoire notifié.

6 Si la conformité avec une norme européenne unifiée est déclarée, tout rapport technique indiquant les résultats des essais.

7 Un exemplaire des instructions des machines.

Pour la fabrication en série, le détail des mesures internes (des systèmes de qualité, par exemple) mises en œuvre pour s'assurer que tout équipement produit reste dans la plage de conformité :

- Le fabricant doit effectuer les recherches ou les essais nécessaires sur les composants, équipements ou sur la machine terminée pour vérifier que, de par sa conception ou construction, elle peut être installée et mise en service avec toutes les garanties de sécurité.

- Le dossier technique ne doit pas nécessairement exister en permanence d'une seule pièce, mais toutes les parties doivent être disponibles afin de pouvoir le constituer dans un délai raisonnable pour être consultable. Il doit rester consultable pendant dix ans après la fabrication du dernier exemplaire. L'incapacité à le produire suite à une demande justifiée de la part d'une autorité de contrôle peut suffire à mettre en cause la réalité de la conformité.

Le dossier technique ne doit pas nécessairement contenir des plans détaillés ou toute autre information spécifique concernant les sous-ensembles utilisés dans la fabrication de la machine, sauf s'ils sont essentiels au contrôle de la conformité avec les EESS.

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

Evaluation de conformité pour les machines listées à l'annexe IV

Evaluations de la conformité

Les équipements de certains types sont soumis à des mesures particulières. C'est le cas des équipements listés à l'Annexe IV de la directive, dont font partie les machines dangereuses telles que certaines machines à bois, presses, machines de moulage par injection, équipements souterrains, de levage de véhicules, etc.

L'annexe IV couvre également certains équipements de sécurité, comme par exemple les barrières immatérielles et les commandes bimanuelles.

Pour les machines listées en annexe IV et conformes à des normes européennes harmonisées, le choix est possible entre trois procédures distinctes :

1. Transmettre le dossier technique à un organisme notifié, qui accuse réception du dossier et le conserve. *Remarque : dans cette option, il n'y a pas d'évaluation du dossier. Il peut servir de document de référence plus tard, en cas de problème ou de réclamation pour non-conformité.*

2. Transmettre le dossier technique à un organisme notifié pour vérification de l'application correcte des normes harmonisées et obtention d'un certificat d'adéquation du dossier.

3. Faire procéder, par un organisme notifié (bureau d'essai) sur un exemplaire de la machine, à un examen CE de type. Si la machine réussit l'examen, l'organisme lui attribue un certificat d'examen CE de type.


Examens par les organismes notifiés

Pour les machines listées en annexe IV non conformes à une norme ou pour lesquelles il n'existe aucune norme européenne harmonisée, un exemplaire de la machine doit être soumis à un organisme notifié (installation d'essai) pour examen CE de type.

Organismes notifiés

Un réseau d'organismes notifiés communiquant entre eux et travaillant selon des critères communs existe dans les pays membres de l'EEE et dans certains autres pays. Les

organismes notifiés sont nommés par les gouvernements (non pas l'industrie) et des renseignements sur les organismes ayant été notifiés peuvent être obtenus à l'adresse :

http://europa.eu.int/comm/enterprise/newapproach/legislation/nb/en 98-37-ec.pdf.

Examen CE de type

Pour pouvoir procéder à un examen CE de type, l'organisme notifié a besoin du dossier technique et doit pouvoir accéder à la machine à examiner. L'examen permettra de contrôler que la machine est fabriquée conformément à son dossier technique et qu'elle répond aux EESS en vigueur. Si l'examen est concluant, l'organisme délivre une attestation d'examen CE de type. Un organisme qui refuserait de délivrer cette attestation est tenu d'en informer les autres organismes notifiés.

Procédure de déclaration de conformité CE

CE La personne en charge doit produire une déclaration de conformité CE et appliquer le marquage CE sur toutes les machines. Les machines doivent en outre être fournies accompagnées de la déclaration de conformité CE.

Remarque : Dans le cadre de la Directive Machines, les composants de sécurité doivent être accompagnés d'une déclaration de conformité CE mais pas du marquage CE (ils peuvent cependant porté le marquage CE pour indiquer leur conformité à d'autres directives, comme la directive CEM et la directive basse tension).

Le marquage CE indique que la machine est conforme aux directives européennes en vigueur et que les procédures d'évaluation de la conformité ont été réalisées. Le fait d'apposer un marquage CE sur une machine si celle-ci n'est pas conforme aux EESS pour toutes les directives en vigueur et ne présente pas, dans les faits, les garanties de sécurité est considéré comme délit. Le fait d'apposer un marquage pouvant être confondu avec le marquage CE est également considéré comme un délit.

Déclaration d'incorporation CE

Dans le cas où l'équipement est fourni pour être assemblé avec d'autres constituants pour former ultérieurement une machine complète, la personne responsable peut le faire accompagner d'une DECLARATION D'INCORPORATION (en lieu et place d'une déclaration de conformité). Le marquage CE ne doit alors PAS y être apposé. La déclaration doit spécifier que l'équipement ne doit pas être mis en service tant que la machine à laquelle il doit être incorporé n'a pas été déclarée conforme.

Cette option n'est pas possible pour les équipements pouvant fonctionner indépendamment ou pour ceux qui modifient la fonction d'une machine.

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

Maykit Wright Ltd.
Déclaration de conformité

Conformément aux directives suivantes :

Directive Machines européenne 98/37/CE. (Toute autre directive concernant les machines, comme la directive CEM, doit être incluse ici.)

Société :

Maykit Wright Ltd.
Main Street
Anytown Industrial Estate
Anytown, England AB1 2DC
Tél. : 00034 000890.
Télécopie : 00034

Machine : Machine pour conditionnement des viandes.
Type : Vacustarwrap 7D
Numéro de série : 00516

Conforme aux normes : *(Toutes les normes européennes harmonisées pertinentes utilisées et, le cas échéant, toutes normes et spécifications nationales.)*

Si la machine est couverte par l'Annexe IV, il est nécessaire à ce stade d'inclure l'un des éléments suivants :

– Le nom et l'adresse de l'Organisme notifié et le numéro du Certificat d'examen de type, ou

– Le nom et l'adresse de l'Organisme notifié qui a établi un Certificat d'adéquation pour le dossier technique, ou

– Le nom et l'adresse de l'Organisme notifié auquel le dossier technique a été transmis.

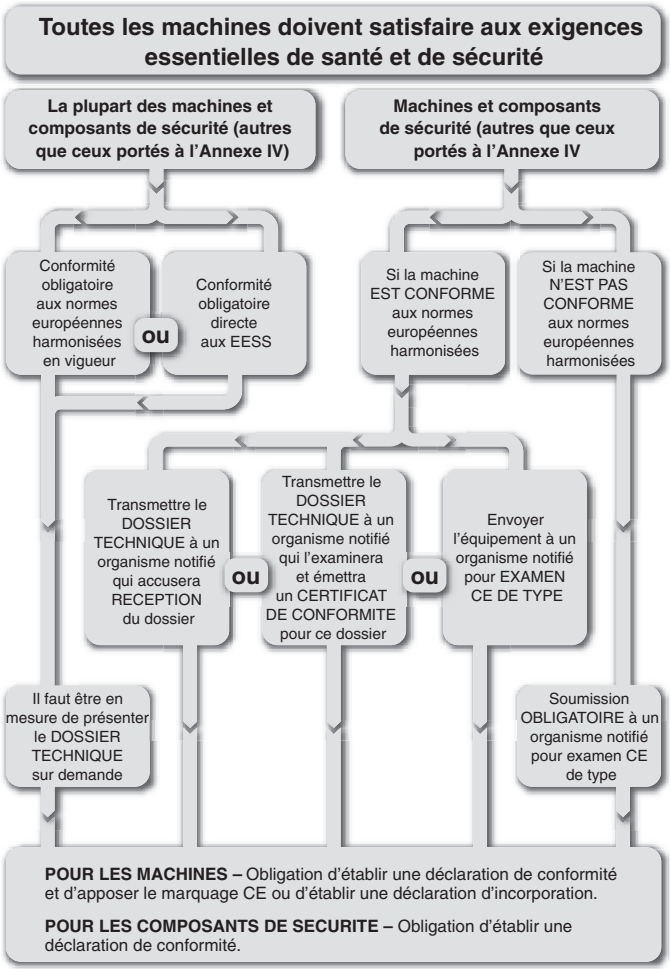
Nous déclarons par la présente que la machine ci-dessus mentionnée est conforme aux Exigences essentielles de santé et de sécurité de la directive Machine européenne 98/37/CE.

G. V. Wright

G.V. Wright, Directeur général
Publié le 17 janvier 2003

Exemple de déclaration de conformité pour machine auto-certifiée

La Directive utilisation d'équipement de travail



Vue d'ensemble de procédure relative à la Directive Machines

Alors que la Directive Machines est destinée aux fournisseurs, cette directive (89/655/CE modifiée par 95/63/CE et 2001/45/CE) est destinée aux utilisateurs des machines. Elle couvre tous les secteurs industriels et impose aux employeurs des obligations générales avec exigences minimales sur la sécurité des équipements de travail. Tous les pays de l'EEE transposent actuellement cette directive dans leur propre législation.

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

Il est plus facile de comprendre la signification des exigences de la directive utilisation d'équipement de travail en consultant un exemple de son application dans la législation nationale. Nous allons voir un exemple de sa mise en application au R.-U. sous le nom de The Provision and Use of Work Equipment Regulations (P.U.W.E.R.). Les modalités de la mise en application peuvent varier d'un pays à l'autre, mais l'effet de la directive est conservé.

Règlements 1 à 10

Ces règlements donnent des détails sur les types d'équipements et lieux de travail concernés par la directive.

Ils fixent également des devoirs d'ordre général aux employeurs, comme d'instituer des méthodes de travail sûres, et de fournir des équipements adaptés sûrs et correctement entretenus. Les opérateurs sur machines doivent recevoir la formation permettant l'utilisation de leur machine en toute sécurité.

Les machines neuves (ainsi que celles d'occasion provenant d'un pays extérieur à l'EEE) livrées après le 1er janvier 1993 doivent répondre à toutes les directives qui les concernent, comme par exemple la Directive Machines (sous réserve de dispositions transitionnelles). L'équipement d'occasion provenant d'un pays membre de l'EEE livré pour la première fois sur le lieu d'utilisation doit satisfaire en l'état aux prescriptions des règlements 11 à 24.

Remarque : Une machine en service ou d'occasion qui a fait l'objet d'une révision ou d'une modification majeure sera classifiée comme équipement neuf afin de s'assurer que les tâches effectuées par celle-ci sont conformes à la Directive Machines (et ce, même si c'est pour un usage interne à l'entreprise).

Le règlement 5 « Adaptation de l'équipement de travail » est au cœur de la directive et il souligne la responsabilité de l'employeur à procéder à une évaluation du risque adaptée.

Le Règlement 6 « Maintenance » impose que la machine fasse l'objet d'un entretien dans les règles. Cela implique en principe l'existence d'un programme d'entretien préventif systématique planifié. Il est recommandé de constituer un journal et de le tenir à jour. Ceci est particulièrement important dans les cas où l'entretien et le contrôle de l'équipement contribuent à l'efficacité permanente d'un dispositif ou système de protection.

Règlements 11 à 24

Ces règlements traitent de risques et dispositions de protection spécifiques aux machines.

Ils n'ont été totalement mis en application qu'au 1er janvier 1997 pour les machines existantes non modifiées qui étaient en service avant le 1er janvier 1993. Ils ont été appliqués immédiatement aux autres équipements. Toutefois, si l'équipement est conforme aux directives qui le concernent (la Directive Machines, par exemple), sa conformité aux prescriptions des règlements 11 à 24 est automatique, puisqu'ils sont par nature similaires aux EESS de cette directive.

Le règlement 11 est particulièrement intéressant, car il donne une hiérarchie des mesures de protection. Il s'agit de :

1. Dispositifs de protection fermés fixes.
2. Autres protections et équipements de protection.
3. Appareils de protection (gabarits, supports, tiges-poussoirs, etc.).
4. L'apport d'informations, d'instructions, d'encadrement et de formation.

Ces mesures sont à appliquer dans l'ordre prescrit dans la mesure du possible et, en général, une combinaison de deux ou trois mesures sera nécessaire.

Règlements des Etats-Unis

Cette section présente certains des règlements sur les protections de sécurité des machines industrielles en vigueur aux Etats-Unis. Ceci n'est qu'un point de départ ; les lecteurs doivent étudier davantage les exigences adaptées à leur application spécifique et prendre des mesures pour s'assurer que la conception, l'utilisation et les procédures de maintenance correspondent à leurs propres besoins, ainsi qu'aux codes et règlements nationaux et locaux.

Nombreux sont les organismes à promouvoir la sécurité industrielle aux Etats-Unis. On trouve parmi eux :

1. des entreprises qui appliquent des spécifications existantes et établissent leurs propres critères internes ;
2. l'OSHA (Occupational Safety and Health Administration) ;
3. des organismes industriels comme la National Fire Protection Association (NFPA), la Robotics Industries Association (RIA) et l'Association of Manufacturing Technology (AMT) ; ainsi que des fournisseurs de produits et solutions de sécurité comme 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

L'OSHA (Occupational Safety and Health Administration)

Aux Etats-Unis, l'OSHA compte parmi les promoteurs les plus actifs de la sécurité industrielle. Cette administration a été créée en 1970 par le vote d'une loi au Congrès, ayant pour objet de fixer un cadre réglementaire aux conditions de sécurité et de santé au travail dans l'industrie et de préserver les ressources humaines. La loi autorise le ministre du travail à édicter des normes de sécurité et de santé au travail obligatoires applicables aux entreprises liées au commerce inter-états. Cette loi s'applique au travail effectué sur le lieu de travail dans un état, dans le district de Columbia, à Puerto Rico, aux Iles Vierges, aux Samoa américaines, à Guam, dans le Trust Territory of the Pacific Islands, à l'île de Wake, sur les terres du plateau continental extérieur définies dans la loi Outer Continental Shelf Lands Act, sur l'Ile Johnston et dans la zone du canal de Panama.

L'article 5 de la loi définit les exigences minimales. Chaque employeur doit fournir à chacun de ses employés un travail et un lieu de travail exempts des dangers connus pouvant entraîner la mort ou des blessures physiques graves et doit se conformer aux normes de sécurité et de santé au travail prescrites par la loi.

Article 5 stipule également que chaque employé doit se conformer aux normes de santé et de sécurité au travail et à toutes les règles, réglementations et ordonnances promulgués en vertu de cette loi qui sont applicables à ses propres actions et à sa conduite.

La loi créant l'OSHA définit les responsabilités attachées à l'employeur et à l'employé. Ceci diffère de façon significative de la Directive Machines, qui impose aux fournisseurs de mettre sur le marché des machines exemptes de tout danger. Aux Etats-Unis, un fournisseur peut vendre une machine sans aucun équipement de protection. Il revient à l'utilisateur d'ajouter l'équipement de protection pour sécuriser la machine. Bien que cela ait été une pratique courante à l'époque où la loi a été approuvée, la tendance est plutôt à l'ajout de l'équipement de protection sur les machines par le fournisseur ; en effet l'intégration de la sécurité dans la machine à la conception est bien plus rentable que d'ajouter les systèmes de protection après la conception et la construction de la machine. Les normes actuelles incitent les fournisseurs et les clients à communiquer sur les exigences de sécurité afin que les machines soient à la fois plus sécurisées et plus productives.

Le ministre du travail a autorité pour promulguer en tant que norme de sécurité et de santé au travail toute norme de consensus national, et toute norme fédérale bien établie, sauf à ce que la promulgation de la dite norme n'entraîne pas une amélioration de la sécurité ou de la santé des employés concernés.

L'OSHA fait appliquer cette loi en publiant des règlements au Titre 29 du Code fédéral (29 CFR). Les normes applicables aux machines industrielles sont publiées par l'OSHA dans la Partie 1910 du 29 CFR. Elles sont librement accessibles sur le site de l'OSHA : www.osha.gov. Contrairement à la plupart des normes, qui ont un caractère volontaire, les normes de l'OSHA font office de lois.

Ci-dessous, certaines parties importantes qui concernent la sécurité des machines :

A - Généralités
B - Adoption et prolongement des normes fédérales établies
C - Prescriptions générales sur la sécurité et la santé
H - Matériaux dangereux
I - Equipement de protection individuelle
J - Mesures générales de protection de l'environnement – incluent condamnation/signalisation (lockout/tagout)
O - Sécurisation des mécanismes et des machines
R - Industries spécialisées
S - Electricité

Certaines normes de l'OSHA font référence à des normes volontaires. La conséquence légale d'une incorporation par référence est que le matériel est traité comme s'il était entièrement publié dans le cadre du Federal Register. Lorsqu'une norme de consensus national est incorporée par référence dans l'une des sous-parties, cette norme fait office de loi. Par exemple, NFPA 70 qui est une norme volontaire connue sous le nom de US National Electric Code, est référencée dans la sous-partie S, ce qui rend les exigences de la norme NFPA70 obligatoires.

29 CFR 1910.147, sous-partie J, couvre la régulation de toute alimentation dangereuse. Ceci est connu sous le nom de norme de condamnation/signalisation (lockout/tagout). La norme volontaire équivalente est ANSI Z244.1. Essentiellement, cette norme requiert que l'alimentation de la machine soit condamnée lorsque l'on entreprend des opérations de service ou de maintenance. L'objectif est d'empêcher toute mise sous tension ou tout démarrage imprévus de la machine qui pourrait entraîner des blessures corporelles.

Les employeurs doivent créer un programme et utiliser des procédures destinés à adjoindre des dispositifs de condamnation ou de signalisation aux appareils d'isolation de l'alimentation ; ils doivent par ailleurs désactiver les machines ou les équipements pour éviter toute mise sous tension, tout démarrage ou toute libération d'énergie stockée imprévu afin d'éviter toute blessure corporelle.

Les changements et réglages mineurs des outils, ainsi que les autres activités mineures d'entretien, qui sont faits au cours des opérations normales de production, ne sont pas couverts par cette norme s'ils sont routiniers, répétitifs et font partie intégrante de l'utilisation de l'équipement pour la production, à condition que le travail soit effectué en utilisant des mesures alternatives qui procurent une protection efficace. Ces mesures alternatives sont constituées de dispositifs de protection, comme les barrières immatérielles, les tapis de sécurité, les barrières munis d'interrupteurs de sécurité et les autres dispositifs similaires connectés à un système de sécurité. Le défi pour le concepteur et l'utilisateur de la machine est de définir ce qui est « mineur » et ce qui est « routinier, répétitif et partie intégrante ».

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

La sous-partie O couvre les machines et la protection des machines. Cette sous-partie liste les exigences générales pour toutes les machines, ainsi que les exigences pour certaines machines spécifiques. Lors de la création de l'OSHA en 1970, cet organisme a adopté de nombreuses normes ANSI existantes. Par exemple, B11.1 pour les presses électriques mécaniques a été adopté sous le numéro 1910.217.

1910.212 est la norme OSHA généraliste pour les machines. Cette norme stipule qu'une ou plusieurs méthodes de protection des machines doivent être fournies afin de protéger l'opérateur et les employés dans la zone autour de la machine des dangers comme ceux créés par le poste de l'opérateur, le pincement, les pièces tournées, la projection de copeaux et les étincelles. Des protections doivent être ajoutées à la machine lorsque c'est possible et maintenues solidement ailleurs lorsqu'il n'est pas possible de les fixer à la machine. La protection ne doit pas constituer elle-même une source de danger.

Le « poste de l'opérateur » est la partie de la machine où le travail est réalisé sur le matériau. Le poste de l'opérateur sur la machine, dont le fonctionnement expose l'employé aux risques de blessures, doit être protégé. Le dispositif de protection doit être conforme aux normes appropriées ou, en l'absence de normes spécifiques en vigueur, il doit être conçu et fabriqué de sorte à empêcher l'opérateur d'avoir une partie de son corps dans la zone à risque pendant le fonctionnement.

La sous-partie S (1910.399) définit les exigences électriques de l'OSHA. Une installation ou un équipement est acceptable pour le sous-secrétaire au travail et est approuvé aux termes de cette sous-partie S si il ou elle est approuvé, certifié, étiqueté ou plus généralement jugé comme sécurisé par un laboratoire d'essai agréé au niveau national.

Qu'est-ce que l'équipement ? Terme générique qui inclut le matériel, les accessoires, les dispositifs, les machines, les supports, les appareils, etc. utilisés dans une installation électrique ou en lien avec une telle installation.

Qu'est-ce qui est « listé » ? L'équipement est « listé » s'il appartient à un type d'équipement mentionné dans une liste qui (a) est publiée par un laboratoire agréé au niveau national et qui réalise des inspections périodiques de la production de tels équipements, et (b) déclare que ces équipements sont conformes aux normes reconnues au niveau national ou ont été testés et reconnus sécuritaires pour une utilisation spécifique.

Depuis juillet 2006, les entreprises suivantes sont des laboratoires d'essai agréés au niveau national :

- Applied Research Laboratories, Inc. (ARL)
- CSA International
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- Electrical Reliability Services, Inc. (ERS)
- Entela, Inc. (ENT)

- FM Global Technologies LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TUV America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TUV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

Certains états ont adopté leur propre organisme OSHA local. Vingt-quatre états, Puerto Rico et les îles Vierges possèdent des plans d'état approuvés par l'OSHA et ont adopté leurs propres normes et leurs propres politiques de mise en application. Pour la plupart, ces états adoptent des normes identiques à celles de l'OSHA au niveau fédéral. Cependant, certains états ont adopté des normes ou des politiques de mise en application différentes.

Les employeurs doivent signaler les incidents à l'OSHA. L'OSHA établit la fréquence des incidents et transmet ces informations aux bureaux locaux, puis les utilisent pour établir les priorités d'inspection. Les moteurs principaux d'inspection sont les suivants :

- Danger imminent
- Catastrophes et décès
- Plaintes des employés
- Industries présentant un risque élevé
- Inspections locales planifiées
- Inspections de suivi
- Programmes nationaux et locaux

Le non-respect des normes OSHA peut entraîner des amendes. Le classement des amendes pour infraction est le suivant :

- Grave : jusqu'à 7 000 $ par infraction
- Autre que grave : discrétionnaire mais pas plus de 7 000 $
- Récidive : jusqu'à 70 000 $ par infraction
- Intentionnel : jusqu'à 70 000 $ par infraction
- Infractions entraînant la mort : autres sanctions
- Refus de se conformer : 7 000 $/jour

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

Le tableau suivant montre 14 assignations faites par l'OSHA entre octobre 2004 et septembre 2005.

Norme	Description
1910.147	Régulation de l'alimentation dangereuse (condamnation/signalisation)
1910.1200	Communication dangereuse
1910.212	Prescriptions générales applicables à toutes les machines
1910.134	Protection respiratoire
1910.305	Méthodes, composants et équipement de câblage pour usage général
1910.178	Camions électriques industriels
1910.219	Transmission mécanique de puissance
1910.303	Critères généraux
1910.213	Machines pour le travail du bois
19102.215	Meules abrasives
19102.132	Critères généraux
1910.217	Presses mécaniques
1910.095	Exposition au bruit dans le travail
1910.023	Protection des ouvertures et trous dans le sol et les murs

Règlements canadiens

Au Canada, la sécurité industrielle est gérée par les provinces. Chaque province possède et applique sa propre réglementation. Par exemple, l'Ontario a créé la Loi sur la santé et la sécurité au travail, qui définit les droits et obligations de toutes les personnes sur le lieu de travail. Son objectif principal est de protéger les travailleurs contre les risques liés à la santé et à la sécurité au travail. La loi définit des procédures de gestion des risques, ainsi que les règles de mise en application de la loi lorsqu'une entreprise ne s'y conforme pas volontairement.

La loi contient le règlement 851, dont article 7 définit l'évaluation de santé et de sécurité pré-démarrage. Cette évaluation est obligatoire en Ontario pour tout équipement nouveau, reconditionné ou modifié et elle doit aboutir à un rapport fait par un ingénieur professionnel.

Normes

Cette section contient une liste de normes internationales et nationales typiques concernant la sécurité des machines. Elle n'a pas pour objectif d'être une liste exhaustive mais de donner un aperçu des problèmes de sécurité des machines qui font l'objet d'une normalisation.

Ce chapitre doit être lu conjointement avec le chapitre 1.

Les pays du monde travaillent vers une harmonisation mondiale des normes. Ceci est particulièrement évident dans le domaine de la sécurité des machines. Les normes de sécurité mondiales sont gouvernées par deux organismes : ISO et CEI. Des normes régionales et nationales sont toujours en vigueur et continuent de réglementer les exigences locales mais dans de nombreux pays la tendance est à l'application de normes internationales produites par l'ISO et la CEI.

Par exemple, les normes EN (norme européenne) sont appliquées dans tous les pays de l'EEE. Toutes les nouvelles normes EN suivent les normes ISO et CEI, et dans la plupart des cas elles comportent un texte identique.

La CEI traite des problèmes électrotechniques et l'ISO traite des autres aspects. La plupart des pays industrialisés sont membres de la CEI et de l'ISO. Les normes de sécurité sur les machines sont écrites par des groupes de travail composés d'experts provenant de nombreux pays industrialisés.

Dans la plupart des pays, l'application des normes peut être considérée comme volontaire, alors que les règlements constituent une obligation légale. Cependant, les normes sont généralement utilisées comme une interprétation pratique des règlements. Par conséquent, les domaines d'application des normes et des règlements sont étroitement liés.

Pour obtenir la liste complète des normes, veuillez consulter le catalogue des produits de sécurité disponible à cette adresse : www.ab.com/safety.

ISO (Organisation internationale de normalisation)

L'ISO est une organisation non gouvernementale composée des organismes normatifs nationaux de la plupart des pays du monde (157 pays au moment de la publication de ce document). Un secrétariat central situé à Genève, en Suisse, coordonne le système. L'ISO produit des normes destinées à rendre la conception, la fabrication et l'utilisation des machines plus efficace, plus sûre et plus écologique. Ces normes servent également à faciliter et à rendre plus équitable le commerce entre les pays.

Les normes ISO sont identifiables par les trois lettres ISO.

Les normes ISO pour les machines sont organisées de la même façon que les normes EN, en trois catégories : A, B et C (voir la section sur les normes européennes harmonisées -EN).

Pour de plus amples informations, visitez le site de l'ISO : www.iso.org.

CEI (Commission électrotechnique internationale)

La CEI prépare et publie des normes internationales dont les domaines d'application sont l'électricité, l'électronique et les technologies connexes. A travers ses membres, la CEI promeut la coopération internationale sur toutes les questions de normalisation électrotechnique et de sujets connexes, comme l'évaluation de la conformité aux normes électrotechniques.

Pour de plus amples informations, visitez le site de la CEI : www.iec/ch

Normes européennes harmonisées (EN)

Il s'agit de normes communes à tous les pays membres de l'EEE, émises par les organismes de normalisation européens que sont le CEN et le CENELEC. Si leur application procède d'une démarche volontaire, la conception et la fabrication d'un équipement conforme avec elles constitue le moyen le plus direct de démontrer la conformité avec les EESS.

Elles sont structurées en 3 catégories : A, B et C.

Catégorie A : couvre les aspects applicables à tous les types de machines.

Catégorie B : subdivisée en 2 groupes.
Groupe B1 : couvre certains aspects particuliers de la sécurité et de l'ergonomie des machines.
Groupe B2 : couvre les composants de sécurité et les dispositifs de protection.

Catégorie C : couvre des types ou groupes spécifiques de machines.

Il est important de noter que la conformité à une norme de la catégorie C implique automatiquement une présomption de conformité avec les EESS. En l'absence d'une norme adaptée à la catégorie C, on peut recourir aux normes des catégories A et B comme preuve partielle ou totale de la conformité avec les EESS, par pointage de conformité avec les sections concernées.

On peut s'appuyer sur le modèle du système solaire pour représenter la relation qui existe entre la Directive Machines et les normes européennes. Les normes sont représentées par les planètes, qui tournent autour du soleil, lequel représente la Directive Machines. Les orbites intérieures symbolisent les normes des catégories « A » et « B ». Les orbites extérieures représentent les normes de la catégorie « C ».

Des accords de collaboration ont été passés entre le CEN/CENELEC et d'autres organismes comme l'ISO et la CEI. Ceci devrait entraîner à terme une harmonisation des normes à l'échelon mondial. Dans la plupart des cas, une norme EN a son équivalent dans les normes CEI ou ISO. En général les deux textes sont identiques et toute différence régionale est indiquée dans l'avant-propos de la norme.

Le chapitre 2 liste certaines normes EN/ISO/CEI et d'autres normes nationales et régionales concernant la sécurité des machines. Lorsqu'une norme EN est indiquée entre crochets, elle est identique ou très proche de la norme ISO ou CEI. Pour consulter une liste complète des normes EN sur la sécurité des machines, visitez le site :
http://europa.eu.int/comm/enterprise/mechan_equipment/machinery/index.htm.

Règlements des Etats-Unis

Normes OSHA

Chaque fois que possible, l'OSHA promulgue des normes de consensus national ou des normes fédérales bien établies comme normes de sécurité. Les prescriptions obligatoires des normes (p. ex. le verbe devoir implique une obligation légale), incorporées par référence, possèdent la même force de loi que les normes listées en partie 1910. Par exemple, la norme de consensus national NFPA 70 est indiquée comme un document de référence dans l'annexe A de la sous-partie S-Electricité de la partie 1910 de 29 CFR. NFPA 70 est une norme volontaire développée à l'origine par la NFPA (National Fire Protection Association). Elle est également connue sous l'acronyme NEC (National Electric Code). En conséquence, toutes les dispositions obligatoires du NEC sont également rendues obligatoires par l'OSHA.

Normes ANSI (American National Standards Institute)

L'ANSI (American National Standards Institute) est l'institut américain de normalisation qui s'est fixé pour mission d'administrer et de coordonner le système de normalisation sur initiative volontaire du secteur privé aux Etats-Unis. C'est un organisme privé, à but non-lucratif, soutenu par un conglomérat de diverses entreprises des secteurs privé et public.

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

L'ANSI n'élabore pas lui-même les normes, il facilite cette élaboration en établissant un consensus entre les groupes qualifiés. Il veille en outre à ce que les groupes qualifiés respectent les principes généraux du consensus, les procédures et l'esprit d'ouverture nécessaires. La liste qui suit recense une partie des normes de sécurité industrielle qu'il est possible d'obtenir auprès de l'ANSI (textes en anglais).

Ces normes sont classées en deux catégories : les normes d'application et les normes de construction. Les normes d'application définissent la manière d'appliquer un système de protection à une machine. On en trouve des exemples dans l'ANSI B11.1, qui apporte des informations sur l'utilisation des protections sur les presses mécaniques, et dans l'ANSI/ RIA R15.06, qui décrit l'application de dispositifs de sécurité pour la protection de robots.

NFPA (National Fire Protection Association)

La National Fire Protection Association (NFPA) a été créée en 1896. Sa mission est de diminuer la pression qu'exerce les feux sur la qualité de vie en encourageant à l'élaboration de codes et des normes de consensus basés sur la science, et en facilitant la recherche et l'éducation sur le feu et sur les questions de sécurité connexes. La NFPA est le promoteur d'un grand nombre de normes visant à remplir cette mission, dont deux très importantes au plan de la sécurité industrielle : le National Electric Code (NEC) et l'Electrical Standard for Industrial Machinery (ESIM).

La National Fire Protection Association a été le promoteur du NEC depuis 1911. Le document du code original date de 1897 et il est le résultat des efforts combinés d'intérêts divers dans les domaines de l'assurance, de l'électricité, de l'architecture et apparentés. Le NEC a été actualisé en de nombreuses occasions ; il est actualisé environ tous les trois ans. L'Article 670 du NEC reprend quelques aspects concernant les machines industrielles et renvoie le lecteur à la norme NFPA 79, « Electrical Standard for Industrial Machinery ».

La norme NFPA 79 est applicable aux équipements électriques/électroniques, appareillages ou systèmes des machines industrielles fonctionnant à une tension nominale inférieure ou égale à 600 volts. Elle a pour objet de fournir des prescriptions détaillées pour l'application des équipements électriques/électroniques, appareillages ou systèmes fournis comme parties intégrantes des machines industrielles, visant à assurer la sécurité des biens et des personnes. Officiellement adoptée en 1962 par l'ANSI, elle est tout à fait comparable dans son contenu à la norme CEI 60204-1.

Les machines qui ne sont pas concernées par des normes OSHA spécifiques sont tenues d'être exemptes de phénomènes dangereux reconnus comme pouvant causer la mort ou des blessures graves. Ces machines doivent être conçues et entretenues de manière à répondre aux prescriptions des normes industrielles en vigueur, voire à les dépasser. La norme NFPA 79 s'applique normalement aux machines non spécifiquement couvertes par les normes OSHA.

Normes canadiennes

Les normes CSA reflètent un consensus national entre les producteurs et les utilisateurs – notamment les fabricants, les consommateurs, les revendeurs, les syndicats, les organisations professionnelles et les agences gouvernementales. Les normes sont largement utilisées dans l'industrie et le commerce, et sont souvent adoptées par les municipalités et les gouvernements provinciaux et fédéral dans leurs règlements, particulièrement dans les domaines de la santé, de la sécurité, de l'architecture, de la construction et de l'environnement.

Les particuliers, les entreprises et les associations, partout au Canada, montrent leur soutien à l'élaboration des normes CSA en apportant leur collaboration bénévole au Comité CSA et soutiennent les objectifs de l'association en étant membres donateurs. Les plus de 7 000 bénévoles du comité et les 2 000 membres donateurs représentent l'ensemble des membres du CSA.

Le Conseil canadien des normes est l'organisme coordonnateur du système de normalisation national, qui est une fédération d'organismes indépendants et autonomes travaillant à l'élaboration et à l'amélioration de la normalisation volontaire dans l'intérêt national.

Normes australiennes

La plupart de ces normes sont très proches des normes ISO/CEI/EN équivalentes

Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001
Téléphone : +61 2 8206 6000
Courriel : mail@standards.org.au
Site Internet : www.standards.org.au

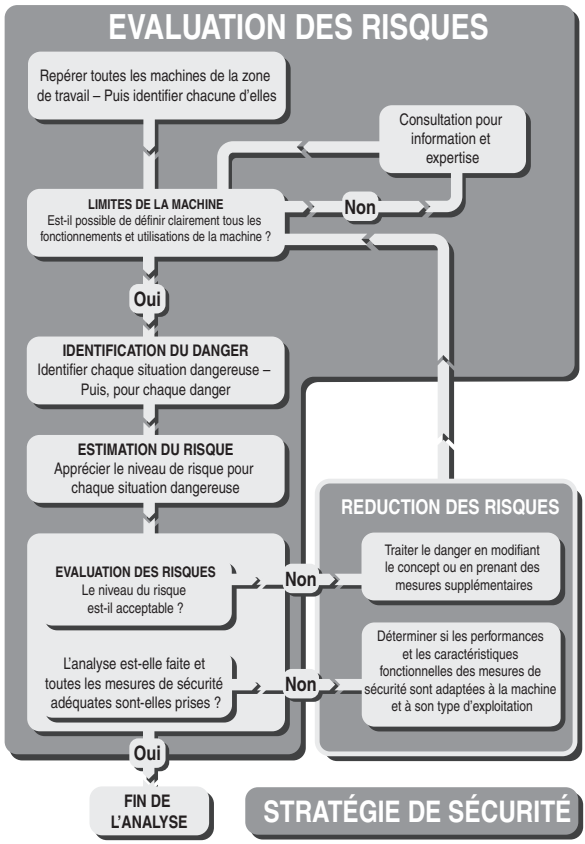
Pour acheter des exemplaires des normes :
SAI Global Limited
286 Sussex Street, Sydney, NSW 2001
Téléphone : +61 2 8206 6000
Fax : +61 2 8206 6001
Courriel : mail@sai-global.com
Site Internet : www.saiglobal.com/shop

Pour obtenir la liste complète des normes, veuillez consulter le catalogue des produits de sécurité disponible à cette adresse : www.ab.com/safety.

STRATEGIE DE SECURITE

D'un point de vue purement fonctionnel, plus une machine est performante dans le traitement des matériaux, meilleure elle est. Pourtant, pour qu'une machine soit viable, elle doit aussi présenter toutes les garanties de sécurité. En effet, la sécurité doit être considérée comme un souci primordial.

Pour concevoir une stratégie de sécurité efficace, deux étapes clés doivent être présentes et doivent fonctionner conjointement.



L'**EVALUTATION DU RISQUE** basée sur une compréhension claire des limites et des fonctions de la machine, ainsi que des interventions sur la machine pouvant s'avérer nécessaires au cours de sa vie.

LA **REDUCTION DES RISQUES** est alors réalisée si nécessaire et les mesures de sécurité sont sélectionnées à partir des informations issues de l'étape d'évaluation du risque.

La manière dont ceci est effectué constitue la base de la STRATEGIE DE SECURITE de la machine.

Une liste de contrôle est donc nécessaire pour faire un suivi et s'assurer que tous les aspects sont pris en compte et que le principe dominant n'est pas dilué dans les détails. L'ensemble du procédé doit être documenté. En plus de garantir une meilleure rigueur dans le travail accompli, cela permet aussi à d'autres parties de consulter les résultats.

Cette section concerne les fabricants et les utilisateurs des machines. Le fabricant doit s'assurer que la machine peut être utilisée en toute sécurité. L'évaluation du risque doit commencer dès la conception de la machine et doit prendre en compte toutes les interventions prévisibles qui devront être faites sur la machine. Cette approche basée sur les interventions dès le début de l'évaluation du risque est très importante. Par exemple, il peut être nécessaire d'effectuer des réglages de façon régulière sur les pièces mobiles de la machine. Au moment de la conception, il devrait être possible de prévoir des mesures qui permettront de mener ce processus à bien en toute sécurité. Si ce n'est pas fait dès le début, il peut être difficile ou même impossible de les mettre en œuvre plus tard. Cela peut avoir pour conséquence que le réglage des pièces mobiles, qui doit quand même être réalisé, doit se faire d'une façon non sécurisée ou inefficace (ou les deux). Une machine dont les interventions ont été prises en considération lors de l'évaluation du risque est une machine plus sûre et une machine plus performante.

L'utilisateur (ou l'employeur) doit s'assurer que les machines présentes dans son environnement de travail sont sécurisées. Même si le fabricant déclare qu'une machine est sûre, l'utilisateur de la machine doit tout de même évaluer les risques afin de déterminer si l'équipement est sûr dans son environnement particulier. Les machines sont souvent utilisées dans des situations non prévues par le fabricant. Par exemple, une fraiseuse utilisée dans un atelier de lycée professionnel devra faire l'objet de considérations supplémentaires par rapport à une autre utilisée dans un espace industriel.

Il ne faut pas non plus oublier que, dans le cas où une entreprise fait l'acquisition de plusieurs machines indépendantes, puis les intègre dans un seul et même procédé industriel, elle devient de fait le fabricant de la machine qui résulte de cette intégration.

Etudions à présent les étapes essentielles de la procédure conduisant à une stratégie de sécurité adéquate. Ce qui suit est applicable aussi bien à une installation industrielle existante qu'à une machine neuve seule.

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

Evaluation du risque

C'est une erreur de considérer l'évaluation du risque comme une contrainte. C'est une procédure utile, qui fournit des informations d'importance vitale, et permet à l'utilisateur ou au concepteur de prendre des décisions logiques sur les voies à suivre pour promouvoir la sécurité.

Il existe différents normes qui traitent ce sujet. Les normes ISO 14121 : « Principes d'appréciation du risque » et ISO 12100 : « Sécurité des machines – Notions fondamentales » contiennent les directives les plus largement appliquées dans le monde.

Quelle que soit la technique utilisée pour évaluer les risques, une équipe pluridisciplinaire produit généralement un résultat dont les applications sont plus étendues et qui est plus équilibré que ce que peut produire une seule personne.

L'évaluation du risque et un processus répétitif, il est reproduit à différentes étapes durant le cycle de vie de la machine. Les informations disponibles varient en fonction de l'étape dans le cycle de vie. Par exemple, le fabricant de la machine qui effectue l'évaluation du risque a accès à tous les détails concernant les mécanismes de la machine et les matériaux de fabrication, mais il ne pourra probablement émettre qu'une hypothèse sur l'environnement dans lequel elle sera utilisée. L'utilisateur qui effectue une évaluation du risque n'aura pas forcément accès aux détails techniques les plus poussés, mais il connaîtra tous les détails de l'environnement de travail des machines. Idéalement le résultat d'une évaluation sert de point de départ pour la suivante.

Détermination des limites de la machine

Ceci implique la collecte et l'analyse des informations concernant les pièces, les machines et les fonctions d'une machine. Il est également nécessaire de prendre en considération tous les types d'intervention humaine sur la machine et l'environnement dans lequel la machine fonctionnera. L'objectif est d'arriver à une compréhension claire de la machine et de son utilisation.

Lorsque des machines sont combinées, mécaniquement ou par système de commande, elles doivent être considérées comme une seule machine ; sauf si elle sont divisées en « zones » par des mesures de protection appropriées.

Il est très important de tenir compte de toutes les limites et phases de la vie de la machine (installation, mise en route, maintenance, mise hors service), de son utilisation et de son exploitation correctes, ainsi que des conséquences d'une exploitation abusive ou de dysfonctionnements normalement prévisibles.

Identification des tâches et des dangers

Tous les dangers entourant la machine doivent être identifiés et listés selon leur nature et emplacement. Les sources de danger incluent : écrasement, cisaillement, happement, projection de pièces, fumées, radiations, substances toxiques, chaleur, bruit, etc.

Les résultats de l'analyse des tâches doivent être comparés aux résultats du processus d'identification des dangers. Ceci permet de mettre en évidence les risques de convergence entre un danger et une personne, c.-à-d. une situation dangereuse. Toutes les situations dangereuses doivent être listées. Il est possible qu'un même danger puisse produire différents types de situations dangereuses selon la nature de la personne ou de la tâche. Par exemple, la présence d'un technicien de maintenance hautement qualifié peut avoir différentes implications par rapport à la présence d'un personnel de nettoyage non qualifié qui n'a aucune connaissance de la machine. Dans cette situation, si chaque cas est listé et abordé séparément, il peut être possible de justifier différentes mesures de protection pour le technicien de maintenance et le personnel de nettoyage. Si les cas ne sont pas listés et abordés séparément, alors il faut utiliser le cas le plus défavorable, et le technicien de maintenance et l'employé de nettoyage seront tous deux couverts par les mêmes mesures de protection.

Quelque fois, il est nécessaire d'effectuer une évaluation du risque pour une machine existante qui a déjà des mesures de protection (p. ex. une machine avec des pièces mobiles dangereuses protégée par une barrière munis d'interrupteurs de sécurité). Les pièces mobiles constituent un danger potentiel pouvant devenir un danger réel en cas de défaillance des interrupteurs de sécurité. Sauf si ce système munis d'interrupteurs de sécurité a déjà été validé (p. ex. par une évaluation du risque ou par une conception conforme à la norme appropriée), sa présence ne doit pas être prise en considération.

Appréciation du risque

C'est l'un des aspects les plus fondamentaux de l'évaluation du risque. Il existe de nombreuses façons d'aborder ce sujet et les pages suivantes en illustrent les principes de base.

Toute machine pouvant être impliquée dans une situation dangereuse présente un risque d'événement dangereux (c.-à-d. de blessure). Plus le risque est important, plus il est important de faire quelque chose pour y remédier. Pour un danger particulier, le risque peut être si faible qu'il est possible de le tolérer, mais pour un autre danger, le risque peut être si important qu'il faut prendre des mesures extrêmes pour s'en protéger. Par conséquent, pour décider s'il convient de prendre des mesures et lesquelles à propos du risque, il faut pouvoir le quantifier.

Le risque est souvent considéré uniquement du point de vue de la gravité des blessures qu'un accident peut occasionner. Or, il faut prendre en compte à la fois la gravité d'une blessure éventuelle ET la probabilité qu'elle survienne pour apprécier correctement le niveau de risque présent.

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

La méthode d'estimation du risque suggérée dans les pages qui suivent ne prétend en aucune manière être définitive, une approche différente pouvant être dictée par des circonstances particulières. ELLE VISE UNIQUEMENT A CONSTITUER UN GUIDE POUR ENCOURAGER UNE STRUCTURE DE TRAVAIL METHODIQUE ET DOCUMENTEE.

Le système à points utilisé n'a été étalonné pour aucun type particulier d'application, il n'est donc peut être adapté à certaines applications. Le rapport technique de l'ISO 14121-2 « Appréciation du risque – Lignes directrices pratiques et exemples de méthodes » est disponible et fournit des conseils pratiques très utiles.

Les informations suivantes ont pour objectif d'expliquer et d'illustrer la section sur l'évaluation du risque de la norme ISO 14121 « Principes d'appréciation du risque ».

Les facteurs suivants sont pris en compte :

- LA GRAVITE DE LA BLESSURE EVENTUELLE.
- LA PROBABILITE POUR QU'ELLE SURVIENNE.

Cette probabilité comprend deux facteurs distincts :

- LA FREQUENCE D'EXPOSITION.
- LA PROBABILITE DE SE BLESSER.

Nous attribuerons une certaine valeur à chaque facteur considéré individuellement.

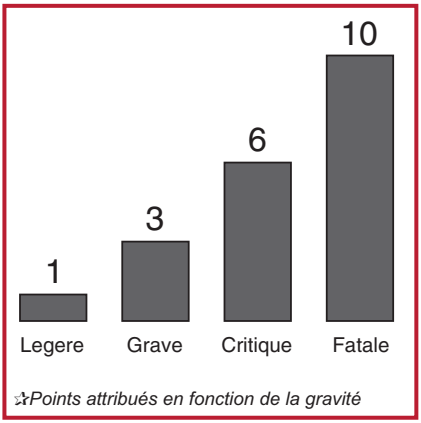
Il faut tirer profit ici de toutes les données et expériences acquises. Toutes les étapes de la vie de la machine sont pris en considération ; pour éviter trop de complexité, les décisions doivent être basées sur le cas le plus défavorable pour chaque facteur.

Il faut également avoir du bons sens. Les décisions doivent s'appuyer sur ce qui est réalisable, réaliste et plausible. C'est à ce stade qu'une approche pluridisciplinaire est utile.

N'oubliez pas que dans le cadre de cet exercice, vous ne devez généralement pas tenir compte des systèmes de protection déjà mis en place. Si l'évaluation du risque montre qu'un système de protection est nécessaire, il existe des méthodologies, décrites plus loin dans ce chapitre, qui peuvent être utilisées pour déterminer les caractéristiques requises.

1. Gravité de la blessure éventuelle

Il est pris pour hypothèse que l'accident ou l'incident s'est produit, peut-être à la suite d'un danger. Une étude attentive de la source de danger doit pouvoir révéler le type de blessure la plus grave possible. Rappel : il est ici pris pour hypothèse que la blessure corporelle est inévitable, seule sa gravité étant considérée. Il est pris pour hypothèse que l'opérateur est exposé au mouvement ou procédé dangereux. La gravité de la blessure doit être estimée entre quatre niveaux :



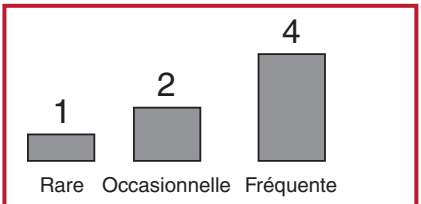
☆Points attribués en fonction de la gravité

- MORTEL : Décès
- MAJEUR : (en principe irréversible) Incapacité permanente, perte de la vue, amputation d'un membre, atteinte respiratoire, etc.
- GRAVE : (en principe réversible) Perte de conscience, brûlures, fractures, etc.
- MINEUR : Contusions, plaies, petites écorchures, etc.

Une valeur en points est attribuée à chaque description, indiqué sur l'illustration.

2. Fréquence d'exposition

La fréquence d'exposition permet de répondre à la question de la fréquence à laquelle l'opérateur ou le personnel de maintenance est exposé au danger. On peut classer la fréquence d'exposition à une source de danger selon trois niveaux :



☆Points attribués en fonction de la fréquence d'exposition

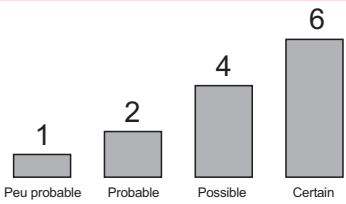
- FREQUENT : Plusieurs fois par jour.
- OCCASIONNELLE : Quotidien.
- RARE : Une fois par semaine ou moins.

Une valeur en points est attribuée à chaque description, indiqué sur l'illustration.

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

3 Probabilité d'accident

Il est pris pour hypothèse que l'opérateur est exposé au mouvement ou procédé dangereux. En considérant les interactions entre l'opérateur et la machine et divers facteurs (vitesse de mise en marche, par exemple), on peut classer la probabilité de se blesser selon quatre niveaux :



☆Points attribués en fonction de la fréquence d'exposition

- PEU PROBABLE
- PROBABLE
- POSSIBLE
- CERTAIN

Une valeur en points est attribuée à chaque description, indiqué sur l'illustration.

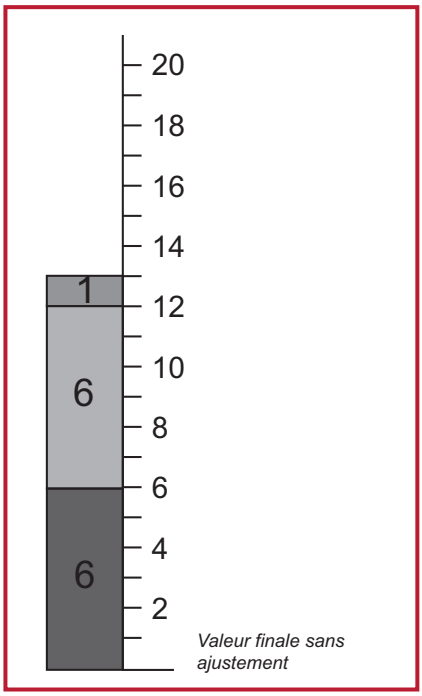
A présent qu'on a attribué une valeur à chacun des facteurs de risque, on les cumule pour obtenir une estimation initiale. La somme des trois composants donne une valeur de 13. Cependant, il est nécessaire de considérer quelques facteurs supplémentaires. (Remarque : Ceci n'est pas nécessairement basé sur les précédentes illustrations en exemple.)

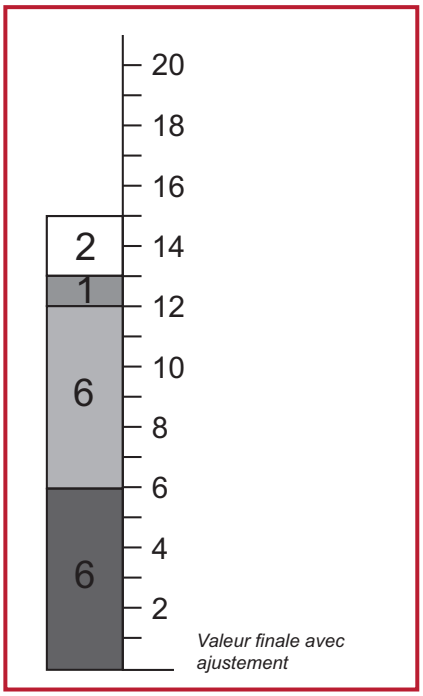
L'étape suivante consiste à affiner l'estimation initiale en considérant des facteurs supplémentaires tels que ceux répertoriés dans le tableau ci-après. Il est fréquent qu'on ne puisse les considérer convenablement que lorsque la machine est installée à son poste définitif.

Type de facteur	**Action proposée**
Plus d'une seule personne exposée à la source de danger.	Multiplier le facteur de gravité par le nombre de personnes.
Présence prolongée dans la zone de danger sans complète isolation de l'alimentation.	Si le temps écoulé pendant l'accès est supérieur à 15 minutes, ajouter 1 point au facteur de fréquence.
Opérateur sans qualification ni formation.	Ajouter 2 points à la valeur totale.
Très longs intervalles de temps (ex. 1 an) entre deux accès. (Possibilité d'une défaillance progressive et non détectée, particulièrement dans les systèmes de surveillance.)	Ajouter à la valeur du facteur de fréquence l'équivalent du maximum possible.

Facteurs additionnels pour l'évaluation du risque

Les résultats d'éventuels facteurs additionnels sont ensuite ajoutés au total précédent comme indiqué.





REDUCTION DES RISQUES

Il nous faut à présent considérer individuellement chaque machine et ses risques, et prendre des mesures pour identifier toutes ses sources de danger.

La figure suivante illustre une partie de tableau correspondant à la procédure documentée de prise en compte de tous les aspects de sécurité de la machine utilisée. Il sert de guide pour les utilisateurs de machines, mais les fabricants ou les fournisseurs de machines peuvent également utiliser le même principe pour confirmer que tous les équipements ont été évalués. Il sert également d'indice pour des rapports plus détaillés sur l'évaluation du risque.

Lorsqu'une machine porte le marquage CE, la procédure est plus simple car les phénomènes dangereux associés à la machine ont déjà été évalués par le fabricant et toutes les mesures nécessaires prises. Même si des équipements sont marqués CE, il peut subsister des phénomènes dangereux, en raison de la nature de l'application ou du matériau traité, que le fournisseur n'a pas pu prévoir.

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

Société – MAYKIT WRIGHT LTD
Etablissement – Atelier d'outillage – Usine Est.
Date – 29/8/95
Profil de l'opérateur – Qualifié

Identification et date de l'équipement	Conformité aux directives	Numéro du rapport d'évaluation des risques	Historique des accidents	Notes	Identification du danger	Type de danger	Action requise	Mis en œuvre et inspecté – Référence
Tour parallèle Bloggs. N° de série 8390726 Installé en 1978	Aucune	RA302	Aucun	Equipement électrique conforme à BS EN 60204 avec arrêt d'urgence (remplacé en 1989)	Rotation de mandrin avec protection ouverte	Coupure par enchevêtrement mécanique	Installer un interrupteur de sécurité	11/25/94 J Kershaw Rapport n° 9567
					Liquide de coupe	Toxique	Changer pour un type non toxique	11/30/94 J Kershaw Rapport n° 9714
					Nettoyage d'ébarbures	Coupure	Fournir des gants	11/30/94 J Kershaw Rapport n° 9715
Tourelle de fraisage Bloggs N° de série 17304294 Fabriquée en 1995 Installée en mai 95	Directive Machines Directive CEM	RA416	Aucun		Mouvement du bâti (vers le mur)	Ecrasement	Déplacer la machine pour donner un espace suffisant	4/13/95 J Kershaw Rapport n° 10064

Hiérarchie des mesures pour la réduction des risques

Il existe trois méthodes à prendre en considération et à utiliser dans l'ordre suivant :

1. Eliminer ou réduire le risque dans toute la mesure du possible (sécurité intrinsèque dans la conception et la fabrication de la machine) ;

2. Installer les systèmes et les mesures de protection nécessaires (p. ex. barrières munis d'interrupteurs de sécurité, barrières immatérielles, etc.) en fonction des risques ne pouvant pas être éliminés à la conception.

3. Informer les utilisateurs des risques résiduels consécutifs aux carences des mesures de protection adoptées, préciser si une formation particulière est nécessaire, et spécifier toute nécessité de fournir un équipement de protection individuelle.

Chaque mesure de l'ordre hiérarchique doit être considérée en démarrant du début et utilisée chaque fois que possible. Ceci conduit généralement à mettre en œuvre plusieurs mesures simultanément.

Sécurité à la conception

Il est possible d'éviter un grand nombre de dangers potentiels au moment de la conception, simplement en faisant attention à des facteurs comme les matériaux, les impératifs d'accès, les surfaces chaudes, les méthodes de transmission, les points pièges, les niveaux de tension, etc.

Par exemple, s'il n'est pas nécessaire d'accéder à une zone à risque, la solution est de la protéger de l'intérieur de la machine ou par un dispositif de protection fermé fixe.

Systèmes et mesures de protection

Si à l'inverse un accès est nécessaire, la situation se complique un peu. Il faut alors veiller à ce que cet accès ne soit possible que lorsque la machine est en situation non dangereuse. Des mesures de protection telles que des dispositifs de protection dotés d'interrupteurs de sécurité et/ou systèmes de déclenchement sont nécessaires. Le choix du dispositif ou système de protection à utiliser doit être largement conditionné par les caractéristiques de fonctionnement de la machine. Cette exigence est extrêmement importante, car un système qui dégrade le rendement de la machine est susceptible d'être mis hors service ou neutralisé sans autorisation.

Dans ce cas de figure, la sécurité de la machine est fonction de l'application adéquate et du fonctionnement correct du système de protection, même en cas de défaillance.

Il faut maintenant prendre en considération le fonctionnement correct du système. Dans chaque type, le choix existe vraisemblablement entre plusieurs technologies plus ou moins performantes en matière de surveillance, de détection ou de prévention des pannes.

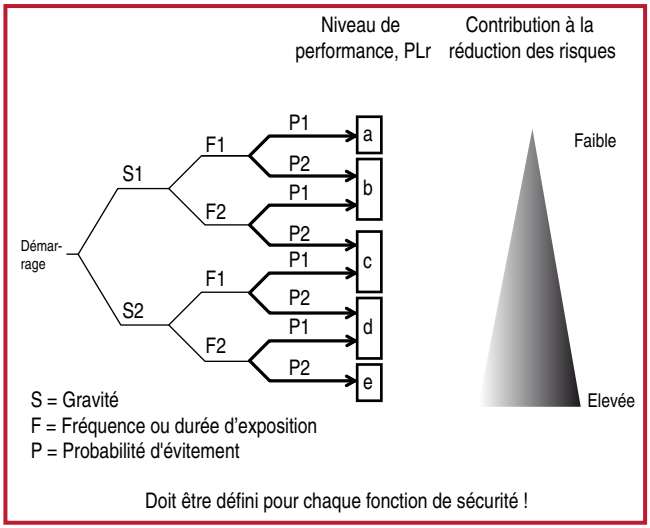
Dans l'idéal, chaque système de protection serait absolument parfait, sans aucune possibilité de se mettre en situation dangereuse. Or, en réalité, nous sommes restreints par les limites actuelles de la connaissance et des matériaux. Une autre contrainte bien réel est le coût. Compte tenu de tous ces facteurs, il devient évident que le sens de la mesure s'impose. Il suffit d'un peu de bon sens pour se rendre compte qu'il serait ridicule d'exiger qu'un système, dont la défaillance n'entraîne dans le pire des cas qu'une contusion légère, offre la même sûreté que celle requise pour tenir un avion gros porteur en vol. Les conséquences d'une défaillance n'ont rien à voir ; c'est pourquoi il nous faut d'une manière ou d'une autre mettre en rapport l'importance des mesures de protection avec le niveau de risque établi lors de la phase d'appréciation du risque.

Quel que soit le type de dispositif de protection adopté, il ne faut pas oublier qu'un « système destiné à la sécurité » est susceptible d'être constitué d'un grand nombre d'éléments, notamment l'équipement de protection, le câblage, le dispositif de commutation de l'alimentation et parfois même certaines parties du système de commande de fonctionnement de la machine. Tous ces éléments du système (y compris les dispositifs de protection, les supports, le câblage, etc.) doivent présenter des caractéristiques de performance admissibles en rapport avec leur principe de conception et leur technologie. La version pré-révision de la norme ISO 13849-1 définit plusieurs catégories pour les pièces de sécurité des systèmes de commande et fournit un graphique présentant les risques dans son annexe B. Ceci est une approche très simple, mais elle peut fournir des conseils utiles pour déterminer certains des critères du système de protection.

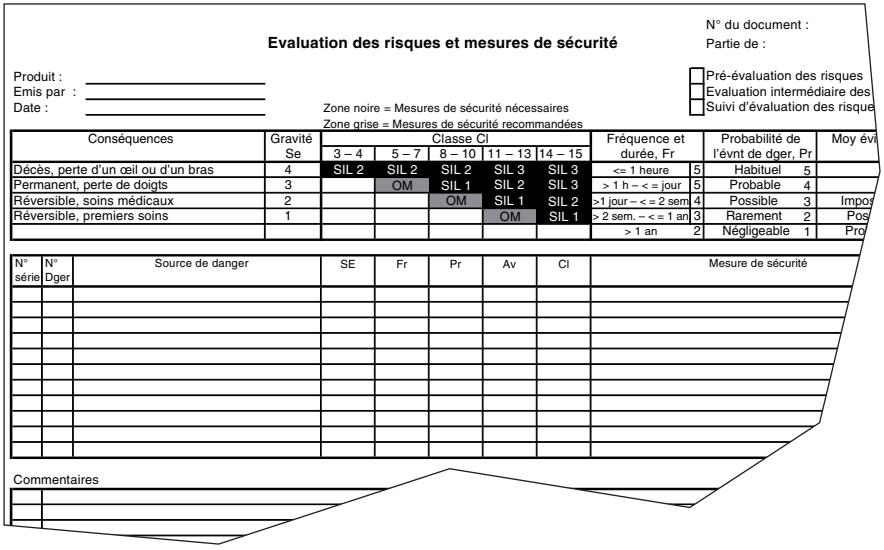
Les versions révisées des normes ISO 13849-1 et CEI 62061 présentent des méthodes et des conseils utiles sur la façon de définir un système de commande de sécurité qui fournit des mesures de protection ou une fonction de sécurité.

EN ISO 13849-1:2008 fournit un graphique des risques amélioré en annexe A.

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



CEI 62061 fournit également une méthode en annexe A, sous la forme présentée ci-dessous.



Evaluation des risques et mesures de sécurité

N° du document :
Partie de :

Produit :
Emis par :
Date :

Zone noire = Mesures de sécurité nécessaires
Zone grise = Mesures de sécurité recommandées

☐ Pré-évaluation des risques
☐ Evaluation intermédiaire des
☐ Suivi d'évaluation des risque

Conséquences	Gravité Se	Classe Cl 3 – 4	5 – 7	8 – 10	11 – 13	14 – 15	Fréquence et durée, Fr		Probabilité de l'évnt de dger, Pr		Moy évi
Décès, perte d'un œil ou d'un bras	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 heure	5	Habituel	5	
Permanent, perte de doigts	3		OM	SIL 1	SIL 2	SIL 3	> 1 h – < = jour	5	Probable	4	
Réversible, soins médicaux	2			OM	SIL 1	SIL 2	>1 jour – < = 2 sem	4	Possible	3	Impos
Réversible, premiers soins	1				OM	SIL 1	> 2 sem. – < = 1 an	3	Rarement	2	Pos
							> 1 an	2	Négligeable	1	Pro

N° série	N° Dger	Source de danger	SE	Fr	Pr	Av	Cl	Mesure de sécurité

Commentaires

L'utilisation d'une des méthodes ci-dessus doit donner des résultats équivalents. Chaque méthode est prévue pour prendre en considération le contenu détaillé de la norme à laquelle elle appartient.

Dans les deux cas, il est très important que les conseils fournis dans le texte de la norme soient suivis. Le graphique ou le tableau des risques ne doit pas être utilisé séparément ou de façon trop simpliste.

Evaluation

Après avoir choisi la mesure de protection et avant de la mettre en œuvre, il est important de refaire une évaluation du risque. Cette procédure est souvent oubliée. Si une mesure de protection est installée, l'opérateur peut se sentir totalement protégé contre le risque envisagé à l'origine. Puisque la conscience du danger n'est plus si présente, il peut interagir avec la machine d'une façon différente. Il peut par exemple être exposé au danger plus souvent ou pénétrer plus loin dans l'espace de la machine. Ce qui signifie qu'en cas de défaillance de la mesure de protection, il y a un plus grand risque que celui envisagé précédemment. C'est ce risque réel qui doit être évalué. Par conséquent, l'évaluation du risque doit être répétée en prenant en compte tout changement prévisible dans la façon dont le personnel peut intervenir sur la machine. Le résultat de cette évaluation est utilisé pour vérifier si les mesures de protection envisagées sont bien adaptées. Pour de plus amples informations, il est recommandé de consulter l'annexe A de la norme CEI 62061.

Formation, équipement de protection individuelle, etc.

Il est primordial que les opérateurs reçoivent la formation nécessaire sur les méthodes de travail en toute sécurité sur une machine. Ceci ne signifie pas que les autres mesures peuvent être omises. Il n'est pas admissible de se contenter de donner à un opérateur l'instruction de ne pas s'approcher des zones à risque (au lieu de mettre en place des équipements de protection).

L'opérateur peut également devoir utiliser certains équipements, comme des gants spéciaux, des lunettes de protection, un appareil respiratoire, etc. Le concepteur de la machine doit spécifier quels équipements sont nécessaires. L'utilisation d'équipements de protection individuelle ne constitue généralement pas la principale méthode de protection individuelle, mais vient en complément des mesures évoquées plus haut.

Normes

De nombreuses normes et divers rapports techniques fournissent des conseils pour l'évaluation du risque. Certains sont destinés à une utilisation généraliste et d'autres à des applications spécifiques.

La liste suivante présente des normes qui contiennent des informations sur l'évaluation du risque.

ANSI B11.TR3 : Risk assessment and risk reduction – A guide to estimate, evaluate and reduce risks associated with machine tools

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

ANSI PMMI B155.1 : Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery (normes de sécurité pour les machines de conditionnement et les machines de transformation pour le conditionnement)

ANSI RIA R15.06 : Safety Requirements for Industrial Robots and Robot Systems (normes de sécurité pour les robots industriels et les systèmes robotisés)

AS 4024.1301-2006 : Principles of risk assessment (notions fondamentales pour l'évaluation du risque)

CSA Z432-04 : Safeguarding of Machinery (protection des machines)

CSA Z434-03 : Industrial Robots and Robot Systems – General Safety Requirements (robot industriels et systèmes robotisés – normes de sécurité)

CEI/EN 61508 : Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

CEI/EN 62061 : Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité

ISO 14121 (EN 1050) : Principes pour l'appréciation du risque

Mesures de protection et équipement complémentaire

Lorsque l'évaluation des risques montre qu'une machine ou un procédé présente un risque de blessure corporelle, la source de danger doit être éliminée ou limitée. Le moyen d'y parvenir dépend du type de machine et de la source de danger. Les systèmes de protection sont définis comme des méthodes dont l'objectif est de limiter l'accès à une zone à risque ou de détecter tout accès à cette zone. Les systèmes de protection incluent des dispositifs comme les barrières fixes, les barrières munies d'interrupteurs de sécurité, les barrières immatérielles, les tapis de sécurité, les commandes bimanuelles et les poignées de sécurité.

Blocage de l'accès avec dispositifs de protection fermés fixes

Si la source de danger a pour siège une partie de la machine dont l'accès n'est pas nécessaire, celle-ci doit être protégée de manière permanente par des dispositifs de protection fixes. Le retrait de ces protections doit nécessiter des outils. Ces dispositifs fixes doivent être capables de 1) résister à l'environnement dans lequel ils sont utilisés, 2) contenir les projectiles le cas échéant et 3) ne pas être une source de danger, par exemple ne pas avoir de bords coupants. Les dispositifs de protection fixes peuvent avoir des ouvertures à l'endroit où le dispositif et la machine se rejoignent, ou des ouvertures dues à l'utilisation d'un treillis métallique.

Des fenêtres permettent de surveiller le fonctionnement de la machine. Le choix du matériau utilisé est important ; en effet, les interactions chimiques avec les liquide de coupe, les rayons ultraviolets et le vieillissement entraînent un dégradation du matériau des fenêtres avec le temps.

La taille des ouvertures ne doit pas permettre à l'opérateur d'atteindre la zone à risque. Le tableau O-10 de la norme OHSA 1910.217 (f) (4), la norme ISO 13854, le tableau D-1 de la norme ANSI B11.19, le tableau 3 de la norme CSA Z432 et la norme AS4024.1 fournissent des conseils sur la distance appropriée entre une ouverture et la zone à risque.

Détection d'accès

Le système de protection est utilisé pour détecter tout accès à la zone à risque. Lorsque la détection est sélectionnée comme méthode de réduction des risques, le concepteur doit être conscient qu'un système de sécurité complet doit être utilisé ; le dispositif de protection seul ne permet pas une réduction des risques suffisante.

Ce système de sécurité est généralement constitué de trois blocs : 1) un capteur qui détecte l'accès à la zone à risque, 2) un dispositif logique qui traite les signaux provenant du dispositif de détection, vérifie l'état du système de sécurité et active ou désactive les dispositifs de sorties, et 3) un dispositif de sorties qui commande l'actionneur (par exemple, un moteur).

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

Dispositifs de détection

Il existe de nombreux dispositifs capables de détecter une personne entrant dans la zone à risque ou présente dans cette zone. Le meilleur choix pour une application particulière dépend de plusieurs facteurs.

- Fréquence d'accès
- Délai d'arrêt du danger
- Nécessité de terminer le cycle de la machine
- Confinement des projectiles, des liquides, des pulvérisations, des vapeurs, etc.

Des protections mobiles adaptées peuvent être interconnectées afin de fournir une protection contre les projectiles, les liquides, les pulvérisations et d'autres types de dangers ; de plus, elles sont souvent utilisées lorsque l'accès à la zone à risque n'est pas fréquent. Des barrières munis d'interrupteurs de sécurité peuvent également être verrouillées pour bloquer l'accès lorsque la machine est en fonctionnement et lorsqu'elle prend beaucoup de temps pour s'arrêter.

Les dispositifs de détection de présence, comme les barrières immatérielles, les tapis et les scrutateurs, fournissent un accès rapide et facile à la zone à risque et sont souvent choisis lorsque les opérateurs doivent fréquemment accéder à la zone à risque. Ces types de dispositifs de protection ne protègent pas contre les projectiles, les pulvérisations, les liquides ou d'autres dangers de ce genre.

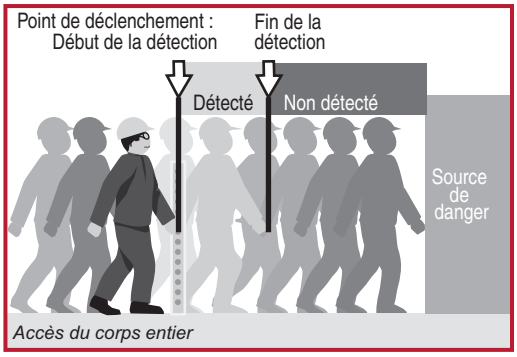
La meilleure protection est celle par laquelle le dispositif ou le système utilisé offre un maximum de protection pour un minimum de gêne dans l'exploitation de la machine. Tous les aspects d'usage de la machine doivent être pris en compte, l'expérience montrant en effet qu'un système difficile à mettre en œuvre est davantage susceptible d'être mis hors service ou neutralisé.

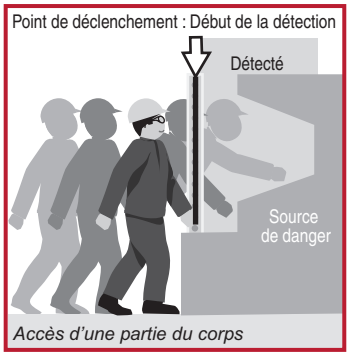
Dispositifs de détection de présence

Lorsqu'il s'agit de décider comment protéger une zone, il est important de comprendre exactement quelles sont les fonctions de sécurité qui sont nécessaires. En général, on trouvera au moins deux fonctions.

- Couper ou désactiver l'alimentation lorsqu'une personne pénètre dans la zone à risque.
- Empêcher la mise sous tension ou l'activation de l'alimentation quand une personne se trouve dans la zone à risque.

A première vue, on pourrait penser qu'il ne s'agit que d'une seule et même fonction, mais il s'agit bien de deux fonctions distinctes même si elles sont manifestement liées et qu'elle sont souvent réalisées au moyen du même équipement. Pour réaliser la première fonction, un dispositif de déclenchement est nécessaire. En d'autres termes, un dispositif qui détecte qu'une personne a partiellement dépassé un certain point et qui envoie un signal pour couper l'alimentation. Si cette personne est en mesure de poursuivre au-delà du point de déclenchement et que sa présence n'est plus détectée, alors la deuxième fonction (prévention de la remise sous tension) ne peut être remplie.





Le schéma donne un exemple d'accès de tout le corps avec comme dispositif de déclenchement, une barrière immatérielle montée verticalement. Les barrières munis d'interrupteurs de sécurité peuvent également être considérées comme dispositifs uniquement déclencheurs lorsqu'il n'y a rien pour empêcher la barrière d'être fermée après être entré dans la zone à risque.

Si l'accès de tout le corps n'est pas possible, c'est-à-dire que la personne ne peut poursuivre au-delà du point de déclenchement, sa présence sera toujours détectée et la deuxième fonction (prévention de la mise sous tension) sera remplie.

Pour les applications de détection d'une partie du corps, ce sont les mêmes types de dispositifs qui assurent le déclenchement et la détection de présence. La seule différence réside dans le type d'application.

Les dispositifs de détection de présence sont utilisés pour détecter la présence des personnes. Cette gamme de dispositifs inclut les barrières immatérielles de sécurité, les barrières de sécurité à faisceau unique, les scrutateurs de zone de sécurité, les tapis de sécurité et les bourrelets de sécurité.

Barrières immatérielles de sécurité

On peut définir simplement les barrières immatérielles de sécurité comme des détecteurs photoélectriques de présence particulièrement conçus pour protéger le personnel contre toute blessure causée par le mouvement dangereux d'une machine. Egalement appelées dispositifs optoélectroniques de protection active et, dans les nouvelles normes équipements de protection électrosensibles, les barrières immatérielles offrent une sécurité optimale, et permettent pourtant une plus grande productivité car elles constituent la meilleure solution ergonomique par rapport aux protections mécaniques. Elles sont particulièrement bien adaptées aux applications dans lesquelles le personnel doit fréquemment accéder à une zone à risque.

Les barrières immatérielles sont conçues et testées en conformité avec les normes CEI 61496-1 et -2. L'annexe IV de la Directive Machines européenne impose une certification des barrières immatérielles par un organisme tiers avant de pouvoir les mettre sur le marché de l'Union

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

européenne. Ces organismes tiers testent les barrières immatérielles pour leur conformité avec cette norme internationale. Underwriter's Laboratory a adopté la norme CEI 61496-1 comme norme nationale aux Etats-Unis.

Scrutateurs laser de sécurité

Les scrutateurs laser de sécurité utilisent un miroir pivotant qui dévie les impulsions lumineuses sur un arc, créant ainsi un plan de détection. L'emplacement de l'objet est déterminé par l'angle de rotation du miroir. En utilisant la technique de la « durée du trajet » d'un faisceau réfléchi de lumière invisible, le scrutateur peut également détecter la distance de l'objet par rapport au scrutateur. En prenant la distance mesurée et l'emplacement de l'objet, le scrutateur laser détermine la position exacte de l'objet.

Tapis de sécurité sensibles à la pression

Ces dispositifs sont affectés à la protection d'une zone de sol autour d'une machine. Une matrice de tapis interconnectés est disposée autour de la zone à risque, et toute pression détectée (par exemple le pas d'un opérateur) entraîne la coupure de la source d'alimentation par l'organe de commande du tapis. Les tapis sensibles à la pression sont fréquemment utilisés dans les zones fermées contenant plusieurs machines – cellules de fabrication adaptables, ou de robotique, par exemple. Lorsqu'il est nécessaire d'accéder à la cellule (pour le réglage ou « l'apprentissage » du robot par exemple), ils empêchent les mouvements dangereux si l'opérateur s'écarte de la zone sécurisée, ou s'il doit atteindre l'arrière d'un équipement.

La taille et le positionnement du tapis doivent prendre en compte la distance de sécurité.

Bourrelets sensibles de sécurité

Ces dispositifs se présentent sous la forme de bandes flexibles pouvant être montées sur le bord d'une partie mobile, comme une table élévatrice ou une porte motorisée, pouvant présenter un risque d'écrasement ou de coupure.

Si la partie mobile se heurte à l'opérateur (et inversement), les bourrelets se compriment et coupent l'alimentation de la machine. Les bourrelets sensibles peuvent aussi être utilisés pour protéger l'opérateur en cas de risque d'étranglement. Si cela se produit, le contact avec le bourrelet sensible entraîne la coupure de l'alimentation de la machine.

Il existe différentes techniques utilisées pour créer des bourrelets de sécurité. Une de ces techniques très répandue consiste à insérer ce qui est essentiellement un long interrupteur dans le bourrelet. Cette technique permet d'obtenir des bourrelets droits et utilise généralement une connectique à 4 fils.

Les barrières immatérielles, les scrutateurs, les tapis de sol et les bourrelets sensibles sont classés « dispositifs déclencheurs. Ils n'interdisent pas le passage mais le « détectent » seulement. Ils s'en remettent entièrement à leur capacité de détection et de coupure de la

source d'alimentation par mesure de sécurité. En général, ils ne conviennent qu'aux machines pouvant s'arrêter dans un délai raisonnablement court après coupure de la source d'alimentation. Du fait qu'un opérateur peut marcher ou atteindre directement la zone à risque, il est de toute évidence nécessaire que le temps nécessaire à l'arrêt du mouvement soit inférieur à celui pris par l'opérateur pour atteindre la zone à risque après déclenchement du dispositif.

Pour de plus amples informations sur la détection de présence, consultez le site www.ab.com/safety.

Interrupteurs de sécurité

Lorsque l'accès à la machine n'est pas fréquent, les protections mobiles (pouvant être actionnés) ont la préférence. Le dispositif de protection est relié à l'alimentation de la source de danger, de sorte que lorsque la barrière de protection n'est pas fermée, l'alimentation de la source de danger est désactivée. Cette approche impose le montage d'un interrupteur de sécurité sur le dispositif de protection. La commande de l'alimentation de la source de danger transite par le circuit interrupteur de l'unité. La source d'alimentation est le plus souvent électrique, mais elle peut également être pneumatique ou hydraulique. Lorsque le mouvement de la barrière de protection (son ouverture) est détecté, l'interrupteur de sécurité coupe toute source d'alimentation, soit directement, soit par l'intermédiaire d'un contacteur de puissance (ou clapet).

Certains interrupteurs incorporent en outre un système de verrouillage qui bloque la barrière en position fermée et interdit son ouverture tant que la machine présente un danger. Dans la majorité des applications, l'utilisation combinée d'une protection mobile et d'un interrupteur de sécurité, avec ou sans verrouillage, constitue la meilleure solution en termes de fiabilité et de coût.

Il existe de nombreuses options d'interrupteurs de sécurité, notamment :

- **Interrupteur de sécurité à broche –** Ces dispositifs ont besoin qu'un actionneur en forme de broche soit inséré et retiré de l'interrupteur pour fonctionner.

- **Interrupteurs de sécurité à charnière –** Ces dispositifs sont placés sur l'axe de la charnière d'une barrière de sécurité et sont actionnés lors de l'ouverture de la barrière.

- **Interrupteurs de sécurité à verrouillage –** Dans certaines applications, il est nécessaire de verrouiller la barrière en position fermée ou de retarder son ouverture. Les dispositifs qui répondent à cette exigence sont appelés interrupteurs de sécurité à verrouillage. Ils conviennent particulièrement aux machines dont l'arrêt n'est pas instantané, mais peuvent également apporter un niveau de protection supplémentaire à la plupart des autres matériels.

- **Interrupteurs de sécurité sans contact –** Ces dispositifs n'ont pas besoin de contact physique pour être actionnés. Certaines versions incluent une fonction de codage pour une meilleure protection contre les modification indésirables.

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

- **Détecteurs de position –** Les actionneurs à came sont généralement des détecteurs de position en mode positif avec came linéaire ou rotative. Ils sont généralement utilisés sur les protections coulissantes.

- **Interrupteurs à clé captive –** Les clés captives peuvent servir pour le verrouillage de commande et le verrouillage d'alimentation. Dans le cas du verrouillage de commande, un dispositif de verrouillage envoie une commande d'arrêt à un dispositif intermédiaire, qui à son tour arrête un autre dispositif afin de couper l'alimentation de l'actionneur. Dans le cas du verrouillage d'alimentation, la commande d'arrêt interrompt directement la source d'alimentation des actionneurs de la machine.

Dispositifs d'interface opérateur

Fonction d'arrêt – Aux Etats-Unis, au Canada, en Europe et au niveau international, une harmonisation des normes existe pour la description des catégories d'arrêt des machines ou des systèmes de fabrication.

REMARQUE : ces catégories sont différentes de celles qui figurent dans la norme EN 954-1 (ISO 13849-1). Voir les normes NFPA79 et CEI/EN 60204-1 pour plus de détails. Les arrêts sont classés en trois catégories :

La **catégorie 0** assure la coupure immédiate de l'alimentation des actionneurs de la machine. On considère que ceci est un arrêt incontrôlé. Une fois l'alimentation coupée, toute action de freinage nécessitant du courant électrique ne fonctionnera pas. Cet arrêt permet aux moteurs de continuer à tourner jusqu'à arrêt absolu après une période relativement longue. Dans d'autres cas, les matériaux tomberont de la machine car ses mécanismes électriques de maintien des matériaux ne seront plus alimentés. L'arrêt mécanique, qui ne nécessite pas d'alimentation électrique, peut aussi être utilisé avec un arrêt de catégorie 0. L'arrêt de catégorie 0 a la priorité sur les arrêts de catégorie 1 ou de catégorie 2.

La **catégorie 1** est un arrêt contrôlé avec maintien de l'alimentation sur les actionneurs de la machine pour pouvoir en assurer l'arrêt. L'alimentation est ensuite coupée au niveau des actionneurs une fois que l'arrêt est effectif. Cette catégorie d'arrêt permet d'arrêter rapidement un mouvement dangereux grâce à un freinage électrique, et ensuite de couper l'alimentation des actionneurs.

La **catégorie 2** est un arrêt contrôlé avec maintien de l'alimentation sur les actionneurs de la machine. Un dispositif d'arrêt de production normal est considéré comme un arrêt de catégorie 2.

Ces catégories d'arrêt doivent être appliquées à chaque fonction d'arrêt, lorsque la fonction d'arrêt est l'action effectuée par les parties de la commande relatives à la sécurité, en réponse à une entrée de catégorie 0 ou 1. Les fonctions d'arrêt doivent être prioritaires sur les fonctions correspondantes de démarrage. Le choix de la catégorie d'arrêt pour chaque fonction d'arrêt doit être déterminée par une appréciation du risque.

Fonction d'arrêt d'urgence

La fonction d'arrêt d'urgence doit fonctionner comme un arrêt de catégorie 0 ou 1, selon l'appréciation du risque. Elle doit pouvoir être déclenchée par une seule action humaine. Lorsqu'elle est déclenchée, elle doit être prioritaire sur toutes les autres fonctions et modes de fonctionnement de la machine. L'objectif est de couper l'alimentation le plus vite possible sans créer de dangers supplémentaires.

Jusqu'à récemment, il était nécessaire d'utiliser des composants électromécaniques câblés dans les circuits d'arrêt d'urgence. Les modifications récentes de normes, comme les normes CEI 60204-1 et NFPA 79, signifient que les PLC de sécurité et autres formes de logique électronique conformes aux exigences des normes comme la CEI 61508, peuvent être utilisés dans le circuit d'arrêt d'urgence.

Dispositifs d'arrêt d'urgence

Chaque fois qu'il y a danger pour un opérateur face à une machine, celle-ci doit être munie d'un dispositif d'arrêt d'urgence rapidement accessible. Le dispositif d'arrêt d'urgence doit être opérationnel en permanence et immédiatement accessible. Le pupitre opérateur doit comporter au moins un dispositif d'arrêt d'urgence. Des dispositifs supplémentaires d'arrêt d'urgence peuvent être implantés à d'autres endroits selon les besoins. Les dispositifs d'arrêt d'urgence se présentent sous diverses formes. Les boutons-poussoirs et les arrêts d'urgence à câble sont des exemples de dispositifs les plus fréquemment utilisés. Lorsque le dispositif d'arrêt d'urgence est actionné, il doit s'enclencher et il ne doit pas être possible de générer la commande d'arrêt sans enclenchement. La réinitialisation du dispositif d'arrêt d'urgence ne doit pas créer de situation à risque. Le redémarrage de la machine doit faire l'objet d'une action distincte et délibérée de la part de l'opérateur.

Pour plus d'informations sur les dispositifs d'arrêt d'urgence, consultez les normes ISO/EN 13850, CEI 60947-5-5, NFPA79 et CEI60204-1, AS4024.1, Z432-94.

Boutons d'arrêt d'urgence

Les dispositifs d'arrêt d'urgence sont considérés comme des équipements de protection complémentaires. Il ne sont pas considérés comme dispositifs de protection principaux parce qu'ils n'empêchent pas l'accès à une source de danger et ne détectent pas l'accès à une zone dangereuse.

Ils prennent souvent la forme d'un bouton-poussoir de couleur rouge et en forme de champignon, implanté sur un boîtier de couleur jaune, et que l'opérateur enfonce en cas de danger (voir Figure 4.59). Ces dispositifs doivent être placés aux points stratégiques et en nombre suffisant autour de la machine pour garantir qu'il y en a toujours un à portée de main dans une zone à risque.

Les boutons d'arrêt d'urgence doivent être facilement accessibles et doivent être utilisables pour tous les modes de fonctionnement de la machine. Lorsqu'un bouton-poussoir est utilisé comme dispositif d'arrêt d'urgence, il doit être en forme de champignon (ou à coup-de-poing),

de couleur rouge et avec un boîtier jaune. Lorsque le bouton est enfoncé, les contacts doivent changer d'état et en même temps le bouton est verrouillé en position enfoncée.

L'une des dernières techniques appliquées aux dispositifs d'arrêt d'urgence est une technique d'auto-surveillance. Un contact supplémentaire est ajouté à l'arrière du dispositif afin de surveiller si l'arrière des composants du panneau sont toujours présents. Ceci est un bloc de contacts à auto-surveillance. Il est constitué d'un contact actionné par ressort qui se ferme lorsque le bloc de contacts est enclenché en position sur le panneau. La figure 4.60 montre le contact à auto-surveillance connecté en série avec un des contacts de sécurité à ouverture directe.

Arrêts d'urgence à câble

Pour des machines comme des convoyeurs à bande, il est souvent plus pratique et plus efficace d'utiliser un arrêt d'urgence à câble placé le long de la zone à risque (voir Figure 4.61). Ces dispositifs incorporent un câble d'acier accroché à des interrupteurs, de telle sorte qu'une traction exercée dans n'importe quelle direction sur le câble en quelque endroit de sa longueur, déclenche l'interrupteur et coupe l'alimentation de la machine.

Ces dispositifs à câble doivent détecter à la fois une tension exercée sur le câble et une absence de tension du câble. La détection du manque de tension permet de s'assurer que le câble n'a pas été coupé et est prêt à fonctionner.

La longueur du câble a un effet sur les performances du dispositif. Pour les petites longueurs, l'interrupteur de sécurité est monté à une extrémité et un ressort de tension est fixé à l'autre extrémité. Pour les grandes longueurs, un interrupteur de sécurité doit être monté à chaque extrémité du câble afin d'assurer que toute action de l'opérateur déclenche la commande d'arrêt. La force exercée sur le câble ne doit pas dépasser 200 N (45 lbs) et sa longueur doit être inférieure à 400 mm (15.75 in) à une position centrée entre deux supports de câble.

Commandes bimanuelles

L'utilisation de commandes nécessitant les deux mains (ou commandes bimanuelles) constitue une solution courante pour empêcher l'accès à la machine lorsque celle-ci présente un danger. Deux commandes doivent être actionnées en même temps (à moins de 0,5 secondes d'intervalle) pour démarrer la machine. Ceci assure que les deux mains de l'opérateur sont occupées en position de sécurité (c'est-à-dire sur les commandes) et qu'elles ne peuvent donc se trouver dans la zone à risque. Les commandes doivent être actionnées en continue temps que le danger est présent. Le fonctionnement de la machine doit cesser dès qu'une des commandes est relâchée ; si l'une des commandes est relâchée, l'autre doit également être relâchée avant de pouvoir redémarrer la machine.

Tout système bimanuel est très largement tributaire de l'efficacité de son système de commande et de surveillance à détecter toute défaillance, si bien qu'il est essentiel que des spécifications correctes soient retenues pour la conception de ce système. Les performances du système de sécurité bimanuel sont définies par types dans la norme ISO 13851 (EN 574), comme indiqué, et ces types sont liés aux catégories de la norme ISO 13849-1. Les types les

plus utilisés pour la sécurité des machines sont les types IIIB et IIIC. Le tableau suivant montre la relation entre ces types et les catégories de performance de sécurité.

Prescriptions	Types				
	I	II	III		
			A	B	C
Activation synchrone			X	X	X
Utilisation de la catégorie 1 (ISO 13849-1)	X		X		
Utilisation de la catégorie 3 (ISO 13849-1)		X		X	
Utilisation de la catégorie 4 (ISO 13849-1)					X

L'ergonomie du pupitre doit rendre impossible toute manœuvre dangereuse (actionnement par la main et le coude, par exemple). Ceci peut être obtenu grâce à la distance ou à des écrans protecteurs. La machine ne doit pas pouvoir enchaîner deux cycles successifs sans que les deux boutons de commande soient relâchés, puis actionnés. Cela empêche de bloquer les deux boutons ensemble pour laisser tourner la machine en continu. Le relâchement de l'un des deux boutons doit entraîner l'arrêt de la machine.

L'utilisation d'une commande bimanuelle doit être envisagée avec discernement, tout risque n'étant en général pas complètement écarté. La commande bimanuelle ne protège que la personne qui l'utilise. L'opérateur protégé doit pouvoir observer tous les accès à la zone de danger, les autres personnes n'étant peut-être pas protégées.

La norme ISO 13851 (EN 574) fournit des conseils supplémentaires sur la commande bimanuelle.

Poignées de sécurité

Les poignées de sécurité permettent à l'opérateur d'entrer dans la zone de danger lorsque la source de danger fonctionne, mais uniquement s'il tient la poignée de sécurité en position active. Ces poignées de sécurité utilisent des interrupteurs à deux ou trois positions. Les interrupteurs à deux positions sont désactivés lorsque l'actionneur n'est pas actionné et activés lorsque l'actionneur est actionné. Les interrupteurs à trois positions sont désactivés lorsqu'ils sont actionnés (position 1), activés lorsqu'il sont maintenus en position centrale (position 2) et désactivés lorsque l'actionneur est actionné au-delà de la position médiane (position 3). De plus, lorsqu'ils repassent de la position 3 à la position 1, le circuit de sortie ne doit pas se fermer lorsqu'il passe par la position 2.

Les poignées de sécurité doivent être utilisées conjointement avec d'autres fonctions de sécurité. Un exemple type consiste à mettre le mouvement dans un mode à action lente commandée. Une fois en mode à action lente, un opérateur peut pénétrer dans la zone de danger en tenant la poignée de sécurité.

Lorsqu'une poignée de sécurité est utilisée, un signal doit indiquer que la poignée est active.

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

Dispositifs logiques

Les dispositifs logiques jouent un rôle central dans la partie sécurité du système de commande. Ces dispositifs vérifient et surveillent le système de sécurité et autorisent la machine à démarrer ou exécutent des commandes pour arrêter la machine.

Différents dispositifs logiques sont disponibles et permettent de créer une architecture de sécurité adaptée à la complexité et aux fonctions requises de la machine. Les petits relais de surveillance de sécurité câblés sont économiques et bien adaptés pour les petites machines sur lesquelles un dispositif logique dédié est nécessaire pour compléter la fonction de sécurité. Des relais de surveillance de sécurité modulaires et configurables sont mieux adaptés lorsqu'un grand nombre et une grande diversité de dispositifs de protection et un contrôle minimal de zone sont requis. Pour les machines de taille moyenne ou de grande taille et plus complexes, les systèmes programmables avec E/S distribuées sont préférables.

Relais de surveillance de sécurité

Les modules à relais de surveillance de sécurité jouent un rôle clé dans de nombreux systèmes de sécurité. Ces modules sont généralement composés de plusieurs relais guidés réciproquement avec circuit complémentaire pour assurer le fonctionnement efficace de la fonction de sécurité.

Les relais guidés réciproquement sont des relais « cube » spécialisés. Les relais guidés réciproquement doivent être conformes aux exigences de performance de la norme EN 50025. Fondamentalement, ils sont prévus pour empêcher les contacts normalement fermés et normalement ouverts d'être fermés simultanément. Les conceptions plus récentes remplacent les sorties électromécaniques par des sorties statiques de sécurité.

Les relais de surveillance de sécurité effectuent de nombreuses vérifications sur le système de sécurité. A la mise sous tension, ils effectuent une auto-vérification sur leurs composants internes. Lorsque les capteurs sont activés, le relais de surveillance de sécurité compare les résultats des entrées redondantes. Le cas échéant, le relais vérifie les actionneurs externes. Si le résultat de la vérification est positif, le relais attend un signal de réinitialisation pour activer ses sorties.

Le choix du relais de sécurité approprié dépend de plusieurs facteurs : le type de dispositif qu'il surveille, le type de réinitialisation, le nombre et le type de sorties.

Types d'entrées

Les dispositifs de protection utilisent différentes méthodes pour indiquer que quelque chose s'est produit.

Interrupteurs à contact et arrêts d'urgence : Contacts mécaniques à une seule voie, avec un contact normalement fermé ou deux voies, les deux normalement fermées. Le relais de surveillance de sécurité doit être capable d'accepter une ou deux voies et doit permettre la détection de défaillances multiples pour la disposition à deux voies.

Interrupteurs sans contacts et arrêts d'urgence : Contacts mécaniques à deux voies, une normalement ouverte et une normalement fermées. Le relais de surveillance de sécurité doit être capable de traiter des entrées variées.

Interrupteurs de sortie statiques : Barrières immatérielles, scrutateurs laser, les dispositifs statiques sans contacts ont deux sorties PNP et font leur propre détection de défaillances multiples. Le relais de surveillance de sécurité doit être capable d'ignorer la méthode de détection de défaillances multiples du dispositif.

Tapis sensibles à la pression : Les tapis créent un court-circuit entre deux voies. Le relais de surveillance de sécurité doit être capable de supporter les courts-circuits répétés.

Bourrelets sensibles à la pression : Certains bourrelets sont conçus comme des tapis à 4 fils. Certains sont des dispositifs à deux fils qui crées un changement dans la résistance. Le relais de surveillance de sécurité doit être capable de détecter un court-circuit ou le changement de résistance.

Tension : Mesure la FCEM d'un moteur pendant la décélération. Le relais de surveillance de sécurité doit être capable de tolérer des tensions élevées, ainsi que des basses tensions lorsque le moteur décélère.

Mouvement arrêté : Le relais de surveillance de sécurité doit détecter les flux d'impulsions provenant de divers capteurs redondants.

Commande bimanuelle : Le relais de surveillance de sécurité doit détecter différentes entrées normalement ouvertes et normalement fermées, et doit fournir une temporisation de 0,5 s et un programme de séquencement.

Les relais de surveillance de sécurité doivent être conçus spécifiquement pour dialoguer avec chacun de ces types de dispositifs, qui ont différentes caractéristiques électriques. Certains relais de surveillance de sécurité sont capables de se connecter à différents types d'entrées, mais une fois le dispositif choisi, le relais ne peut dialoguer qu'avec ce dispositif. Le concepteur doit choisir un relais compatible avec le capteur.

Impédance d'entrée

L'impédance d'entrée des relais de surveillance de sécurité détermine le nombre de capteurs pouvant être raccordés au relais et la distance à laquelle les capteurs peuvent être montés. Par exemple, un relais de sécurité peut avoir une impédance d'entrée acceptable maximale de 500 ohms. Si l'impédance d'entrée est supérieure à 500 ohms, le relais ne commute pas sur ses sorties. L'utilisateur doit donc veiller à ce que l'impédance d'entrée reste inférieure au maximum spécifié. La longueur, la section et le type du câblage utilisés conditionnent l'impédance d'entrée.

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

Nombre de capteurs

La procédure d'évaluation du risque permettra de déterminer le nombre de capteurs pouvant être raccordés à un élément de relais de surveillance de sécurité, ainsi que la périodicité à laquelle ils doivent être contrôlés. Pour s'assurer que les arrêts d'urgence et les interrupteurs de sécurité d'accès sont opérationnels, leur fonctionnement doit être contrôlé à intervalles réguliers, comme établi par l'appréciation du risque. Par exemple, une entrée de relais de surveillance de sécurité à deux voies raccordée à une barrière protégée qui doit être ouverte à chaque cycle machine (c'est-à-dire plusieurs fois par jour) ne doit pas nécessairement être contrôlée. La raison en est que l'ouverture de la protection déclenche l'auto-vérification par le relais de ses entrées et de ses sorties (selon la configuration) en vue de détecter des défaillances isolées. Plus le dispositif de protection est ouvert souvent, plus la sûreté du processus de contrôle est élevée.

Autre exemple : les arrêts d'urgence. Ces derniers n'étant le plus souvent utilisés qu'en cas d'urgence, ils sont probablement rarement utilisés. C'est pourquoi leur efficacité doit être confirmée par l'établissement d'un programme prévoyant leur actionnement à intervalles réguliers. L'utilisation du système de sécurité de cette façon s'appelle effectuer un essai de sûreté, et l'intervalle entre les tests de validité est appelé intervalle entre essais de sûreté. Troisième exemple : les panneaux d'accès pour le réglage des machines ; qui, comme les arrêts d'urgence, peuvent être rarement utilisés. Là encore, un programme doit être mis au point pour réaliser la fonction de vérification à intervalles réguliers.

L'évaluation des risques aide à déterminer la nécessité de contrôle des capteurs et la périodicité de ces contrôles. Plus le niveau de risque est élevé, plus la fiabilité requise pour le processus de contrôle doit être importante. Par ailleurs, la fréquence du contrôle « manuel » imposé est inversement proportionnelle à celle du contrôle « automatique ».

Détection de défaillances multiples d'entrées

Dans les systèmes à deux voies, les défauts de court-circuit entre voies des capteurs, également appelés défaillances multiples, doivent être détectés par le système de sécurité. Ceci est réalisé par le capteur ou le relais de surveillance de sécurité.

Les relais de surveillance de sécurité à base de microprocesseur, comme les barrières immatérielles, les scrutateurs laser et les détecteurs sans contact évolués, détectent ces courts-circuits de différentes façons. Une façon courante de détecter les défaillances multiples est d'utiliser différents tests par impulsion. L'impulsion des signaux de sortie est très rapide. L'impulsion de la voie 1 est décalée par rapport à l'impulsion de la voie 2. Si un court-circuit se produit, les impulsions se produisent simultanément et sont détectées par le dispositif.

Les relais de surveillance de sécurité électromécaniques utilisent une technique de diversification différente : une entrée à enclenchement et une entrée à déclenchement. Un court-circuit entre la voie 1 et la voie 2 active le dispositif de protection contre les surintensités et le système de sécurité s'arrête.

Sorties

Les relais de surveillance de sécurité possèdent un nombre différent de sorties. Le types des sorties permet de déterminer quel relais de surveillance de sécurité doit être utilisé dans des applications spécifiques.

La plupart des relais de surveillance de sécurité possèdent au moins 2 sorties de sécurité pouvant fonctionner immédiatement. Les sorties de sécurité des relais sont caractérisés comme normalement ouvertes. Elles sont classées comme sorties de sécurité en raison de la redondance et du contrôle interne. Un deuxième type de sortie sont les sorties à temporisation. Les sorties à temporisation sont généralement utilisées dans les arrêts de catégorie 1, lorsque la machine requiert du temps pour exécuter la fonction d'arrêt avant de permettre l'accès à la zone de danger. Les relais de surveillance de sécurité possèdent également des sorties auxiliaires. Elles sont généralement considérées comme normalement fermées.

Puissances de sortie

Les puissances de sortie indiquent la capacité d'un dispositif de protection à commuter des charges. En principe, les puissances des dispositifs industriels, sont décrites comme résistives ou inductives. Une charge résistive peut être un élément chauffant. Les charges électromagnétiques sont généralement des relais, des contacteurs ou des électro-aimants, pour lesquels il existe la charge à un fort caractère inductif. L'annexe A de la norme CEI 60947-5-1 décrit les caractéristiques des charges. Ceci est également indiqué dans le catalogue des équipements de sécurité, dans la section des principes.

Identification : L'identification est formée d'une lettre suivie d'un chiffre, par exemple A300. La lettre se rapporte au courant thermique conventionnel sous boîtier et indique si le courant est continu ou alternatif. Par exemple, la lettre A représente 10 ampères en courant alternatif. Le chiffre indique la tension d'isolation. Par exemple, 300 représente 300 V.

Utilisation : Les catégories d'emploi indiquent les types de charges que le dispositif doit commuter. Les catégories d'emploi relevant de la norme CEI 60947-5 sont répertoriées dans le Tableau.

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

Utilisation	Description des charges
AC-12	Commande de charges résistives et statiques avec isolement par optocoupleurs
AC-13	Commande de charges statiques avec isolement par transformateur
AC-14	Commande de petites charges électromagnétiques (inférieures à 72 VA)
AC-15	Charges inductives supérieures à 72 VA
DC-12	Commande de charges résistives et statiques avec isolement par optocoupleurs
DC-13	Commande d'électroaimants
DC-14	Commande de charges inductives pourvues de résistances d'économie dans le circuit

Courant thermique, Ith : Le courant thermique conventionnel sous boîtier correspond à la valeur du courant utilisé pour les essais d'échauffement de l'équipement monté dans un boîtier spécifié.

Tension (Ue) et intensité (Ie) nominales de fonctionnement : L'intensité et la tension nominales de fonctionnement définissent les capacités de fermeture et d'ouverture des éléments de coupure en fonctionnement normal. Les produits Allen-Bradley Guardmaster sont spécifiquement conçus pour 125 V c.a., 250 V c.a. et 24 V c.c. Consulter l'usine pour une utilisation sous des tensions différentes des valeurs spécifiées.

VA : Les caractéristiques en VA (Volt-Ampère) indiquent les pouvoirs d'établissement et de coupure du circuit.

Exemple n° 1 : La classification A150, AC-15 indique que les contacts peuvent fermer un circuit de 7 200 VA. Sous 120 V c.a., les contacts peuvent établir un circuit sous 60 A. Puisque AC-15 est une charge électromagnétique, les 60 A ne sont que pour une courte durée ; celle du courant d'appel de la charge électromagnétique. La coupure du circuit ne se fait qu'à 720 VA, car le courant de régime établi de la charge inductive est de 6 A, ce qui correspond au courant de service nominal.

Exemple n° 2 : La classification N150, DC-13 indique que les contacts peuvent établir un circuit de 275 VA. Sous 125 V c.a., les contacts peuvent établir un circuit sous 2,2 A. En courant continu, les charges électromagnétiques n'ont pas un courant d'appel comme en

courant alternatif. La coupure du circuit ne se fait également qu'à 275 VA, car le courant en régime établi de la charge électromagnétique est de 2,2 A, ce qui correspond au courant de service nominal.

Redémarrage de la machine

Si, par exemple, une barrière munies d'interrupteur de sécurité est ouverte alors que la machine fonctionne, elle provoque l'arrêt de cette dernière. Dans la plupart des cas, il est impératif que la machine ne redémarre pas directement sitôt la barrière refermée. Une façon courante de réaliser cela est de s'appuyer sur un démarrage avec contacteur à loquet.

L'appui et le relâchement du bouton de démarrage met sous tension momentanément la bobine de commande du contacteur, laquelle ferme les contacts d'alimentation. Tant que les contacts d'alimentation restent sous tension, la bobine de commande reste alimentée (verrouillage électrique) via les contacts auxiliaires du contacteur qui sont reliés mécaniquement aux contacts d'alimentation. Toute interruption de l'alimentation électrique principale ou du système de commande entraîne la désactivation de la bobine et l'ouverture des contacts d'alimentation principale et auxiliaires. Le système d'interrupteur de sécurité du protecteur est relié au circuit de commande du contacteur. Cela implique que pour redémarrer la machine, il faut fermer le protecteur, puis mettre en position « ON » le bouton normal de démarrage qui réarme le contacteur et démarre la machine.

La norme ISO TR 12100-1 définit clairement les impératifs à respecter pour les situations normales d'interdiction de redémarrage (extrait du paragraphe 3.22.4) :

« Lorsque la protection est en position fermée, les actions dangereuses de la machine protégées par la protection peuvent être exécutées, mais la fermeture de la protection ne peut à elle seule les lancer. »

Un nombre important de machines sont déjà dotées de contacteurs simples ou doubles, au fonctionnement identique à ce qui est précédemment décrit (ou qui utilisent un système qui permet d'obtenir le même résultat). Lorsqu'on monte un dispositif d'interrupteur de sécurité sur une machine existante, il est nécessaire de déterminer si la disposition de commande d'alimentation électrique répond à cette exigence et de prendre au besoin des mesures complémentaires.

Fonctions de réarmement

Les relais de surveillance de sécurité Guardmaster d'Allen-Bradley sont conçus au choix avec réarmement manuel surveillé ou réarmement automatique/manuel.

Réarmement manuel surveillé

Le réarmement manuel surveillé nécessite la fermeture et l'ouverture d'un circuit après fermeture du protecteur ou réarmement de l'arrêt d'urgence. Les contacts auxiliaires du contacteur de puissance, reliés mécaniquement et normalement fermés, sont branchés en série à un bouton de

réarmement à impulsion. Après ouverture puis fermeture du protecteur, le relais de sécurité n'autorise pas le redémarrage de la machine sans une pression de réarmement sur le bouton-poussoir. Une fois cette action réalisée, le relais de sécurité vérifie (donc surveille) que les deux contacteurs sont hors tension et que les deux circuits d'interrupteur de sécurité (et par conséquent les protections) sont fermés. Si ces contrôles sont positifs, la machine peut être redémarrée normalement. L'interrupteur de sécurité doit être placé de manière à offrir à l'opérateur une bonne visibilité de la source de danger, afin de lui permettre de vérifier que la zone est dégagée avant la mise en route.

Réarmement automatique/manuel

Certains relais de sécurité sont dotés d'un réarmement automatique/manuel. Le mode de réarmement manuel n'est pas surveillé et le réarmement se produit lorsque le bouton est enfoncé. Un interrupteur de réarmement en court-circuit ou bloqué n'est pas détecté. Dans ce cas, la ligne de réarmement peut être court-circuitée, ce qui autorise un réarmement automatique. L'utilisateur doit alors prévoir un autre mécanisme pour empêcher le redémarrage de la machine à la fermeture de la porte.

Un dispositif de réarmement automatique ne nécessite aucune action de commutation, mais après désactivation il contrôlera systématiquement la sécurité du système avant de réarmer le système. On ne doit pas confondre un réarmement automatique avec un dispositif dépourvu de fonctions de réarmement. Avec ce dernier, le système de sécurité sera immédiatement en service après désactivation, mais il n'y aura pas de contrôle de sécurité du système.

Protection de commande

Une protection de commande arrête une machine lorsque le protecteur est ouvert et la démarre à nouveau directement lorsque le protecteur est fermé. L'emploi de protections de commande n'est permis que dans certaines conditions strictes en raison du caractère extrêmement dangereux d'un redémarrage intempestif ou d'une impossibilité à s'arrêter. Le système d'interrupteur de sécurité doit présenter un niveau de fiabilité le plus élevé possible (il est souvent souhaitable de recourir au verrouillage du protecteur). L'emploi de protections de commande ne peut être SEULEMENT envisagé que sur une machine où il n'y a AUCUNE POSSIBILITE pour un opérateur ou une partie de son corps de se trouver dans une zone à risque ou de l'atteindre lorsque le protecteur est fermé. La protection de commande doit être la seule voie d'accès à la zone à risque.

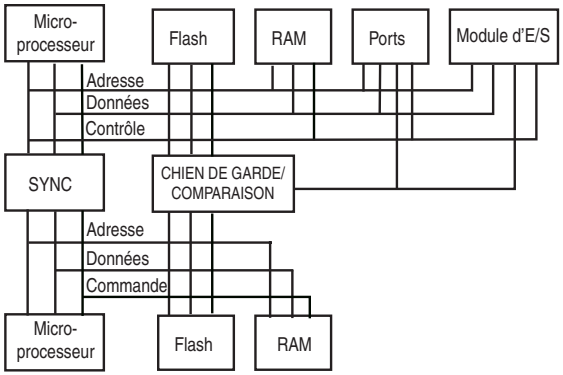
Commande logique programmable de sécurité

Le besoin d'applications de sécurité flexibles et évolutives a conduit à l'élaboration de PLC/automates de sécurité. Les automates de sécurité programmables fournissent aux utilisateurs le même niveau de flexibilité de commande dans une application de sécurité que celui auquel ils sont habitués avec les automates programmables standard. Cependant, il existe de grandes différences entre les PLC standard et de sécurité. Les PLC de sécurité existent pour différentes plates-formes afin de répondre aux impératifs d'évolutivité, d'intégration et fonctionnels des systèmes de sécurité les plus complexes.

Matériel

La redondance des UC, de la mémoire, des circuits d'E/S et des diagnostics internes présente sur les PLC de sécurité est une caractéristique qui n'est pas nécessaire sur les PLC standard. Un PLC de sécurité passe beaucoup plus de temps à effectuer des diagnostics internes sur la mémoire, les communications et les E/S. Ces opérations supplémentaires sont nécessaires pour obtenir la certification de sécurité requise. Cette redondance et ces diagnostics supplémentaires sont pris en charge par le système d'exploitation de l'automate, ce qui rend ces opérations transparentes pour le programmeur ; les PLC de sécurité se programment donc sensiblement comme les PLC standard.

Les microprocesseurs qui commandent ces dispositifs effectuent des diagnostics internes complets afin d'assurer les bonnes performances de la fonction de sécurité. La figure ci-dessous fournit un exemple de schéma fonctionnel d'un PLC de sécurité. Bien que les automates à base de microprocesseurs diffèrent légèrement d'une gamme à l'autres, des principes similaires sont mis en œuvre pour obtenir une classification de sécurité.



Architecture 1oo2D

Plusieurs microprocesseurs sont utilisés pour gérer les E/S, la mémoire et les communications de sécurité. Les circuits du chien de garde effectuent une analyse diagnostique. Ce type de construction est décrite ainsi : 1oo2D ; parce que un ou deux microprocesseurs peuvent prendre en charge la fonction de sécurité et que des diagnostics complets sont effectués afin de s'assurer que les deux microprocesseurs travaillent de façon synchronisée.

Chaque circuit d'entrée est également testé en interne de nombreuses fois chaque seconde pour vérifier qu'il fonctionne correctement. Même si le dispositif d'arrêt d'urgence n'est actionné qu'une fois par mois, le circuit est testé de façon continue, ce qui permet d'assurer que l'arrêt d'urgence sera détecté correctement dans le PLC de sécurité.

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

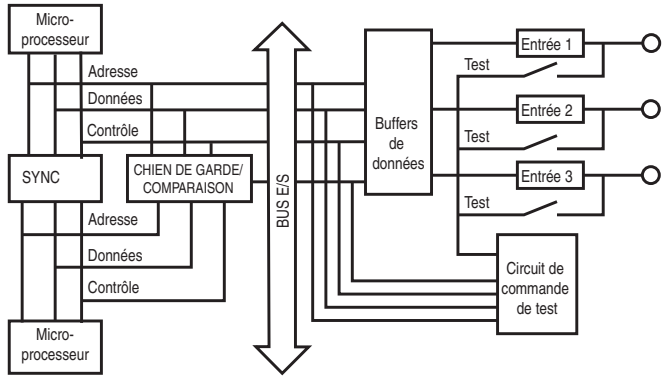


Schéma fonctionnel de module d'entrées de sécurité

Les sorties de PLC de sécurité sont des sorties statiques électromagnétiques ou de sécurité. Comme les circuits d'entrée, les circuits de sorties sont testés de nombreuses fois chaque seconde afin qu'ils peuvent désactiver la sortie. Si l'un des trois est défectueux, la sortie est désactivée par les deux autres, et la défaillance est signalée par le circuit de contrôle interne.

Lorsque des dispositifs de sécurité sont utilisés avec des contacts mécaniques (arrêts d'urgence, interrupteurs de barrière, etc.), l'utilisateur peut utiliser un test par impulsion pour détecter les défaillances multiples. Afin de ne pas utiliser des sorties de sécurité qui coûtent cher, de nombreux PLC de sécurité fournissent des sorties à impulsion spécifiques qui peuvent être connectées à des dispositifs à contact mécanique.

Logiciel

Les PLC de sécurité se programment de façon très semblable à celle des PLC standard. Tous les diagnostics supplémentaires et la vérification d'erreur mentionnés plus haut sont réalisés par le système d'exploitation, le programmeur n'a donc même pas conscience de ces opérations. La plupart des PLC de sécurité possèdent des instructions spéciales utilisées pour écrire le programme du système de sécurité, et ces instructions ressemblent à la fonction de leur équivalent dans le relais de sécurité. Par exemple, l'instruction d'arrêt d'urgence fonctionne de façon très semblable à un relais de surveillance de sécurité 127. Bien que la logique qui sous-tend chacune de ces instructions est complexe, les programmes de sécurité ont l'air relativement simples parce que le programmeur ne fait que relier ces blocs entre eux. Ces instructions, avec d'autres instructions logiques, mathématiques, de manipulation de données, etc. sont certifiées par un organisme tiers afin de s'assurer que leur fonctionnement est cohérent avec les normes en vigueur.

Les blocs fonctionnels constituent la méthode principale pour programmer les fonctions de sécurité. En plus des blocs fonctionnels et de la logique à relais, les PLC de sécurité fournissent également des instructions pour application de sécurité certifiées. Les instructions

de sécurité certifiées permettent un comportement particulier de l'application. Cet exemple montre une instruction d'arrêt d'urgence. Accomplir la même fonction avec la logique à relais nécessiterait environ 16 lignes de logique à relais. Puisque le comportement logique est intégré dans l'instruction d'arrêt d'urgence, la logique intégrée n'a pas besoin d'être testée.

Des blocs fonctionnels certifiés sont disponible pour dialoguer avec presque tous les dispositifs de sécurité. Une exception à cette liste est le bourrelet de sécurité qui utilise la technologie résistive.

Les PLC de sécurité génèrent une « signature » qui permet de voir si des modifications ont été apportées ou non. Cette signature est généralement une combinaison du programme, de la configuration des entrées/sorties et de l'horodatage. Lorsque le programme est finalisé et validé, l'utilisateur doit enregistré cette signature dans le cadre des résultats de la validation pour pouvoir s'y reporter plus tard. Si le programme doit être modifié, une nouvelle validation est nécessaire et une nouvelle signature doit être enregistrée. Le programme peut également être verrouillé avec un mot de passe afin d'empêcher les modifications non autorisées.

Avec les systèmes logiques programmables, le câblage est simplifié par rapport aux relais de surveillance de sécurité. Contrairement au câblage sur des bornes spécifiques des relais de surveillance de sécurité, les dispositifs d'entrées sont connectés à n'importe quelle borne d'entrée et les dispositifs de sorties sont connectés à n'importe quelle borne de sortie. Les bornes sont ensuite attribuée par le logiciel.

Automates à sécurité intégrée

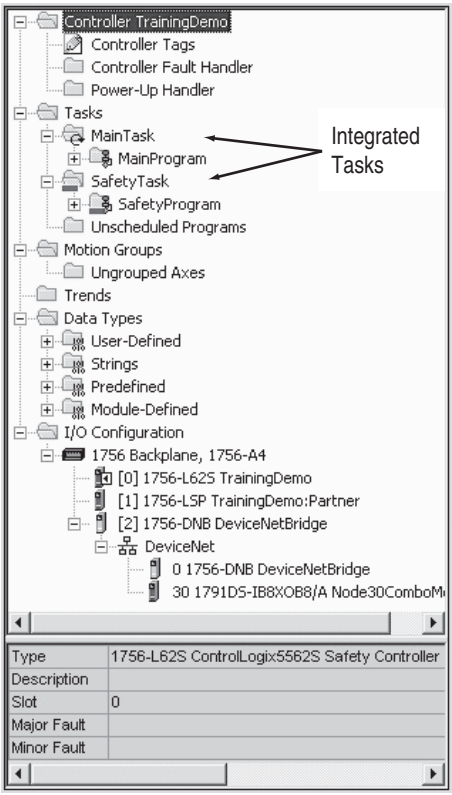
Les solutions de commande fournissent désormais une intégration totale avec une unique architecture de commande dans laquelle résident et collaborent les fonctions de commande de sécurité et standard. La capacité d'avoir la commande de mouvement, de variation de vitesse, de processus, de traitement par lots, séquentielle haute vitesse et de sécurité SIL3 dans un seul automate apporte des avantages significatifs. L'intégration des commandes de sécurité et standard permet d'utiliser des outils et des technologies courants, ce qui réduit les coûts de conception, d'installation, de mise en service et de maintenance. La possibilité d'utiliser du matériel de commande courant, des E/S ou des dispositifs de sécurité distribués sur les réseaux de sécurité et des dispositifs IHM courants, permet de réduire les coûts d'acquisition et de maintenance, ainsi que le temps de développement. Toutes ces fonctions améliorent la productivité, la vitesse de dépannage et réduisent les coûts de formation en raison de la standardisation.

Le schéma suivant donne un exemple d'intégration de la commande et de la sécurité. Les fonctions de commande standard, non liées à la sécurité, résident dans la tâche principale (Main Task). Les fonctions de sécurité résident dans la tâche de sécurité (Safety Task).

Toutes les fonctions standard et de sécurité sont isolées les unes des autres. Par exemple, les points de sécurité peuvent être directement lus par le programme logique standard. Les points de sécurité peuvent être échangés entre les automates GuardLogix sur EtherNet, ControlNet

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

ou DeviceNet. Les données de point de sécurité peuvent être directement lues par des dispositifs externes, des interfaces homme-machine (IHM), des ordinateurs personnels (PC) ou d'autres automates.



1. Les points standard et le programme logique se comportent de la même façon qu'avec ContrrolLogix.

2. Données de point standard, de programme ou d'automate et dispositifs externes, IHM, PC, autres automates, etc.

3. En tant qu'automate intégré, GuardLogix permet de déplacer (mapper) des données de point standard dans des points de sécurité pour une utilisation dans la tâche de sécurité. Ceci permet aux utilisateurs de lire les l'état à partir du côté standard de GuardLogix. Ces données ne doivent pas être utilisées pour commander directement une sortie de sécurité.

4. Les points de sécurité peuvent être lus directement par le programme logique standard.

5. Les points de sécurité peuvent être lus ou écrits par le programme logique de sécurité.

6. Les points de sécurité peuvent être échangés entre les automates GuardLogix sur EtherNet.

7. Les données de point de sécurité, de programme ou d'automate peuvent être lues par des dispositifs externes, des IHM, des PC, d'autres automates, etc. Remarque : une fois ces données lues, elles sont considérées comme des données standard, non comme des données de sécurité.

Réseaux de sécurité

Les réseaux de communication d'usine ont traditionnellement donné aux fabricants la possibilité d'améliorer la flexibilité, d'accroître les diagnostics, d'augmenter la distance, de réduire les coûts d'installation et de câblage, de faciliter la maintenance et plus généralement d'améliorer la productivité. Ces mêmes objectifs sont le moteur de la mise en œuvre des réseaux de sécurité industriels. Ces réseaux de sécurité permettent aux fabricants de répartir les E/S de sécurité et les dispositifs de sécurité autour de leurs machines à l'aide d'un unique

câble réseau, réduisant ainsi les coûts d'installation tout en améliorant les diagnostics et en permettant aux systèmes de sécurité d'augmenter la complexité. Ils autorisent également des communications sécurisées entre les PLC et les automates de sécurité, ce qui permet aux utilisateurs de répartir leur commande de sécurité entre plusieurs systèmes intelligents.

Les réseaux de sécurité n'empêchent pas les erreurs de communication de se produire. Ils sont plus capables de détecter les erreurs de transmission, puis de permettre aux dispositifs de sécurité à prendre les mesures appropriées. Les erreurs de communication détectées incluent : insertion de message, perte de message, corruption de message, retard de message, répétition de message et séquence de message incorrecte.

Pour la plupart des applications, lorsqu'une erreur est détectée, le dispositif passe à un état désactivé, généralement appelé « état de sécurité ». Le dispositif d'entrée ou de sortie de sécurité est responsable de la détection de ces erreurs de communication et du passage en état de sécurité le cas échéant.

Les premiers réseaux de sécurité étaient liés à un type de câble ou à un schéma d'accès câblé particuliers, les fabricants devaient donc utiliser du matériel spécifique (câbles, cartes d'interface réseau, routeurs, passerelles, etc.) qui faisait alors partie de la fonction de sécurité. Ces réseaux étaient limitées puisqu'ils ne prenaient en charge que les communications entre des dispositifs de sécurité. Ceci signifiait que les fabricants devaient utiliser plusieurs réseaux pour leur stratégie de commande des machines (un réseau pour la commande standard et un autre pour la commande de sécurité), ce qui augmentait les coûts d'installation, de formation et des pièces de rechange.

Les réseaux de sécurité modernes permettent à un seul câble réseau de communiquer avec des dispositifs de commande de sécurité et standard. CIP (Common Industrial Protocol) Safety est un protocole standard ouvert publié par l'ODVA (Open DeviceNet Vendors Association) qui permet les communications de sécurité entre dispositifs de sécurité sur les réseaux DeviceNet, ControlNet et EtherNet/IP. CIP Safety étant une extension du protocole CIP standard, les dispositifs de sécurité et standard peuvent tous résider sur le même réseau. Les utilisateurs établissent également des passerelles entre les réseaux contenant des dispositifs de sécurité, ce qui leur permet de subdiviser les dispositifs de sécurité pour affiner les temps de réponse de la sécurité, ou tout simplement pour faciliter la répartition des dispositifs de sécurité. Etant donné que le protocole de sécurité relève de la seule responsabilité des dispositifs finaux (PLC/automate de sécurité, module d'E/S de sécurité, composant de sécurité), des câbles, cartes d'interfaces réseau, passerelles et routeurs standard sont utilisés, ce qui élimine le matériel et les dispositifs réseau spécialisés de la fonction de sécurité.

Dispositifs de sorties

Relais de contrôle de sécurité et contacteurs de sécurité

Les relais de contrôle et les contacteurs sont utilisés pour couper l'alimentation de l'actionneur. Des fonctions spécialisées sont ajoutées aux relais de contrôle et aux contacteurs pour en faire des dispositifs de sécurité.

Les contacts normalement fermés à couplage mécanique sont utilisés pour renvoyer l'état des relais de contrôle et des contacteurs vers le dispositif logique. L'utilisation des contacts à couplage mécanique permet d'assurer la fonction de sécurité. Pour être conforme aux exigences des contacts à couplage mécanique, les contacts normalement fermés et normalement ouverts ne peuvent pas être en position fermée en même temps. La norme CEI 60947-5-1 définit les critères pour les contacts à couplage mécanique. Si les contacts normalement ouverts devaient se souder, les contacts normalement fermés restent ouverts d'au moins 0,5 mm. Réciproquement, si les contacts normalement fermés devaient se souder, les contacts normalement ouverts restent ouverts.

Les systèmes de sécurité ne doivent être démarrés qu'à des emplacements spécifiques. L'armature des relais de contrôle et contacteurs standard peut être enfoncée pour fermer les contacts normalement ouverts. Sur les dispositifs de sécurité, l'armature est protégée contre le contournement manuel afin de limiter les démarrage imprévus.

Sur les relais de contrôle de sécurité, le contact normalement fermé est commandé par la clé à-boulon principale. Les contacteurs de sécurité utilisent un bloc de contacts supplémentaire pour localiser les contacts à couplage mécanique. Si le bloc de contacts tombe de la base, les contacts à couplage mécanique restent fermés. Les contacts à couplage mécanique sont fixés de façon permanente au relais de contrôle de sécurité ou au contacteur de sécurité.

Sur les plus gros contacteurs, un bloc de contacts supplémentaire n'est pas suffisant pour refléter de façon précise l'état de la clé à boulon plus large. Les contacts miroir, illustrés sur la figure 4.81, sont situés sur les côtés du contacteur utilisé.

La durée de déclenchement des relais de contrôle ou des contacteurs joue un rôle dans le calcul de la distance de sécurité. Un suppresseur de surtension est souvent placé sur la bobine pour améliorer la durée de vie des contacts qui commandent la bobine. Pour les bobines c.a., la durée de déclenchement n'est pas affectée. Pour les bobines c.c., la durée de déclenchement est augmentée. L'augmentation dépend du type de suppression sélectionnée.

Les relais de contrôle et les contacteurs sont conçus pour basculer de fortes charges, de 0,5 A à plus de 100 A. Le système de sécurité fonctionne avec des courants faibles. Le signal de retour généré par le dispositif logique du système de sécurité peut être de quelques milli-ampères jusqu'à des dizaines de milliampères, généralement à 24 V c.c. Les relais de contrôle et les contacteurs de sécurité utilisent des contacts jumelés plaqués or pour commuter de façon fiable ce faible courant.

Protection contre les surcharges

Une protection contre les surcharges moteur est imposée par les normes électriques. Les diagnostics fournis par le dispositif de protection contre les surcharges améliorent non seulement la sécurité de l'équipement, mais également la sécurité de l'opérateur. Les technologies disponibles actuellement peuvent détecter les conditions d'erreur, comme la surcharge, la perte de phase, le défaut de mise à la terre, le rotor bloqué, le blocage, la sous-charge, le courant asymétrique et la surchauffe. La détection et la communication de conditions anormales avant le déclenchement permet d'améliorer le temps de disponibilité pour la production et de protéger les opérateurs et le personnel de maintenance de situations dangereuse imprévues.

Variateurs et servo-variateurs

Les variateurs et servo-variateurs de sécurité peuvent être utilisés pour empêcher une énergie de rotation d'être transmise afin d'obtenir un arrêt sécurisé, ainsi qu'un arrêt d'urgence.

Les variateurs c.a. obtiennent la classification de sécurité avec des voies redondantes pour couper l'alimentation du circuit de commande de la barrière de protection. Une voie est le signal de validation ; un signal matériel qui supprime le signal d'entrée vers le circuit de commande de la barrière. La deuxième voie est celle d'un relais guidé réciproquement qui coupe l'alimentation du circuit de commande de la barrière de protection. Le relais guidé réciproquement fournit également un signal d'état au système logique. Cette approche redondante permet au variateur de sécurité d'être utilisé dans les circuits d'arrêt d'urgence sans avoir besoin d'un contacteur.

Le servo-variateur obtient un résultat d'une façon similaire aux variateurs c.a. qui utilisent les signaux de sécurité redondants utilisés pour la fonction de sécurité. Un signal interrompt le variateur vers le circuit de commande de la barrière. Un deuxième signal interrompt l'alimentation du circuit de commande de la barrière. Deux relais guidés réciproquement sont utilisés pour supprimer les signaux et pour fournir un retour au dispositif logique de sécurité.

Systèmes de raccordement

Les systèmes de raccordement apportent une valeur ajoutée en réduisant les coûts d'installation et de maintenance des systèmes de sécurité. La conception doit prendre en compte les considérations de voie unique, double voie, double voie avec indication et multiples types de dispositifs.

Lorsqu'un montage en série d'interrupteurs à deux voies est nécessaire, un boîtier de distribution peut simplifier l'installation. Avec leur classification IP67, ces types de boîtiers peuvent être montés sur la machine dans des sites distants. Lorsque différents dispositifs sont nécessaires, un boîtier d'E/S Guard I/O ArmorBlock peut être utilisé. Les entrées peuvent être configurées avec le logiciel pour accepter différents types de dispositifs.

Calcul de la distance de sécurité

Les sources de danger doivent être en état de sécurité avant que l'opérateur puisse pénétrer dans la zone de danger. Pour le calcul de la distance de sécurité, il existe deux groupes de normes. Dans ce chapitre, ces normes sont regroupées ainsi :

ISO EN : (ISO 13855 et EN 999)

US CAN (ANSI B11.19, ANSI RIA R15.06 et CAN/CSA Z434-03)

Formule

La distance de sécurité minimale dépend du temps requis pour traiter la commande d'arrêt et sur quelle distance l'opérateur peut pénétrer dans la zone de détection avant d'être détecté. La formule utilisée dans le monte entier a la même forme est les mêmes critères. Les différences sont les symboles utilisés pour représenter les variables et les unités de mesure.

Les formules sont les suivantes :

ISO EN : $S = K \times T + C$

US CAN : $Ds = K \times (Ts + Tc + Tr + Tbm) + Dpf$

Où : Ds et S sont la distance de sécurité minimale entre la zone de danger et le point de détection le plus proche.

Angle d'approche

Pour le calcul de la distance de sécurité lorsqu'une barrière immatérielle ou un scrutateur de zone est utilisé, l'angle d'approche vers le dispositif de détection doit être pris en considération. Trois angles d'approche sont prises en considération :

Normale – approche perpendiculaire au plan de détection ;

Horizontale – approche parallèle au plan de détection ;

Suivant un angle – approche à un certain angle de la zone de détection.

Constante de vitesse

K est la constante de vitesse. La valeur de la constante de vitesse dépend des mouvements de l'opérateur (c'est-à-dire le mouvement des mains, la vitesse de déplacement et la longueur des pas). Ce paramètre est basé sur des recherches qui montrent que l'on peut raisonnablement considérer une vitesse de 1 600 mm/s (63 in/s) pour le déplacement des mains d'un opérateur lorsque son corps est stationnaire. Les conditions réelles d'application sont toutefois à prendre en compte. En règle générale, la vitesse d'approche varie entre 1 600 mm/s (63 in/s) et 2 500 mm/s (100 in/s). La constante de vitesse appropriée doit être déterminée par l'évaluation du risque.

Délai d'arrêt

T est le temps nécessaire pour arrêter le système. La durée totale, en secondes, commence au moment où le signal d'arrêt est initié jusqu'à la fin du danger. Cette durée peut être divisée selon ses différentes composantes (Ts, Tc, Tr et Tbm) pour faciliter l'analyse. Ts est le temps le plus long pour arrêter la machine/équipement Tc est le temps le plus long pour arrêter le système de commande Tr est le temps de réponse du dispositif de protection, notamment son interface. Tbm est le temps d'arrêt supplémentaire autorisé par le contrôleur de freinage avant de détecter une détérioration du temps d'arrêt qui dépasse les limites prédéfinies par l'utilisateur. Tbm est utilisé avec des presses mécaniques rotatives. Ts + Tc + Tr sont généralement mesurés par un dispositif de mesure du temps d'arrêt si les valeurs sont inconnues.

Facteurs de pénétration

Le facteur de pénétration est représenté par les symboles C et Dpf. Il s'agit de la distance de déplacement maximale vers la source de danger avant la détection par le dispositif de protection. Le facteur de pénétration change selon le type de dispositif et d'application. La norme appropriée doit être vérifiée afin de déterminer quel est le meilleur facteur de pénétration. Pour une approche normale d'une barrière immatérielle ou d'un scrutateur de zone, dont la sensibilité de détection est inférieure à 64 mm (2,5 in), les normes ANSI et canadiennes utilisent :

Dpf = 3,4 x (Sensibilité de détection – 6,875 mm), mais pas moins de 0.

Pour une approche normale d'une barrière immatérielle ou d'un scrutateur de zone, dont la sensibilité de détection est inférieure à 40 mm (1,57 in), les normes ISO et EN utilisent :

C = 8 x (sensibilité de détection – 14 mm), mais pas moins de 0.

Ces deux formules ont un point d'intersection de 19,3 mm. Pour la détection d'objets inférieurs à 19 mm, l'approche US CAN est plus restrictive ; en effet, la barrière immatérielle ou le scrutateur de zone doit être placé plus loin de la source de danger. Pour la détection d'objets supérieurs à 19,3 mm, la norme ISO EN est plus restrictive. Les fabricants de machines qui construisent des machines destinées au marché international doivent utiliser le cas le plus défavorable des deux équations.

Applications à pénétration traversante

Pour la détection de plus grands objets, les normes US CAN et ISO EN diffèrent légèrement en ce qui concerne le facteur de pénétration et la sensibilité aux objets. La figure 5.2 résume ces différences. La valeur ISO EN est de 850 mm alors que la valeur US CAN est de 900 mm. Les normes diffèrent également par leur sensibilité aux objets. Alors que la norme ISO EN permet 40 à 70 mm, la norme US CAN permet jusqu'à 600 mm.

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

Applications à pénétration par dessus

Les deux normes prescrivent que la hauteur minimale du faisceau le plus bas doit être de 300 mm, mais elles diffèrent en ce qui concerne la hauteur minimale du faisceau le plus haut. La norme ISO EN stipule 900 mm, alors que la norme US CAN impose 1 200 mm. La valeur pour le faisceau le plus haut semble être purement théorique. Si l'on considère qu'il s'agit d'une application à pénétration traversante, la hauteur du faisceau le plus haut doit être bien supérieure pour le cas d'un opérateur se tenant debout. Si l'opérateur peut passer par dessus le plan de détection, le critère de pénétration par dessus s'applique.

Un ou plusieurs faisceaux

Les faisceaux unique ou multiples sont définis plus précisément par les normes ISO EN. La figure ci-après montre les hauteurs « pratiques » des faisceaux multiples par rapport au sol. La pénétration est de 850 mm dans la plupart des cas et 1 200 mm pour l'utilisation du faisceau unique. En comparaison, l'approche US CAN prend cela en considération à travers les critères de la pénétration traversante. La pénétration par dessus, en dessous ou par le côté d'un ou plusieurs faisceaux doit toujours être prise en considération.

Nombre de faisceaux	Hauteur par rapport au sol (mm)	C (mm)
1	750	1 200
2	400, 900	850
3	300, 700, 1 100	850
4	300, 600, 900, 1 200	850

Calcul de la distance

Dans le cas d'une approche normale d'une barrière immatérielle, le calcul de la distance de sécurité pour les normes ISO EN et US CAN est proche, mais il existe des différences. Dans le cas d'une approche normale d'une barrière immatérielle verticale pour laquelle la détection d'objets est au maximum de 40 m, l'approche ISO EN requiert deux étapes. Il faut d'abord calculer S en utilisant 2 000 comme constante de vitesse.

S = 2 000 x T + 8 x (d -1 4)

La distance minimale de S est 100 mm.

Une deuxième étape peut être utilisée lorsque la distance est supérieure à 500 mm. Dans ce cas, la valeur de K peut être réduite à 1 600. Avec K = 1 600, la valeur minimale de S est 500 mm.

La norme US CAN utilise une approche à une seule étape : Ds = 1 600 x T * Dpf

Ceci conduit à des différences supérieures à 5 % entre les normes, lorsque le temps de réponse est inférieur à 560 ms.

Approche selon un angle

La plupart des installations qui utilisent des barrières immatérielles et scrutateurs sont montées verticalement (approche normale) ou horizontalement (approche en parallèle). Ces installations ne sont pas considérées comme ayant un angle si elles sont à ±5° de la configuration prévue à la conception. Lorsque l'angle est supérieur à ±5°, les risques potentiels (p. ex., distance plus courte) posés par les différentes approches prévisibles doivent être pris en considération. En général, des angles supérieurs à 30° par rapport au plan de référence (p. ex. le sol) doivent être considérés comme normaux et les angles inférieurs à 30 doivent être considérés comme parallèles.

Tapis de sécurité

Avec les tapis de sécurité, la distance de sécurité doit prendre en considération la vitesse de déplacement et la foulée des opérateurs. Etant entendu que l'opérateur se déplace et que le tapis de sécurité est fixé au sol, le premier pas de l'opérateur sur le tapis est un facteur de pénétration de 1 200 mm (48 in). Si l'opérateur doit monter sur la plate-forme, le facteur de pénétration peut être réduit d'un facteur de 40 % de la hauteur de la marche.

Exemple

Exemple : Un opérateur approche normalement d'une barrière immatérielle de 14 mm, qui est connectée à un relais de surveillance de sécurité, lui-même raccordé à un contacteur d'alimentation c.c. avec atténuateur à diode. Le temps de réponse du système de sécurité (Tr) est 20 + 15 + 95 = 130 ms. Le délai d'arrêt de la machine (Ts+Tc) est 170 ms. Aucun contrôleur de freinage n'est utilisé. La valeur Dpf est 2,54 cm (1 in) et la valeur C est 0. Le calcul est le suivant :

Dpf = 3,4 (14 – 6,875) = 24,2 mm (1 in)

Ds = K x (Ts + Tc + Tr + Tbm) + Dpf
Ds = 63 x (0,17 + 0,13 + 0) + 1
Ds = 63 x (0,3) + 1
Ds = 18,9 + 1
Ds = 505 mm (19,9 in)

C = 8 (14-14) = 0

S = K x T + C
S = 1 600 x (0,3) + 0
S = 480 mm (18,9 in)

Par conséquent, la distance de sécurité minimale à laquelle la barrière immatérielle doit être montée par rapport à la source de danger est de 508 mm (20 in) ; pour pouvoir utiliser la machine n'importe où dans le monde.

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

Prévention de mise sous tension imprévue

La prévention des mises sous tension imprévues est abordée dans de nombreuses normes. Par exemple, ISO 14118, EN 1037, ISO 12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 et AS 4024.1603. Ces normes ont une approche commune : la principale méthode pour empêcher les mises sous tension imprévues est de retirer l'alimentation du système et de le verrouiller en mode désactivé. L'objectif est de permettre aux personnes de pénétrer en toute sécurité dans les zones de danger de la machine.

Condamnation/signalisation

Les nouvelles machines doivent être construites avec des dispositifs d'isolation de l'énergie verrouillables. Ces dispositifs servent à tous les types d'énergie, notamment électrique, hydraulique, pneumatique, pesanteur et lasers. La condamnation signifie utiliser un verrou à un dispositif d'isolation de l'énergie. Le verrou ne doit être retiré que par son propriétaire ou par un superviseur dans des conditions contrôlées. Si plusieurs personnes doivent travailler sur la machine, chaque personne doit apposer son verrou sur le dispositif d'isolation de l'énergie. Le propriétaire de chaque verrou doit pouvoir être identifié.

Aux Etats-Unis, la signalisation (tagout) est une alternative à la condamnation (lockout) pour les machines plus anciennes sur lesquelles un dispositif de verrouillage n'a jamais été installé. Dans ce cas, la machine est arrêtée et une étiquette est apposée pour prévenir le personnel de ne pas démarrer la machine pendant que la personne qui a apposé l'étiquette travaille sur la machine. Depuis 1990, les machines qui sont modifiées doivent être modernisées et inclure un dispositif d'isolation de l'énergie verrouillable.

Un dispositif d'isolation de l'énergie est un dispositif mécanique qui empêche physiquement la transmission ou la libération d'énergie. Ce dispositif peut être un disjoncteur, un interrupteur sectionneur, un interrupteur manuel, une combinaison prise/fiche ou un clapet manuel. Les dispositifs d'isolation électriques doivent commuter tous les conducteurs d'alimentation non mis à la terre et aucun pôle ne doit fonctionner indépendamment.

L'objectif de la condamnation et de la signalisation est d'empêcher le démarrage imprévu de la machine. Un démarrage imprévu peut avoir différentes causes : défaillance du système de commande ; action inappropriée d'une commande de démarrage, d'un capteur, d'un contacteur ou d'une vanne ; restauration de l'alimentation après une interruption ; ou autres causes internes ou externes. Après la fin du processus de condamnation ou de signalisation, la dissipation d'énergie doit être vérifiée.

Systèmes d'isolation de sécurité

Les systèmes d'isolation de sécurité exécutent un arrêt automatique sans perte de données d'une machine et fournissent également une méthode facile pour condamner l'alimentation d'une machine. Cette approche fonctionne bien pour les machines de taille importante et les systèmes de fabrication, particulièrement lorsque plusieurs sources d'énergie sont situées à l'entresol ou dans un site distant.

Rupteurs de charge

Pour l'isolation locale de dispositifs électriques, des interrupteurs peuvent être placés juste en amont du dispositif qui doit être isolé et condamné. Les interrupteurs de charge Série 194E sont un exemple de produit capable d'isolation et de condamnation.

Systèmes à clé captive

Les systèmes à clé captive sont une autre méthode pour mettre en œuvre un système de condamnation. De nombreux systèmes à clé captive commencent pas un dispositif d'isolation de l'énergie. Lorsque l'interrupteur est désactivé par la clé « principale », l'alimentation électrique de la machine est coupée simultanément de tous les conducteurs d'alimentation non mis à la terre. La clé principale peut alors être retirée et déplacée dans un endroit où il est nécessaire d'accéder à la machine. La figure 6.4 montre un exemple du système de base, un interrupteur d'isolement et un verrou d'accès. Divers composants peuvent être ajoutés pour répondre à des besoins de condamnation plus complexes.

Mesures alternatives à la condamnation

La condamnation et la signalisation doivent être utilisées pour l'entretien et la maintenance des machines. Les interventions sur les machines pendant les opérations normales de production sont couvertes par les mesures de protection. La différence entre l'entretien/la maintenance et les opérations normales de production n'est pas toujours claire.

Certains réglages mineurs et certaines tâches d'entretien courant, effectués pendant les opérations normales de production, ne nécessitent pas forcément un verrouillage de la machine. Par exemple, le chargement et le déchargement de matériaux, changements et réglages mineurs d'outils, lubrification et retrait des déchets. Ces tâches doivent être routinières, répétées et faire partie intégrante de l'utilisation de l'équipement dans le cadre de la production, et le travail doit être réalisé à l'aide de mesures alternatives, comme des dispositifs de protection, qui fournissent une protection efficace. Les dispositifs de protection incluent des dispositifs comme les barrières munies d'interrupteurs de sécurité, les barrières immatérielles et les tapis de sécurité. Lorsqu'ils sont utilisés avec un programme de sécurité et les dispositifs de sorties appropriés, les opérateurs peuvent accéder en toute sécurité aux zones de danger de la machine pendant le fonctionnement normal et les opérations d'entretien mineures.

Structure des systèmes de commande de sécurité

Introduction

Qu'est-ce qu'un système de commande de sécurité (souvent abrégé en anglais par SRCS) ? 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).

Les systèmes de commande de sécurité sont conçus pour exécuter des fonctions de sécurité. Le système doit continuer à fonctionner correctement dans toutes les situations prévisibles. Qu'est-ce qu'une fonction de sécurité, comment concevoir un système de sécurité et lorsque c'est fait, comment le montrer ?

Fonction de sécurité

Une fonction de sécurité est mise en œuvre par les dispositifs de sécurité du système de commande de la machine afin de maintenir l'équipement dans un état sécurisé par rapport à un danger spécifique. Un défaillance de la fonction de sécurité peut entraîner une augmentation immédiate des risques, c'est-à-dire d'une situation dangereuse.

Une machine doit présenter au moins un « danger » potentiel, autrement ce n'est pas une machine. On parle de « situation dangereuse » lorsqu'une personne est exposée à un danger. Une situation dangereuse n'implique pas que la personne est blessée. La personne exposée peut être consciente du danger et éviter des blessures. La personne exposée peut ne pas être consciente du danger, ou le danger peut être initié par un démarrage imprévu. La tâche principale du concepteur du système de sécurité est de prévenir situations dangereuses et d'empêcher les démarrages imprévus.

La fonction de sécurité peut souvent être décrite par des critères multi-parties. Par exemple, la fonction de sécurité initiée par une barrière munie d'interrupteurs de sécurité a trois parties :

1. la source du danger protégée par la barrière de protection ne peut fonctionner tant que la barrière n'est pas fermée ;

2. l'ouverture de la barrière entraîne l'arrêt de la source de danger si elle fonctionne au moment de l'ouverture ; et

3. la fermeture de la barrière ne redémarre pas la source de danger protégée par la barrière.

Lors de l'explicitation d'une fonction de sécurité pour une application spécifique, le mot « danger » doit être changé et remplacé par la source de danger spécifique. La source de danger ne doit pas être confondue avec les conséquences du danger. L'écrasement, les coupures et les brûlures sont des conséquences du danger. Exemples de source de danger : moteur, vérin, couteau, torche, pompe, laser, robot, effecteur terminal, électro-aimant, clapet, autre type d'actionneur ou danger mécanique impliquant la pesanteur.

Lorsque l'on parle de systèmes de sécurité, l'expression « au moment ou avant un appel de la fonction de sécurité » est utilisée. Qu'est-ce qu'un appel de la fonction de sécurité ? Il s'agit par exemple de l'ouverture d'une barrière munie d'interrupteurs de sécurité, l'interruption d'une barrière immatérielle, le fait de marcher sur un tapis de sécurité ou de l'appui sur un arrêt d'urgence. L'opérateur demande que la source de danger s'arrête ou reste désactivée si elle est déjà arrêtée.

La fonction de sécurité est exécutée par les dispositifs de sécurité du système de commande de la machine. Elle n'est pas exécutée par un seul dispositif, par exemple uniquement par la barrière. Le dispositif de verrouillage sur la barrière envoie une commande à un dispositif logique, qui à son tour désactive un actionneur. La fonctions de sécurité commence avec la commande et se termine par son exécution.

Le système de sécurité doit être conçu avec un niveau d'intégrité correspondant aux risques de la machine. Plus les risques sont importants, plus les niveaux d'intégrité doivent être élevés pour assurer l'efficacité de la fonction de sécurité. Les systèmes de sécurité des machines peuvent être classés en fonction du type de conception et de la capacité à assurer l'efficacité de la fonction de sécurité.

Catégories de systèmes de commande

La présentation suivante des catégories est basée sur la norme ISO 13849-1:1999, qui est équivalente à la norme EN 954-1:1996. En 2006, la norme ISO 13849-1 a été révisée de façon significative afin de l'harmoniser avec les normes CEI 62061 et CEI 61508, qui sont toutes deux utilisées en priorité pour les systèmes de sécurité complexes. La version 2006 de la norme ISO 13849-1 continue d'utiliser les catégories de performance de la sécurité ; ces catégories sont considérées comme la « structure » ou l'« architecture » des systèmes de commande de sécurité. Des informations complémentaires portant sur les composants et la conception du système complètent cette « structure » afin de fournir une classification de « niveau de performance ». La présentation des catégories faite ici s'appuie sur les révisions de 1999 et de 2006 de la norme ISO 13849-1.

La norme ISO 13849-1 « Parties des systèmes de commande relatives à la sécurité – Partie 1 : Principes généraux de conception » définit une « langue » de cinq catégories pour tester et décrire les performances des systèmes de commande de sécurité.

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

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

Remarque 2 : une série de plusieurs pannes dues à une cause d'origine 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 ? Le choix de la catégorie découle du processus d'évaluation du risque. 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.

La redondance, la diversité et la surveillance sont les clés de ces catégories. La redondance est la duplication de la même technique. La diversité consiste à utiliser deux techniques différentes. La surveillance consiste à vérifier l'état des dispositifs, puis à déclencher les actions appropriées en fonction de l'état. La méthode habituelle, mais pas la seule, pour la surveillance consiste à dupliquer les fonctions essentielles à la sécurité et de comparer le fonctionnement.

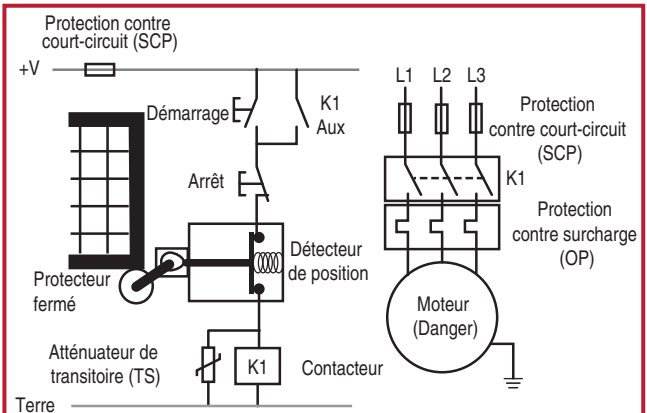
Résumé des prescriptions	Comportement du système
CATEGORIE B (voir remarque 1) Les parties des systèmes de commande relatives à la sécurité et leur équipement de protection, ainsi que leurs composants, doivent être conçus en conformité avec les normes en vigueur afin de pouvoir résister aux influences prévues. Les principes de base de la sécurité doivent être appliqués.	Toute panne risque de conduire à la perte de la fonction de sécurité.
CATEGORIE 1 Les prescriptions de la catégorie B s'appliquent avec utilisation de principes et de composants de sécurité dûment éprouvés.	Comme décrit pour la catégorie B mais avec une fiabilité plus élevée de la fonction de sécurité. (Plus la fiabilité est élevée, plus la probabilité de panne est faible.)
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.
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. Lorsque c'est possible, une seule panne doit être détectée.	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'une seule panne de n'importe lequel de ses composants n'entraîne pas la perte de la fonction de sécurité. Cette panne unique doit être détectée au moment de l'appel de la fonction de sécurité ou avant l'appel suivant. 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 pannes multiples. Les défauts sont détectés à temps pour prévenir la perte des fonctions de sécurité.

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

Catégorie B

La catégorie B prescrit les critères de base pour tout système de commande ; qu'il s'agisse d'un système de commande de sécurité ou non. Un système de commande doit fonctionner dans l'environnement prévu. Le concept de fiabilité fournit une base pour les systèmes de commande puisque la fiabilité est définie comme la probabilité qu'un dispositif exécute la fonction pour laquelle il a été conçu pendant une durée spécifique dans certaines conditions définies. Bien qu'ayant un système conforme aux objectifs de fiabilité, nous savons qu'il sera défaillant tôt ou tard. Le concepteur du système de sécurité doit savoir si la défaillance du système se produira avec présence d'un danger ou dans un état sécurisé. Le mantra est le suivant : « Comment le système se comporte-t-il en présence de pannes ? ». En commençant par ce concept, quels sont les principes qui doivent être observés pour guider la conception du système ? La catégorie B nécessite la mise en application de principes de sécurité de base. La norme ISO 13849-2 définit les principes de sécurité de base des systèmes électriques, pneumatiques, hydrauliques et mécaniques. Les principes électriques sont résumés ainsi :

- Sélection, combinaison, dispositions, assemblage et installation appropriés (c'est-à-dire, selon les directives du fabricant)
- Compatibilité des composants avec les tension et les intensités
- Résistance aux conditions ambiantes
- Utilisation du principe de mise hors tension
- Suppression des transitoires
- Réduction du temps de réponse
- Protection contre les démarrages imprévus
- Fixation sécurisée des capteurs (p. ex., montage de dispositifs de verrouillage)
- Protection du circuit de commande (selon NFPA79 & IEC 60204-1)
- Liaison de protection correcte

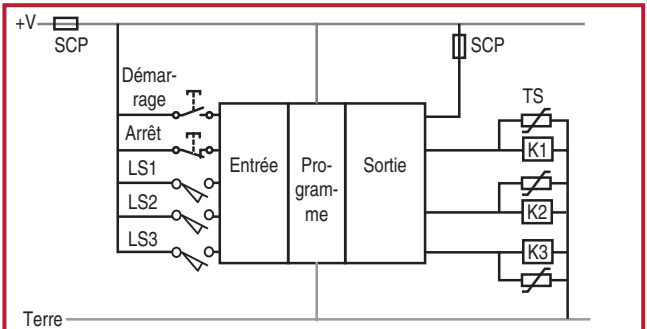


Système de catégorie B simple

Le schéma présente un système de catégorie B. La barrière est verrouillé par un détecteur de position en mode négatif (à ressort). Une protection contre les courts-circuits et les surcharges est fournie pour la conformité aux exigences des normes électriques sur la protection contre les courts-circuits. La suppression des transitoires est utilisée

pour aider à empêcher le soudage des contacts lorsque la bobine du contacteur est hors tension. Si le principe de mise hors tension est utilisé, le dispositif de verrouillage de la protection arrête le moteur. Les composants doivent être sélectionnés et installés en fonction des conditions ambiantes prévisibles, ainsi que des exigences de tension et d'intensité. A noter qu'aucune mesure spéciale de sécurité n'est appliquée dans le cadre de la catégorie B, des mesures complémentaires peuvent donc être nécessaires.

Appuyez sur le bouton de démarrage avec la barrière de protection fermée afin de mettre le moteur sous tension, ce qui symbolise le danger. Lorsque le contacteur K1 se ferme, un contact auxiliaire maintient le circuit et le bouton de démarrage peut être relâché. Appuyez sur le bouton d'arrêt ou ouvrez la barrière de protection pour arrêter le moteur. Relâchez le bouton d'arrêt ou fermer la barrière de protection ne fait pas redémarrer le moteur.



Système de catégorie B complexe

Le schéma présente un système complexe de catégorie B. Ici plusieurs capteurs (détecteurs de position) et boutons-poussoirs sont connectés au module d'entrées d'un automate programmable (PLC). Plusieurs actionneurs sont connectés au module de sorties. Un module logique, utilisant un logiciel détermine quelles sorties activées ou désactivées en réponse à l'état des capteurs.

Comment savoir si ces circuits sont conformes à la catégorie B ? Tout d'abord, le concepteur doit faire sa sélection, son installation et son assemblage en respectant les directives du fabricant. Ces dispositifs doivent fonctionner dans les limites des tensions et intensités nominales prévues. Les conditions ambiantes prévisibles, comme la compatibilité électromagnétique, la résistance aux vibrations, la tenue aux chocs, la résistance aux contaminations et aux projections, doivent également être prises en considération. Le principe de mise hors tension est utilisé, La protection contre les transitoires est installée sur les bobines du contacteur. Le moteur est protégé contre les surcharges. Le câblage et la mise à la terre sont conformes aux normes électriques appropriées.

L'étape suivante de l'analyse de sécurité consiste à décomposer le système en ses principaux constituants, puis à examiner leurs modes de défaillance potentielle. Dans un chapitre précédent, nous avons décomposé le système en trois blocs, ENTREES – LOGIQUE – SORTIES. Lorsque l'on aborde les performances du système de sécurité, le câblage doit également être inclus dans l'analyse.

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

Dans les exemples de la catégorie B, les composants sont :

- Dispositif de verrouillage (détecteur de position)
- Automate programmable
- Contacteur
- Câblage

Interrupteur de sécurité

Le détecteur de position est un dispositif mécanique. Sa tâche est simple : ouvrir les contacts lorsqu'une barrière de protection est ouverte. Il y a de nombreux années, les détecteurs de position étaient utilisés de cette façon. Mais sa conception présente des inconvénients qui vont à l'encontre d'un meilleur fonctionnement de la sécurité. Les normes électriques imposent l'utilisation de dispositifs de protection contre les courts-circuits (p. ex., fusibles ou disjoncteurs) pour les circuits de dérivation. Cette protection peut être insuffisante pour éviter le soudage d'un contact dans le détecteur de position. Les contacts du détecteur de position sont conçus pour s'ouvrir sous l'action d'un ressort. Malheureusement, la force de rappel du ressort n'est pas toujours suffisante pour compenser la résistance d'un contact soudé. Un autre point à considérer est le ressort lui-même. La flexion répétée peut finir par entraîner une rupture et la force exercée sur les contacts peut pas être insuffisante pour ouvrir le circuit. D'autres pannes internes dans la tête de l'opérateur ou la liaison peuvent également avoir pour conséquence le maintien fermé du contact lorsque la barrière est ouverte. Une autre considération importante est le contournement. Lorsque la barrière est ouverte, le détecteur de position est facile à contourner en poussant le levier en position activée et en le maintenant en place par du ruban adhésif, du fil ou tout autre outil simple.

Automate programmable

Les PLC constituent le système de commande privilégié pour les machines. Les dispositifs d'entrée, comme le dispositif de verrouillage du détecteur de position, sont connectés aux modules d'entrées. Les dispositifs de sortie, comme les contacteurs, sont connectés aux modules de sorties. Le dispositif logique assigne les dispositifs d'entrée aux dispositifs de sortie appropriés selon les conditions logiques.

Bien que la fiabilité des PLC s'est considérablement améliorée depuis leur introduction, ils finissent par s'user et par tomber en panne. Le concepteur du système de sécurité doit avoir connaissance des machines de la défaillance et si ces défaillances entraînent une situation de danger. Les PLC présentent deux catégories principales de défaillance : matérielle et logicielle. Les défaillances matérielles peuvent être internes, dans les modules d'entrées, logique ou de sorties. Lors de ces défaillances, les sorties peuvent rester activées, même si une commande d'arrêt a été initiée. Les défaillances logicielles dans le programme d'application ou dans le firmware peuvent également laisser les sorties activées, même si une commande d'arrêt a été initiée.

Contacteur

Les contacteurs activent les actionneurs de la machine, soit les moteurs, les électro-aimants, les éléments chauffant et autres types d'actionneurs. Les actionneurs utilisent des intensités élevées, et certains ont des surintensité pouvant être 10 fois supérieures à leur régime permanent. Les contacts des contacteurs devraient toujours être rotégés contre les surcharges et les courts-circuits afin d'éviter le soudage. Même avec cette protection, il existe un risque que les contacts de commutation de puissance restent fermés. Ceci peut être dû au soudage ou à une armature bloquée. Lorsqu'un défaut de ce type se produit, le bouton d'arrêt devient inefficace et la machine doit être mise hors tension par le coupe-circuit principal. Les contacteurs doivent être inspectés régulièrement pour détecter les connexions desserrées pouvant provoquer une surchauffe et une déformation. Le contacteur doit être conforme aux normes pertinentes qui prescrivent les caractéristiques et les conditions d'utilisation. Les normes CEI 60947-4-1 et CEI 60947-5-1 décrivent en détail les tests que les contacteurs doivent réussir pour être utilisés dans différentes applications.

Câblage

Bien qu'une conception et une installation conformes aux normes électriques appropriées réduisent les risques de défaillance du câblage, les pannes de câblage peuvent se produire et cela se produit régulièrement. Les défaillances de câblage à prendre en considération incluent les courts-circuits et les circuits ouverts. L'analyse des courts-circuits doit inclure les courts-circuits sur l'alimentation, sur la mise à la terre ou sur d'autres circuits, qui peuvent créer une situation dangereuse.

Commutateurs de démarrage et d'arrêt

Il faut également prendre en considération les commutateurs de démarrage et d'arrêt. Si le bouton de démarrage est en court-circuit, la machine redémarre de façon inopinée lorsque le bouton d'arrêt est relâché ou lorsque la barrière de protection est fermée. Heureusement, la barrière doit être fermée pour pouvoir démarrer le moteur. Si la barrière est fermée, l'accès à la source de danger est normalement protégé. Si le bouton d'arrêt est défectueux ou si ses contacts sont en court-circuit, la commande d'arrêt est bloquée et ne peut être exécutée. Là encore, si la barrière est fermée, l'accès à la source de danger est normalement protégé.

Les dispositifs de sécurité du système de commande doivent être interfacés avec les dispositifs sans fonction de sécurité. Puisque des défaillances sur les dispositifs de commande de démarrage et d'arrêt ne doivent pas entraîner une perte de la fonction de sécurité, ces dispositifs ne sont pas considérés comme faisant partie du système de sécurité. Ce circuit de démarrage/arrêt/maintien symbolise les dispositifs sans fonction de sécurité du circuit de commande de la machine et il peut être remplacé par un PLC.

La catégorie B donne les fondations pour la conception du système de sécurité. Bien que conception, sélection et installation correctes constituent la base d'un système robuste, de nombreux facteurs peuvent individuellement provoquer la perte du système de sécurité. En portant attention à ces facteurs, il est possible de diminuer ces risques de défaillance cause de danger. L'utilisation de la catégorie B seule ne convient pas pour la plupart des applications de sécurité.

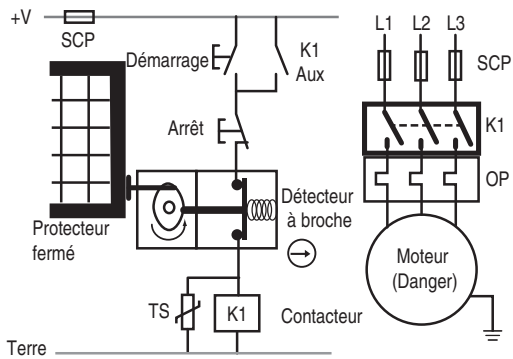
Catégorie 1

La catégorie 1 impose que le système soit conforme aux termes de la catégorie B et qu'il utilise des composants de sécurité éprouvés. Qu'est-ce que des composants de sécurité et comment sait-on qu'ils sont éprouvés ? La norme ISO 13849-2 permet de répondre à ces questions pour les systèmes mécaniques, hydrauliques, pneumatiques et électriques. L'annexe D traite des composants électriques.

Les composants sont considérés comme éprouvés s'ils ont été utilisés avec succès dans de nombreuses applications similaires. Les nouveaux composants de sécurité sont considérés comme éprouvés s'ils ont été conçus et vérifiés en accord avec les normes appropriées.

Composants éprouvés	**Norme**
Interrupteur avec activation en mode positif (manœuvre positive d'ouverture)	CEI 60947-5-1
Dispositif d'arrêt d'urgence	ISO 13850, CEI 60947-5-5
Fusible	CEI 60269-1
Disjoncteur	CEI 60947-2
Contacteurs	CEI 60947-4-1, CEI 60947-5-1
Contacts mécaniques	CEI 60947-5-1
Contacteur auxiliaire (p. ex., contacteur, relais de commande, relais guidés réciproquement)	EN 50205 CEI 60204-1, CEI 60947-5-1
Transformateur	CEI 60742
Câble	CEI 60204-1
Verrous	ISO 14119
Interrupteur à température	CEI 60947-5-1
Manomètre à pression	CEI 60947-5-1 + exigences pneumatiques et hydrauliques
Dispositif ou équipement de commutation de commande et de protection	CEI 60947-6-2
Automate programmable	CEI 61508, CEI 62061

Si l'on veut utiliser des composants éprouvés dans un système de catégorie B, ce la signifie remplacer le détecteur de position par un interrupteur à broche à manœuvre positive d'ouverture et cela implique de surdimensionner le contacteur pour une meilleure protection contre le soudage des contacts.



Système de sécurité de catégorie 1 simple

Le schéma montre les modifications apportées au système simple de catégorie B afin d'être conforme à la catégorie 1. L'e dispositif de verrouillage et le contacteur jouent les rôles clés dans le retrait de l'énergie de l'actionneur, lorsqu'il est nécessaire d'accéder à la source de danger. Le dispositif de verouillage à broche est conforme à la norme CEI 60947-5-1 pour les commandes à manœuvre positive d'ouverture, qui est indiqué par le symbole de la flèche dans le cercle. Avec les composants éprouvés, la probabilité de suppression de l'énergie est plus grande pour la catégorie 1 que pour la catégorie B. L'utilisation de composants éprouvés a pour objet d'empêcher la perte de la fonction de sécurité. Même avec ces améliorations, une seule panne peut tout de même entraîner la perte de la fonction de sécurité.

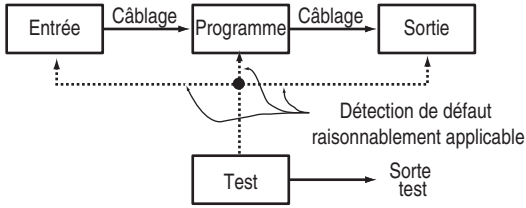
Peut-on appliquer les mêmes principes au système de catégorie B à base de PLC pour améliorer les performances de sécurité afin d'obtenir une catégorie 1 ? Il y a du pour et du contre. Il est sûr que remplacer tous les détecteurs de position fonctionnant en mode négatif par des commandes à manœuvre positive d'ouverture et en surdimensionnant les contacteurs améliorera la probabilité d'exécution de la fonction de sécurité. Le PLC devient alors le centre d'intérêt. Le PLC a-t-il été utilisé dans beaucoup d'applications similaires ? Le programme relais est-il validé et stable, ou est-il peaufiné en permanence pour l'améliorer et le régler ? Le firmware (la partie du logiciel que l'utilisateur ne peut pas modifier) a-t-il été révisé récemment ? Quel est l'historique des défaillances matérielles créant un danger dans les nombreuses applications similaires ? Des mesures ont-elles été prises pour éliminer ou réduire ces défaillances à un niveau acceptable ? En théorie, il est possible qu'un PLC puisse être considéré comme un composant éprouvé sur la base d'une structure en fonction elle-même éprouvée. Adopter cette approche pour un dispositif comme un PLC est une tâche importante qui implique de consigner et d'analyser de nombreuses données. Pour simplifier la situation et éviter l'utilisation arbitraire des PLC « ordinaires », la norme ISO 13849-1:1999 stipule que « au niveau des composants électroniques, il n'est normalement pas possible d'obtenir une catégorie 1 ».

Les catégories B et 1 sont destinées à la prévention. La conception a pour objet d'éviter une situation dangereuse. Lorsque la prévention elle-même ne permet pas une réduction suffisante des risques, la détection de panne doit être utilisée. Les catégories 2, 3 et 4 sont destinées à la détection des pannes, avec des critères plus stricts pour obtenir améliorer la réduction des risques.

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

Catégorie 2

En plus d'être conforme aux critères de la catégorie B et d'utiliser des principes de sécurité éprouvés, le système de sécurité doit subir des tests pour être conforme à la catégorie 2. Ces tests doivent être conçus pour détecter les pannes dans les composants de sécurité du système de commande. Si aucune panne n'est détectée, le système peut fonctionner. Si des pannes sont détectées, le test doit initier une commande. Lorsque c'est possible, la commande doit amener la machine à un état sécurisé.

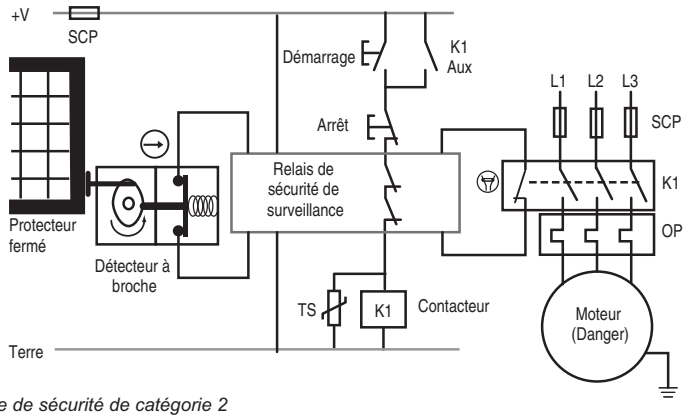


Le test doit permettre une détection des pannes dont la mise en œuvre est raisonnablement possible. L'équipement de test peut faire partie du système de sécurité ou être un équipement séparé.

Les tests doivent être effectués :

- à la première mise sous tension de la machine,
- avant l'amorçage d'un danger, et
- périodiquement si c'est jugé nécessaire après l'évaluation du risque.

Les mots « lorsque c'est possible » et « raisonnablement possible » indiquent que toutes les pannes ne peuvent pas être détectées. Etant donné qu'il s'agit d'un système à une seule voie (c'est-à-dire, un fil connecte l'entrée à la logique, puis à la sortie), une seule panne peut provoquer la perte de la fonction de sécurité. Dans certains cas, la catégorie 2 ne peut pas être complètement appliquée à un système de sécurité ; cela parce que tous les composants ne peuvent pas être vérifiés.

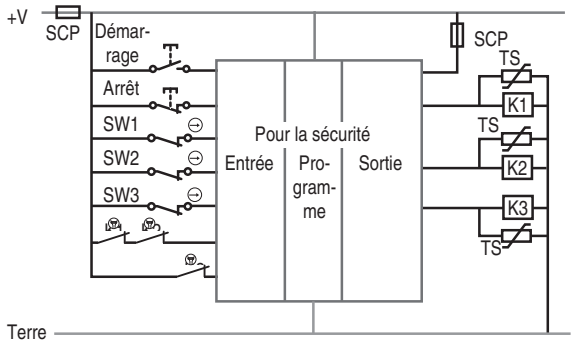


Système de sécurité de catégorie 2

Le schéma montre un système simple de catégorie 1 amélioré pour être conforme à la catégorie 2. Un relais de surveillance de sécurité effectue les tests. A la mise sous tension, le relais vérifie ses composants internes. Si aucune panne n'est détectée, le relais vérifie l'interrupteur à broche en surveillant le cycle de fonctionnement de ses contacts. Si aucune panne n'est détectée et que la barrière de protection est fermée, le relais de surveillance de sécurité vérifie le dispositif de sortie : les contacts mécaniques du contacteur. Si aucune panne n'est détectée et que le contacteur est désactivé, le relais active sa sortie interne et connecte la bobine de K1 au bouton d'arrêt. A ce moment, les composants standard du système de commande de la machine, le circuit démarrage/arrêt/verrouillage, peuvent arrêter ou démarrer la machine.

L'ouverture de la barrière de protection désactive la sortie du relais de surveillance de sécurité. Lorsque la barrière est refermée, le relais répète les vérifications du système de sécurité. Si aucune panne n'est détectée, le relais active sa sortie interne. Le relais de surveillance de sécurité permet à ce circuit d'être conforme à a la catégorie 2 en effectuant des tests sur le dispositif d'entrée, le dispositif logique (lui-même) et le dispositif de sortie. Le test est réalisé lors de la première mise sous tension et avant l'amorçage du danger.

Grâce à ses capacités logiques intrinsèques, un système de sécurité à base de PLC peut être conçu pour être conforme à la catégorie 2. Comme indiqué dans la discussion sur la catégorie 1 ci-dessus, la justification du caractère éprouvé du PLC (y compris ses capacités de test) constitue le défi. Pour les systèmes de sécurité complexes qui requièrent un classement de catégorie 2, un PLC de sécurité conforme CEI 61508 doit être soumis pour le PLC standard.



Système de sécurité de catégorie 2 complexe

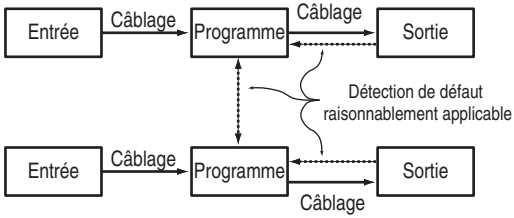
Le schéma présente un exemple de système complexe qui utilise un PLC de sécurité. Un PLC de sécurité est considéré comme éprouvé si sa conception est conforme à la norme appropriée. Les contacts mécaniques des contacteurs sont reliés à l'entrée du PLC pour les tests. Ces contacts peuvent être branchés en série à une borne d'entrée ou à des bornes d'entrée individuelles, selon le programme logique.

Bien que des composants de sécurité éprouvés soient utilisés, une seule panne se produisant entre les vérifications peut entraîner la perte de la fonction de sécurité. Par conséquent, les systèmes de catégorie 2 sont utilisés dans les applications présentant un risque faible. Lorsqu'une tolérance élevée aux défaillances est nécessaire, le système de sécurité doit être conforme à la catégorie 3 ou 4.

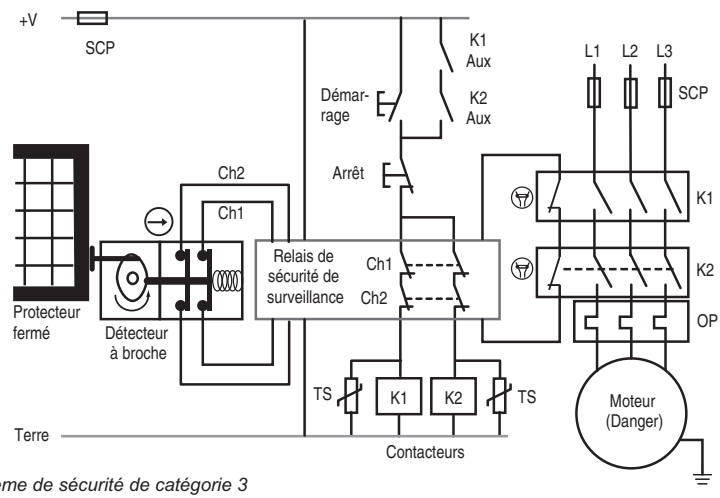
Catégorie 3

En plus de la conformité aux exigences de la catégorie B et des principes de sécurité éprouvés, la catégorie 3 requiert que la fonction de sécurité puisse être exécutée en présence d'une panne. La panne doit être détectée au moment de l'appel ou avant l'appel suivant de la fonction de sécurité, lorsque c'est raisonnablement possible.

Ici également nous trouvons l'expression « lorsque c'est raisonnablement possible ». Ceci couvre les pannes qui ne sont pas détectées. Tant que la panne non détectable ne conduit pas à la perte de la fonction de sécurité, cette fonction peut être conforme à la catégorie 3. Par conséquent, une accumulation de pannes non détectées peut entraîner la perte de la fonction de sécurité.



Le schéma explique les principes d'un système de catégorie 3. La redondance combinée à une surveillance réciproque pouvant raisonnablement être mise en œuvre et une surveillance des sorties est utilisée pour assurer le bon fonctionnement de la fonction de sécurité.



Système de sécurité de catégorie 3

Le schéma présente un système de catégorie 3 Un jeu de contacts redondant est ajouté à l'interrupteur de sécurité à broche. Le relais de surveillance de sécurité contient en interne des circuits redondants qui se surveillent réciproquement. Un jeu de contacts redondant coupe l'alimentation du moteur. Les contacteurs sont surveillés par le relais de surveillance de sécurité par le biais des contacts mécaniques « raisonnablement possible ».

La détection de panne doit être prise en considération pour chaque partie du système de sécurité, ainsi que pour les connexions (c.-à-d., le système). Quels sont les modes de défaillance d'un interrupteur à broche double voie ? Quels sont les modes de défaillance du relais de surveillance de sécurité ? Quels sont les modes de défaillance des contacteurs K1 et K2 ? Quels sont les modes de défaillance du câblage ?

L'interrupteur de sécurité à broche est conçu avec des contacts à manœuvre positive d'ouverture. Nous savons donc que l'ouverture de la barrière de protection est prévue pour ouvrir un contact soudé. Ceci résout un mode de défaillance. Existe-t-il d'autres modes de défaillance ?

L'interrupteur à manœuvre positive d'ouverture est généralement conçu avec un rappel par ressort. Si la tête est retirée ou cassée, les contacts de sécurité reviennent par l'action du ressort à l'état fermé (sécurisé). De nombreux dispositifs de verrouillage sont conçus avec des têtes amovibles pour faciliter l'installation dans diverses applications. La tête peut être retirée et positionnée dans deux à quatre positions différentes.

Une panne peut se produire si les vis de fixation de la tête ne sont pas serrées correctement. Dans ce cas, les vibrations de la machine peuvent provoquer le dévissage des vis. La tête de commande, sous la pression du ressort, supprime la pression exercée sur les contacts de

sécurité et ces contacts se ferment. Par la suite, l'ouverture de la barrière de protection n'ouvre pas les contacts de sécurité et une panne se produit avec création d'un danger.

Le mécanisme de fonctionnement à l'intérieur du dispositif de verrouillage doit également être examiné. Quelle est la probabilité que la panne d'un seul composant entraîne la perte de la fonction de sécurité ? La réponse à ces questions sera donnée plus tard étant donné qu'une durée moyenne de fonctionnement avant défaillance dangereuse, le champ d'application des diagnostics et une fraction de panne sans danger doivent être fournis pour compléter les connaissances nécessaires afin d'assurer le bon fonctionnement de la fonction de sécurité.

Une pratique courante consiste à utiliser des interrupteurs à broche avec double contacts dans les circuits de catégorie 3. Cet usage doit être basé sur l'exclusion de l'échec d'ouverture des contacts de sécurité par l'interrupteur. Ceci est considéré comme une « exclusion de défaillance » et est abordé plus loin dans ce chapitre.

Un relais de surveillance de sécurité électromécanique est un dispositif peu complexe souvent évalué par un organisme tiers et reçoit une classification de catégorie. Les capacités du relais incluent souvent la double voie, la surveillance de dispositif externe et la protection contre les courts-circuits. Aucune norme spécifique n'est écrite sur la façon de concevoir ou d'utiliser les relais de surveillance de sécurité. Ces relais sont évalués pour leur capacité à exécuter la fonction de sécurité selon la norme ISO 13849-1 ou la norme précédente EN 954-1. Pour être conforme à la catégorie de sécurité d'un système, le relais doit avoir au moins la même classification.

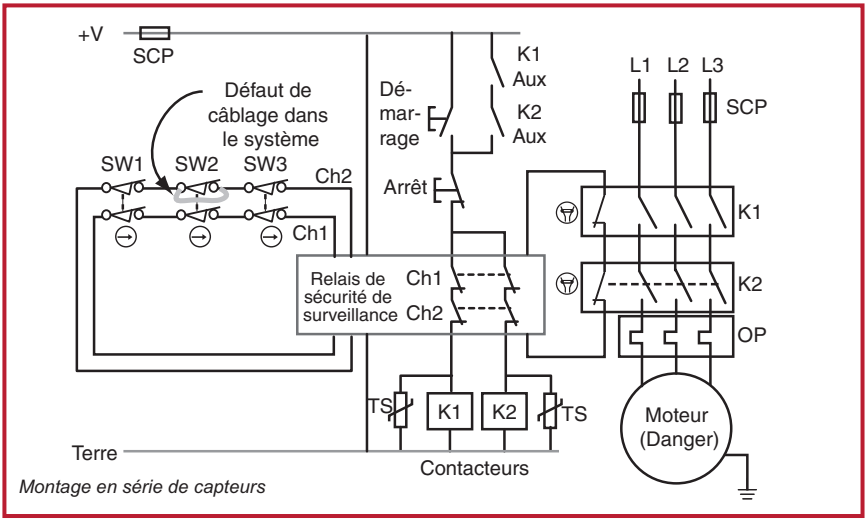
Deux contacteurs permettent de s'assurer que la fonction de sécurité est remplie par les dispositifs de sortie. Avec la protection contre les surcharges et les courts-circuits, la probabilité de panne du contacteur à cause du soudage de contacts est faible, mais pas impossible. Un contacteur peut également tombé en panne à cause de ses contacts de commutation de puissance en raison du blocage de son armature. Si un contacteur tombe en panne en créant un danger, le deuxième contacteur coupe l'alimentation de la source de danger. Le relais de surveillance de sécurité détecte le contacteur défaillant lors du cycle suivant de la machine. Lorsque la barrière de protection est fermée et que le bouton de démarrage est enfoncé, les contacts mécaniques du contacteur défaillant restent ouverts et le relais de surveillance de sécurité ne peut pas fermer ses contacts de sécurité, ce qui met en évidence la panne.

Pannes non détectées

Comme indiqué plus haut, certaines pannes ne peuvent pas être détectées. Ces pannes n'entraîne pas à elles seules la perte de la fonction de sécurité. Lors de l'évaluation des pannes, il faut poser certaines questions. Selon la réponse à la première question, la question suivante diffère : *Première question :* La panne peut-elle être détectée ?

Si la réponse est oui, il faut alors savoir si cette détection est immédiate ou lors de la requête suivante. Il faut également savoir si elle peut être masquée (c.-à-d., effacée) par un autre dispositif.

Si la réponse est non, la panne a-t-elle entraîné la perte de la fonction de sécurité ? Une panne ultérieure peut-elle entraîner la perte de la fonction de sécurité ?



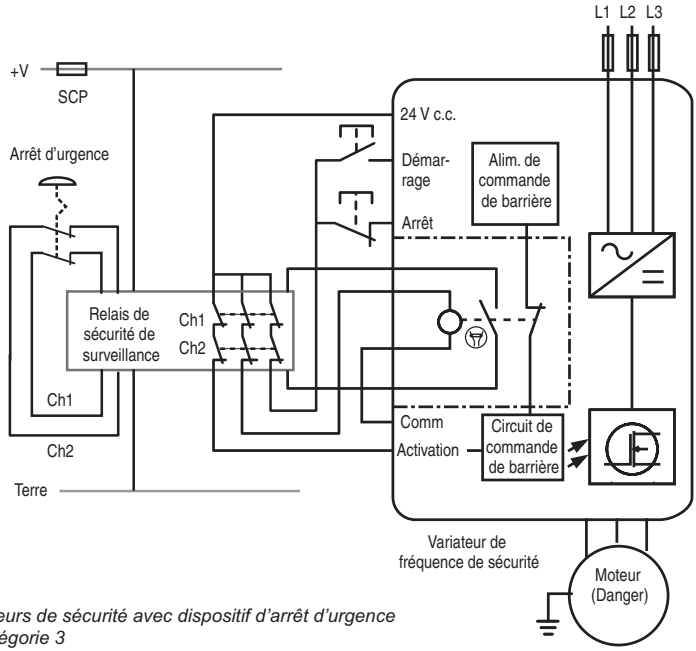
Montage en série de capteurs

Le schéma montre une approche couramment utilisée pour connecter plusieurs dispositifs à un relais de surveillance de sécurité. Chaque dispositif contient deux contacts à manœuvre positive d'ouverture normalement ouverts. Ces dispositifs peuvent être une combinaison de dispositifs de verrouillage ou de boutons d'arrêt d'urgence. Cette approche permet de réduire le coût du câblage puisque les capteurs sont montés en série. Supposons qu'un court-circuit se produise sur l'un des contacts, peut-il être détecté ?

Lorsque les interrupteurs Sw1 et Sw3 sont ouverts, le relais de surveillance de sécurité coupe l'alimentation de la source de danger. Lorsque Sw1 et Sw3 sont fermés, la source de danger peut être redémarrée en appuyant sur le bouton de démarrage. Pendant ces actions, la panne n'a pas été détectée mais elle n'a pas entraîné la perte de la fonction de sécurité. Quand est-il lorsque Sw2 est ouvert ?

Lorsque Sw2 s'ouvre, Ch1 s'ouvre et Ch2 reste fermé. Le relais de surveillance de sécurité met la source de danger hors tension parce que Ch1 s'est ouvert. Lorsque Sw2 ferme. le moteur ne peut pas être démarré lorsque l'on appuie sur le bouton de démarrage, ceci parce que Ch2 ne s'est pas ouvert. La panne est détectée. La faiblesse de ce concept est que l'interrupteur Sw1 ou Sw3 peut être ouvert ou fermé et masquer la panne. Une panne ultérieure (un court-circuit sur le deuxième contact ou sur Sw2) entraîne la perte de la fonction de sécurité. La connexion en série des contacts mécaniques est limitée à la catégorie 3 puisqu'elle peut conduire à la perte de la fonction de sécurité en raison d'une accumulation de pannes.

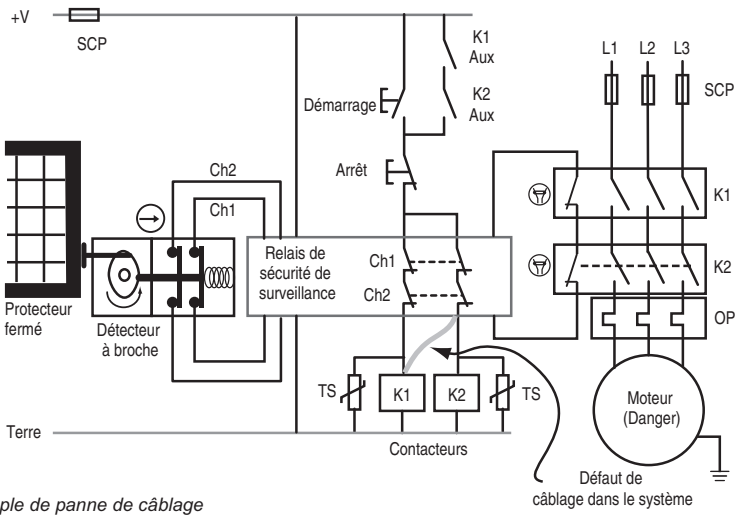
AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles
Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr



Variateurs de sécurité avec dispositif d'arrêt d'urgence de catégorie 3

Le schéma montre un circuit de catégorie 3 qui utilise un variateur de fréquence de sécurité. Les développements récents de la technologie des variateurs, combinés à l'actualisation des normes électriques, permettent d'utiliser des variateurs de sécurité dans les circuits d'arrêt d'urgence sans avoir besoin de rupteur électromécanique de l'actionneur (p. ex., le moteur).

Un appui sur le dispositif d'arrêt d'urgence ouvre les sorties du relais de surveillance de sécurité. Ceci envoie un signal d'arrêt au variateur, supprime le signal de validation et ouvre l'alimentation de commande de la barrière. Le variateur exécute un arrêt de catégorie 0 – coupure immédiate de l'alimentation du moteur. Le variateur est classé catégorie 3 parce qu'il possède des signaux redondants pour couper l'alimentation du moteur : le signal de validation et un relais guidé réciproquement. Le relais guidé réciproquement fournit un retour à l'actionneur. Le variateur lui-même est analysé pour vérifier qu'une seule panne n'entraîne pas la perte de la fonction de sécurité.

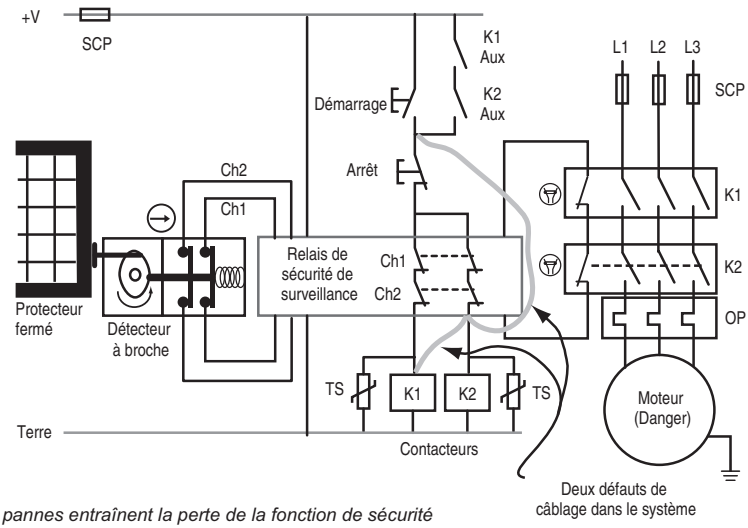


Exemple de panne de câblage

Le schéma montre un exemple de panne du câblage, un court-circuit, entre la sortie de sécurité de la voie 2 du relais de surveillance de sécurité et la bobine du contacteur K1. Tous les composants fonctionnent correctement. Cette panne du câblage peut se produire avant la mise en service de la machine ou plus tard pendant les opérations de maintenance ou le mise à niveau.

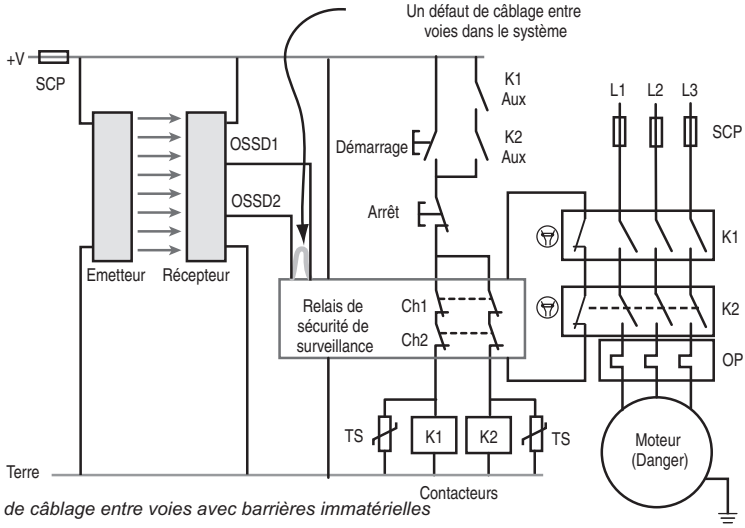
Cette panne peut-elle être détectée ?

Dans cette exemple, la panne ne peut pas être détectée par le système de sécurité. Heureusement, elle n'entraîne pas la perte de la fonction de sécurité. Cette panne, tout comme la panne entre Ch1 et K2, doit être détectée pendant les opérations de mise en service.



Deux pannes entraînent la perte de la fonction de sécurité

Le schéma montre une deuxième panne qui entraîne la perte de la fonction de sécurité. C'est un court-circuit entre le relais de surveillance de sécurité et le bouton de démarrage. A la mise sous tension, avec la barrière de protection fermée, ces deux pannes ne sont pas détectées. Un appui sur le bouton de démarrage amorce le danger. L'ouverture de la barrière de protection n'arrête pas la source de danger.



Panne de câblage entre voies avec barrières immatérielles

Le schéma montre un exemple de système de sécurité avec barrières immatérielles (sorties OSSD)

Le système de sécurité peut-il détecter cette panne ?

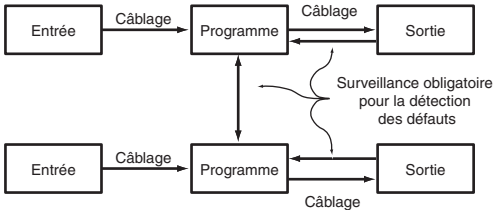
Le relais de surveillance de sécurité ne peut pas détecter cette panne parce que les deux entrées sont +V. Dans cet exemple, la panne du câblage est détectée par la barrière immatérielle. Certaines barrières immatérielles utilisent une technique de détection de panne appelée test par impulsion. Avec ces barrières, la détection de la panne est immédiate et la barrière immatérielle arrête ses sorties. Dans d'autres barrières, la détection se fait lorsque la barrière immatérielle est initialisée. Lorsqu'elle tente d'activer ses sorties, la panne est détectée et les sorties restent désactivées. Dans les deux cas, la source de danger reste désactivée en présence de la panne.

Détection de panne avec test par impulsion

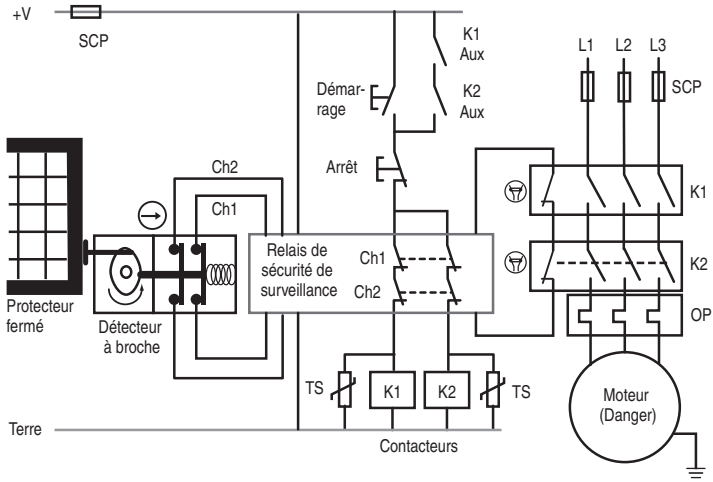
Les circuits de sécurité sont conçus pour transporter le courant lorsque le système de sécurité est actif et que la source de danger est protégée. Le test par impulsion est une technique dans laquelle le courant du circuit chute à zéro pendant une très courte période. La durée est trop courte pour que le circuit de sécurité réagisse et désactive la source de danger, mais elle est suffisamment longue pour être détectée par un système à microprocesseur. Les impulsions sur les voies sont décalées les unes par rapport aux autres. Si un court-circuit se produit, le microprocesseur détecte les impulsions sur les deux voies et initie une commande pour arrêter la source de danger.

Catégorie 4

Comme la catégorie 3, la catégorie 4 requiert que le système soit conforme à la catégorie B et qu'il utilise les principes de sécurité et exécute la fonction de sécurité en présence d'une seule panne. A l'inverse de la catégorie 3 pour laquelle une accumulation de pannes entraîne la perte de la fonction de sécurité, la catégorie 4 requiert que la fonction de sécurité puisse être exécutée, même en présence de plusieurs pannes. Lorsque l'on parle d'accumulation de pannes, 2 pannes peuvent être suffisantes, mais 3 peuvent être nécessaires pour certains systèmes.



L'illustration montre le schéma fonctionnel de la catégorie 4. La surveillance des deux dispositifs de sortie et la surveillance réciproque sont nécessaires en tout temps, pas uniquement lorsque c'est raisonnablement possible. Ceci permet de différencier la catégorie 4 de la catégorie 3.



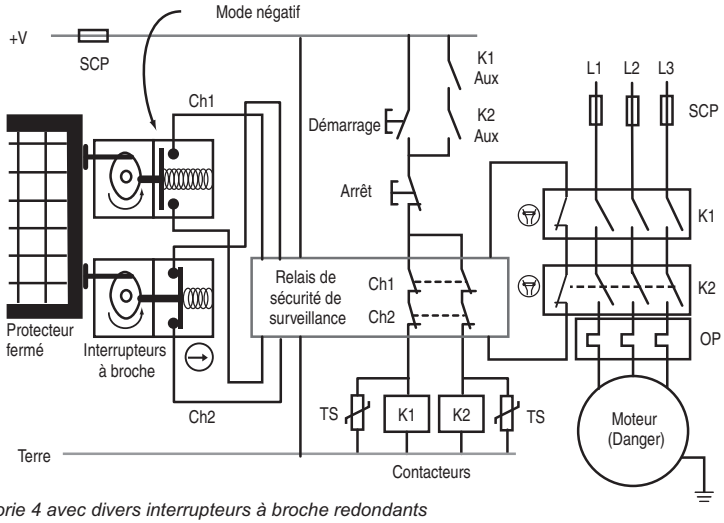
Catégorie 4 avec exclusion de pannes pour interrupteur à broche

Le schéma montre un exemple de circuit de catégorie 4 qui utilise l'exclusion de panne pour l'interrupteur à broche. L'exclusion de panne permet de ne pas prendre en considération la défaillance d'ouverture des contacts de l'interrupteur à broche. L'exclusion de panne doit avoir une justification technique et doit être identifiée. Cette justification doit prendre en

considération la vitesse de l'actionneur, la position de l'actionneur, les dispositifs d'arrêt mécaniques et une tête de commande sécurisée.

Si le concepteur du système de sécurité préfère utiliser des interrupteurs à broche mais ne désir par utiliser l'exclusion de panne sur ces interrupteurs, les deux interrupteurs à broche peuvent être utilisés pour la conformité à la catégorie 4. Le relais de surveillance de sécurité lui-même doit être conforme à la catégorie 4, et les deux contacteurs de sortie, qui utilisent des contacts mécaniques, doivent être surveillés.

Une diversité peut être appliquée pour réduire encore plus la probabilité de perte de la fonction de sécurité en raison du mode commun ou de la cause d'origine commune de défaillances, l'un des interrupteurs de sécurité à broche peut être converti au mode négatif. Un interrupteur fonctionnant en mode négatif est acceptable si un deuxième interrupteur utilise des contacts à manœuvre positive d'ouverture. Le schéma suivant montre un exemple de cette approche diversifiée. Avec cette approche, le relais de surveillance de sécurité doit être prévu pour accepter les entrées normalement ouvertes et normalement fermées.



Catégorie 4 avec divers interrupteurs à broche redondants

Caractéristiques nominales des composants et du système

La norme ISO 13849-1 requiert des caractéristique nominales aussi bien pour les composants et que pour le système. Ceci génère une certaine confusion qu'il est possible de clarifier par la compréhension des composants et de leurs capacités. Il est possible d'utiliser un composant de catégorie 1 dans un système de catégorie 2, 3 ou 4, selon l'architecture du système.

Les catégories B et 1 sont définies comme des catégories basées sur la prévention, alors que les catégories 2, 3 et 4 sont décrites comme des catégories basées sur la détection. Ces catégories sont appliquées en fonction des composants, mais également selon le système. Le système de sécurité type est constitué d'un interrupteur de sécurité, d'un relais de sécurité et d'un contacteur de sécurité. L'interrupteur et le contacteur sont classés catégorie 1 parce qu'il ne servent qu'à la prévention. Il utilisent les principes de sécurité mais n'exécute aucune détection ou auto-vérification. Ces dispositifs peuvent être utilisés pour la redondance dans les systèmes de catégories 3 et 4, dans le cas où le dispositif logique se charge de la détection.

Les dispositifs logiques ne servent pas qu'à la prévention, ils servent également à la détection. Ils font une auto-vérification interne pour assurer un fonctionnement correct. Par conséquent, les relais de surveillance de sécurité et les automates de sécurité programmables ont des caractéristiques conformes aux catégories 2, 3 ou 4.

Considérations sur les pannes et exclusions

L'analyse de sécurité requiert une analyse approfondie des pannes et une bonne compréhension du fonctionnement du système de sécurité en présence de pannes le cas échéant. Les normes ISO 13849-1 et ISO 13849-2 fournissent des détails sur les critères et les exclusions des pannes.

Si une panne résulte de la défaillance ultérieure d'un composant, la première panne et toutes les pannes ultérieures sont considérées comme une seule panne.

Si plusieurs pannes résultent d'une seule cause, ces pannes sont considérées comme une seule panne. Ceci s'appelle une panne d'origine commune.

L'apparition de plusieurs pannes en même temps est considérée comme très improbable et n'est pas prise en compte dans cette analyse. Dans l'hypothèse de base, une seule panne se produit entre les requêtes soumises au système de sécurité.

Lorsque les composants et les systèmes sont conçus selon les normes appropriées, l'apparition de la panne peut être exclue. Par exemple, la défaillance d'ouverture des contacts normalement fermés peut être exclue si l'interrupteur est conforme à la norme CEI 60947-5-1, annexe K. La norme ISO 13849-2 fournit une liste des exclusions de pannes.

Systèmes avec arrêts de catégorie 1

Tous les exemples précédents ont présenté des dispositifs d'arrêt de catégorie 0 (coupure immédiate de l'alimentation des actionneurs). Un dispositif d'arrêt de catégorie 1 (activer le freinage jusqu'à l'arrêt, puis couper l'alimentation de l'actionneur) est obtenu avec une sortie temporisée. Une barrière muni d'interrupteurs de sécurité accompagne souvent un dispositif d'arrêt de catégorie 1. Ceci permet de maintenir la barrière en position fermée jusqu'à ce que la machine soit dans un état de sécurité (c.-à-d., arrêtée).

Arrêter une machine sans prendre en considération l'automate programmable peut affecter le redémarrage et peut entraîner une détérioration grave des outils et de la machine. Il n'est pas possible de réaliser un arrêt de sécurité uniquement avec un PLC standard (sans sécurité) ; il faut donc considérer d'autres approches.

Trois solutions possibles sont proposées ci-après :

1. Automates programmables de sécurité

Utilisez un PLC avec un niveau d'intégrité de sécurité suffisamment élevé pour une utilisation de sécurité. En pratique, cela est possible en utilisant un PLC de sécurité comme GuardLogix pour la commande de sécurité et standard.

2. Relais de sécurité avec commande de contournement temporisée

Un relais de sécurité avec sorties immédiates et temporisées est utilisé (p. ex. MSR138DP). Les sorties à action immédiate sont raccordées aux entrées du dispositif programmable (automate programmable, par exemple) et les sorties temporisées au contacteur. Lorsque l'interrupteur de sécurité est actionné, les sorties immédiates du relais de sécurité commutent, signalant au système programmable de procéder à un arrêt correctement séquencé. Suite à un délai suffisant autorisant l'opération, la sortie temporisée du relais de sécurité commute pour couper le contacteur principal.

Remarque : Tout calcul pour déterminer le temps d'arrêt complet doit prendre en compte le délai de temporisation des sorties du relais de sécurité. C'est particulièrement important lorsque ce facteur est utilisé pour déterminer le positionnement des dispositifs en conformité avec le calcul de la distance de sécurité.

3. Dispositifs de verrouillage programmables commandés par le système

Cette solution offre le même niveau élevé de sécurité qu'un circuit câblé, tout en assurant un arrêt immédiat correctement séquencé, mais elle n'est applicable que lorsque le phénomène dangereux est protégé par une protection.

Pour que l'ouverture de la barrière de protection soit autorisée, l'électro-aimant de l'interrupteur de verrouillage doit recevoir un signal de déclenchement de la part de l'automate programmable. Ce signale n'est donné qu'après une séquence de commande

d'arrêt terminée, afin de diminuer le risque de détérioration d'outil ou de perte de programme. Lorsque l'électro-aimant est activé, la barrière peut être ouverte. Le contacteur de la machine est interrompu par les contacts du circuit de commande de l'interrupteur de verrouillage. Pour surmonter les ralentissements machine ou les faux signaux de déclenchement, il peut être nécessaire d'associer à l'automate programmable une unité de temporisation (p. ex., MSR178DP) ou un détecteur d'arrêt de mouvement (p. ex., CU2).

Exigences pour les systèmes de commande de sécurité aux Etats-Unis

Les exigences relatives aux systèmes de commande de sécurité aux Etats-Unis se trouvent dans différentes normes, mais deux documents se dégagent : ANSI B11.TR3 et ANSI R15.06. Le rapport technique ANSI B11.TR3 définit quatre niveaux qui sont caractérisés par le niveau de réduction des risques qu'ils fournissent.

Ci-dessous, les exigences de chaque niveau.

Niveau de réduction des risques le plus faible

Dans la norme ANSI B11.TR3, les protections qui fournissent le plus faible niveau de réduction des risques incluent les dispositifs électriques, électroniques, hydrauliques ou pneumatiques et les systèmes de commande associés qui utilisent une configuration à une seule voie. Implicite dans la liste des exigences, est l'obligation d'utilisation des dispositifs de sécurité. Ceci est très proche de la catégorie 1 de la norme ISO 13849-1.

Niveau de réduction faible/intermédiaire des risques

Dans la norme ANSI B11.TR3, les protections qui fournissent une réduction faible/intermédiaire des risques incluent les systèmes de commande redondants pour lesquels le bon fonctionnement du système de sécurité peut être vérifié manuellement. Si l'on regarde uniquement les exigences de base, le système doit utiliser une redondance simple. L'utilisation d'une fonction de vérification n'est pas obligatoire. Sans fonction de vérification, l'un des composants de sécurité redondants peut tomber en panne et le système de sécurité ne s'en aperçoit pas. Ceci résulte en un système à une seule voie. Ce niveau de réduction des risques s'accorde le mieux avec la catégorie 2 lorsque la vérification est utilisée.

Niveau de réduction élevé/intermédiaire des risques

Dans la norme ANSI B11.TR3, les protections qui fournissent une réduction élevée/intermédiaire des risques incluent les systèmes de commande redondants avec auto-vérification au démarrage pour confirmer le bon fonctionnement du système de sécurité. Pour les machines devant être démarrées chaque jour, l'auto-vérification est une amélioration significative pour l'intégrité de la sécurité par rapport au système purement redondant. Pour les machines qui fonctionnent 24/24 h 7 jours sur 7, l'auto-vérification n'est qu'une amélioration marginale. L'utilisation de la surveillance du système de sécurité permet d'être conforme à la catégorie 3.

Niveau de réduction des risques le plus élevé

La norme ANSI B11.TR3 permet le niveau le plus élevé de réduction des risques pour les systèmes de commande redondants et avec auto-vérification permanente. L'auto-vérification doit vérifier le bon fonctionnement du système de sécurité. Le défi du concepteur du système de sécurité est de déterminer ce qui est permanent. De nombreux systèmes de sécurité exécutent leurs vérifications su démarrage et lorsqu'une requête est soumise au système de sécurité.

A l'inverse, certains composants exécutent une auto-vérification en permanence. Les barrières immatérielles, par exemple, activent et désactivent séquentiellement leurs voyants. Etant donné que l'auto-vérification est permanente, si une panne se produit, la barrière immatérielle désactive ses sorties avant qu'une requête ne soit soumise au système de sécurité. Les relais et PLC de sécurité à microprocesseurs sont d'autres composants qui exécutent une vérification permanente.

L'exigence d'une auto-vérification « permanente » du système de commande n'a pas pour objectif de limiter le choix des composants aux barrières immatérielles et aux dispositifs logiques à microprocesseurs. La vérification doit se faire au démarrage et après chaque requête soumise au système de sécurité. Ce niveau de réduction des risques a pour objectif la conformité avec la catégorie 4 de la norme ISO 13849-1.

Normes pour robots : Etats-Unis/Canada

Les normes pour robots aux Etats-Unis (ANSI RIA R15.06) et au Canada (CSA Z434-03) sont similaires. Les deux ont quatre niveaux, qui sont similaires aux catégories de la norme EN 954-1:1996.

Simple

A ce niveau le plus faible, les systèmes de commande de sécurité simples doivent être conçus et fabriqués avec des circuits à une seule voie validés ; ils peuvent également être programmables. Au Canada, ce niveau est également limité aux utilisations de signalisation et d'indication. Le défi du concepteur du système de sécurité est de déterminer ce qui est « validé ». Qu'est-ce qu'un système à une voie validé ? Pour qui ce système est-il validé ? Le niveau Simple est le plus proche de la catégorie B de la norme EN 954-1:1996.

Voie unique

Le niveau suivant est un système de commande de sécurité simple voie qui

- est basé sur le matériel ou est un dispositif logiciel/firmware de sécurité ;
- inclut des composants de sécurité ;
- est utilisé dans le respect des recommandations du fabricant ; et
- utilise une configuration à circuit ouvert.

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

Un exemple de circuit validé est un dispositif à ouverture positive électromécanique à simple voie qui signale un arrêt en mode désactivé. Etant un système à une voie, la panne d'un seul composant peut entraîner la perte de la fonction de sécurité. Le niveau Simple se rapproche le plus de la catégorie 1 de la norme EN 954-1:1996.

Dispositif logiciel/firmware de sécurité

Bien que les systèmes matériels aient été la méthode privilégiée pour fournir une protection aux robots, les dispositifs logiciels/firmware deviennent un choix répandu en raison de leur capacité à prendre en charge des systèmes complexes. Les dispositifs logiciels/firmware (PLC ou automates de sécurité) sont autorisés à condition d'être des dispositifs de sécurité. Cette classification requiert que la défaillance d,un seul composant ou firmware de sécurité n'entraîne pas la perte de la fonction de sécurité. Lorsqu'un défaut est détecté, le fonctionnement automatique ultérieur du robot est empêchée jusqu'à ce que le défaut soit effacé.

Pour être classé dispositif de sécurité, un laboratoire agréé doit tester le dispositif logiciel/ firmware pour une norme approuvée. Aux Etats-Unis, l'OSHA tient à jour une liste des laboratoires d'essai agréés au niveau national. Au Canada, le Conseil canadien des normes (CCN) tient à jour une liste similaire.

Voie unique avec surveillance

Les systèmes de commande de sécurité à une voie avec surveillance doivent se conformer aux exigences liées à la voie unique : avoir une classification de sécurité et utiliser la vérification. La vérification de la fonction de sécurité doit être exécutée au démarrage de la machine et à intervalles réguliers pendant le fonctionnement. La vérification automatique est préférable à la vérification manuelle.

La vérification permet le fonctionnement si aucune panne n'a été détectée ou elle génère un signal d'arrêt si elle détecte une panne. Un avertissement doit être émis si un danger demeure après la fin du mouvement. Bien sûr, la vérification elle-même ne doit pas créer une situation dangereuse. Après la détection de la panne, le robot doit rester dans son état de sécurité jusqu'à ce que la panne soit corrigée.

Le niveau voie unique avec surveillance se rapproche le plus de la catégorie 2 de la norme EN 954-1:1996.

Fiabilité de commande

Le niveau le plus élevé de réduction des risques pour les robots aux Etats-Unis et au Canada est obtenu par les systèmes de commande de sécurité conformes aux exigences de fiabilité de commande. Les systèmes de commande de sécurité avec fiabilité de commande sont des architectures double voie avec surveillance. La fonction d'arrêt du robot ne doit pas être bloquée par la panne d'un seul composant, y compris la fonction de surveillance.

La fonction de surveillance doit générer une commande d'arrêt lors de la détection d'une panne. Un avertissement doit être émis si un danger demeure après la fin du mouvement. Le système de sécurité doit rester en état de sécurité jusqu'à la correction de la panne.

Il est préférable que la panne soit détectée lorsqu'elle se produit. Si cela n'est pas possible, la défaillance doit être détectée lors de la requête suivante soumise au système de sécurité.

Les défaillances en mode commun doivent être prises en considération s'il existe une probabilité significative qu'une telle défaillance se produise.

Au Canada, il existe deux exigences supplémentaires par rapport aux Etats-Unis. Premièrement, le système de commande de sécurité doit être indépendant des systèmes de commande du programme normal. Deuxièmement, les système de sécurité ne doit pas être facile à contourner sans que cela soit détecté.

Les systèmes avec fiabilité de commande se rapprochent des catégories 3 et 4 de la norme EN 954-1:1996.

Commentaires sur la fiabilité de commande

L'aspect le plus fondamental de la fiabilité de commande est la tolérance aux pannes. Les exigences décrivent comment le système de sécurité doit répondre en présence d'une « panne unique », « toute panne unique » ou « toute défaillance d'un composant unique ».

Trois concepts importants doivent être pris en considération : (1) toutes les pannes ne sont pas détectées, (2) l'ajout du mot « composant » soulève des questions sur le câblage et (3) le câblage fait partie intégrante du système de sécurité. Les pannes du câblage peuvent entraîner la perte d'une fonction de sécurité.

L'objectif de la fiabilité de commande est clairement l'exécution de la fonction de sécurité en présence d'une panne. Si la panne est détectée, le système de sécurité doit exécuter une action de sécurité, avertir de la panne et empêcher le fonctionnement de la machine jusqu'à ce que la panne soit corrigée. Si la panne n'est pas détectée, la fonction de sécurité doit quand même être exécutée si une requête est soumise.

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 à la sécurité fonctionnelle des systèmes de commande

Important : *Les normes et les exigences abordées dans cette section sont relativement nouvelles. Le travail est toujours en cours sur certains aspects, particulièrement sur la clarification et la combinaison de certaines normes. Il est donc probable que certains informations données ici subissent des modifications. Pour obtenir les dernières informations, consultez : http://www.ab.com/safety.*

Au moment de la publication de ce document, il y a une prise de conscience grandissante des implications d'une nouvelle génération de normes couvrant la sécurité fonctionnelle des systèmes et des dispositifs de commande de sécurité.

En quoi consiste la sécurité fonctionnelle ?

La sécurité fonctionnelle, dans le cadre d'un système de sécurité général, dépend de la réaction appropriée des processus ou équipements aux entrées. Le site de la CEI fournit l'exemple suivant pour aider à clarifier ce que signifie la sécurité fonctionnelle. « Un thermostat installé dans les bobines d'un moteur électrique permettant de le mettre hors tension en cas de risque de surchauffe est un exemple de sécurité fonctionnelle. Mais fournir une isolation spécialisée pour résister à des températures élevées n'est pas un exemple de sécurité fonctionnelle (bien que ce soit tout de même un exemple de sécurité et que cela peut protéger contre le même danger). » Comme autre exemple, comparons un dispositif de protection matérielle à un dispositif de protection à verrouillage. La protection matérielle n'est pas considérée comme « sécurité fonctionnelle » alors qu'elle peut protéger contre l'accès à la même source de danger que la protection à verrouillage. A l'inverse, la barrière de protection à verrouillage est considérée comme un dispositif de sécurité fonctionnelle. En effet, lorsque la barrière est ouverte, le mécanisme de verrouillage communique avec le système afin de prévenir toute situation à risque. L'équipement de protection individuelle est également utilisé comme mesure de protection pour améliorer la sécurité des personnes. Cet équipement n'est cependant pas considéré comme dispositif de sécurité fonctionnelle.

Le terme sécurité fonctionnelle a été introduit par la norme CEI 61508:1998. Depuis, il a quelques fois été uniquement associé aux systèmes de sécurité programmable. C'est pourtant un concept erroné. La sécurité fonctionnelle recouvre de nombreux dispositifs utilisés pour créer des systèmes de sécurité. Les dispositifs comme les dispositifs de verrouillage, les barrières immatérielles, les relais de sécurité, les PLC de sécurité, les contacteurs de sécurité et les variateurs de sécurité sont interconnectés pour former un système de sécurité qui exécute une fonction de sécurité spécifique. C'est cela la sécurité fonctionnelle. Par conséquent, la sécurité fonctionnelle d'un système de commande électrique est très pertinent pour le contrôle des dangers créés par les pièces mobiles des machines.

La sécurité fonctionnelle ne peut être obtenue qu'en mettant en œuvre deux types d'exigences :

- la fonction de sécurité ;
- l'intégrité de la sécurité.

Le processus d'évaluation du risque joue un rôle clé dans l'élaboration des exigences liées à la sécurité fonctionnelle. Les impératifs de la fonction de sécurité (ce qui fait la fonction) découlent de l'analyse du danger. Les impératifs de l'intégrité de la sécurité (la probabilité que la fonction de sécurité réussisse) découlent de l'évaluation du risque.

Les trois principales normes en vigueur pour la sécurité fonctionnelle des machines sont les suivantes :

1. **CEI/EN 61508** « Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité ».

   Cette norme présente les impératifs et les prescriptions applicables lors de la conception de systèmes et de sous-systèmes électroniques et programmables complexes. Cette norme est générique, elle n'est donc pas limitée au secteur des machines.

2. **CEI/EN 62061** « Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité ».

   Cette norme est la version spécifique aux machines de la norme CEI/EN 61508. Elle définit les exigences applicables lors de la conception des systèmes de commande électriques relatifs à la sécurité des machines, et également lors de la conception de sous-systèmes et de dispositifs peu complexes. Elle prescrit que les sous-systèmes complexes ou programmables doivent être conformes à la norme CEI/EN 61508

3. **EN ISO 13849-1:2008** « Sécurité des machines – Parties des systèmes de commande relatives à la sécurité ».

   L'objectif de cette norme est de permettre une méthode de transition des catégories vers la sécurité fonctionnelle.

Les normes sur la sécurité fonctionnelle représentent une évolution significative par rapport aux exigences existantes comme la Fiabilité de commande et le système des catégories de la norme ISO 13849-1:1999 (EN 954-1:1996). Les catégories n'ont pas encore disparu, la norme d'origine reste en vigueur jusqu'en 2010 afin de fournir une période de transition avec sa nouvelle version révisée. Cette nouvelle version de la norme ISO/EN 13849-1 s'appuie sur le concept de sécurité fonctionnelle et introduit une nouvelle terminologie et de nouvelles exigences. Dans la présente section, cette nouvelle version de la norme est appelée EN ISO-13849-1:2008.

L'intérêt pour les normes sur la sécurité fonctionnelle va aller en grandissant parce qu'elles représentent le futur et elles permettent plus de flexibilité, ainsi que l'utilisation d'une nouvelle technologie pour la sécurité des machines.

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

CEI/EN 62061 et EN ISO 13849-1:2008

Les normes CEI/EN 62061 et ISO/EN 13849-1:2008 concernent toutes deux les systèmes de commande électriques relatifs à la sécurité. En définitive, elles seront regroupées comme les deux parties d'une même norme et utiliseront une terminologie commune. Toutes deux permettent d'obtenir les mêmes résultats, mais font appel à des méthodes différentes. Leur objectif est de fournir aux utilisateurs la possibilité de choisir celle qui est la mieux adaptée à leurs situations. Un utilisateur peut décider d'utiliser l'une ou l'autre de ces normes.

Ces deux normes produisent des niveaux de sécurité comparables. Ces méthodes sont en effet adaptées en fonction des utilisateurs auxquels elles sont destinées. Une restriction de la norme EN ISO 13849-1:2008 est indiquée dans le tableau 1 de son introduction. Lorsqu'une technologie programmable et complexe est utilisée, le niveau de performance (PL) maximum pris en considération est PLd.

La méthodologie utilisée dans la norme CEI/EN 62061 a pour objectif de permettre la mise en œuvre de fonctionnalités de sécurité complexes qui peuvent être implémentées par des architectures système non conventionnelles antérieures. L'objectif de la norme ISO 13849-1:2008 est d'offrir une solution plus directe et moins complexe pour les fonctionnalités de sécurité plus conventionnelles implémentées par les architectures système classiques.

L'élément qui différencie le plus ces deux normes se rapporte à leur domaine d'application respectif. La norme CEI/EN 62061 est limitée aux systèmes électriques. La norme EN ISO 13849-1:2008 est applicable aux systèmes pneumatiques, hydrauliques, mécaniques et électriques.

Les présentations suivantes révèlent des similarités sous-jacentes de valeurs et de fondements entre les différentes normes. Il ne s'agit cependant que de brèves présentations. Les deux normes couvrent bien plus de sujets que ce qui est indiqué ici et il est important de prendre en considération l'ensemble des textes des deux normes.

Le tableau suivant fournit un organigramme simplifié pour aider le concepteur de systèmes de sécurité à choisir laquelle de ces deux normes utiliser. Les deux solutions ont des procédures en commun : fonctions de sécurité et évaluation du risque. En ce qui concerne les informations sur la conception du système (p. ex., PFH, MTTF, DC, SFF), les deux normes prennent des approches différentes.

SIL et CEI/EN 62061

La norme CEI/EN 62061 décrit à la fois le niveau de risque à réduire et la capacité d'un système de commande à réduire ce risque en termes de classification SIL (Safety Integrity Level). Il existe 3 niveaux de classification SIL utilisés dans le secteur des machines, le niveau le plus faible est SIL1 et le plus élevé est SIL3.

Des risques plus importants peuvent exister dans d'autres secteurs, comme dans l'industrie des procédés, et c'est pour cette raison que la norme CEI 61508 et la norme CEI 61511

spécifique au secteur des procédés incluent un niveau SIL4. La classification SIL concerne la fonction de sécurité. Le sous-système qui compose le système chargé de la mise en œuvre de la fonction de sécurité doit avoir une capacité SIL appropriée. C'est ce que l'on appelle parfois en anglais SIL Claim Limit (SIL CL). Une étude complète de la norme CEI/EN 62061 est nécessaire avant de pouvoir l'appliquer correctement. Certaines des exigences les plus couramment appliquées de la norme peuvent être résumées ainsi :

PL et EN ISO 13849-1:2008

La norme EN ISO 13849-1:2008 n'utilise pas l'abréviation SIL, mais PL (pour Performance Level, niveau de performance). Les classifications PL et SIL sont comparables à de nombreux égards. Il existe cinq niveaux de performance, PLa est le plus faible et PLe est le plus élevé.

Comparaison de PL et SIL

Ce tableau compare de façon approximative les classifications PL et SIL lorsqu'elle sont appliquées aux structures de circuits typiques de la technologie électromécanique peu complexe.

PL (niveau de performance)	PFH_D (probabilité de panne dangereuse par heure)	SIL (niveau d'intégrité de la sécurité)
A	$\geq 10^{-5}$ to $< 10^{-4}$	Aucun
B	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
C	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
D	$\geq 10^{-7}$ to $< 10^{-6}$	2
E	$\geq 10^{-8}$ to $< 10^{-7}$	3

Correspondance approximative entre PL et SIL

IMPORTANT : *Le tableau précédent est donné uniquement à titre informatif et NE DOIT PAS être utilisé à des fins de conversion. La totalité des exigences des normes doivent être prises en considération.*

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

Conception du système selon la norme CEI/EN 62061

CEI/EN 62061, « Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité », est la version spécifiquement adaptée aux machines de la norme CEI/EN 61508. Elle définit les exigences applicables lors de la conception des systèmes de commande électriques relatifs à la sécurité des machines, et également lors de la conception de sous-systèmes et de dispositifs peu complexes.

L'évaluation du risque débouche sur une stratégie de réduction des risques, qui à son tour permet d'identifier les besoins associés aux fonctions de commande de sécurité. Ces fonctions doivent être décrites et doivent inclure les éléments suivants :

- caractéristiques des exigences fonctionnelles ;
- caractéristiques des exigences d'intégrité de la sécurité.

Les exigences fonctionnelles incluent des détails comme la fréquence de fonctionnement, le temps de réponse requis, les modes de fonctionnement, les cycles de travail, les conditions d'utilisation et les fonctions de réaction aux pannes. Les exigences d'intégrité de la sécurité sont exprimées en différents niveaux appelés niveaux d'intégrité (Integrity Level – SIL). En fonction de la complexité du système, certains des éléments, ou tous les éléments, du tableau ci-dessous doivent être pris en considération pour déterminer si la configuration du système est conforme à la classification SIL nécessaire.

Eléments à prendre en considération pour la classification SIL	**Symbole**
Probabilité de panne dangereuse par heure	PFH_D
Tolérance aux pannes matérielles	HFT
Fraction de pannes sans danger	SFF
Intervalle entre essais de sûreté	T1
Intervalle entre tests de diagnostic	T2
Sensibilité aux pannes d'origine commune	ß
Couverture de diagnostic	DC

Eléments à prendre en considération pour la classification SIL

Pour les systèmes électroniques, le temps représente une cause significative de pannes ; alors que pour les dispositifs électro-mécaniques c'est le nombre d'opérations. Par conséquent, le nombre de pannes pour les systèmes électroniques est exprimé sur une base horaire. Une analyse doit être conduite pour déterminer la probabilité de défaillance. Pour les systèmes de sécurité, plus que la probabilité de pannes, ce qui est important c'est la

probabilité de pannes créant une source de danger sur une base horaire (PFHD). Une fois cette information connue, le tableau peut être utilisé pour déterminer quel niveau SIL est obtenu.

SIL (niveau d'intégrité de la sécurité)	PFH_D (probabilité de panne dangereuse par heure)
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

Probabilité de panne dangereuse en fonction des niveaux SIL

Le système de sécurité est divisé en sous-systèmes. Le niveau d'intégrité de la sécurité du matériel pouvant être invoqué pour un sous-système est limité par la tolérance aux pannes du matériel et par la fraction de panne sans danger du sous-système. La tolérance aux pannes du matériel est la capacité du système à exécuter sa fonction en présence de pannes. Une tolérance égale à zéro signifie que la fonction n'est pas exécutée lorsqu'une panne est présente. Une tolérance aux pannes de un autorise le sous-système à exécuter sa fonction en présence d'une seule panne. La fraction de panne sans danger est la partie du nombre de panne qui n'entraîne pas de panne dangereuse. La combinaison de ces deux éléments est la contrainte architecturale et s'appelle SILCL. Le tableau suivant montre la relation entre la contrainte architecturale et la classification SILCL.

Fraction de panne sans danger (SFF)	Tolérance aux pannes matérielles		
	0	1	2
< 60 %	Non autorisé sauf exception spécifique	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL3
≥ 99 %	SIL3	SIL3	SIL3

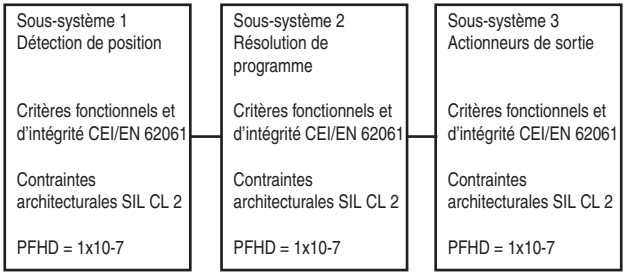
Contraintes architecturales de la classification SIL

Par exemple, une architecture avec une tolérance à une seule panne et une fraction de panne sans danger de 75 % est limitée à un niveau d'intégrité maximum SIL2, quelle que soit la probabilité d'apparition d'une panne dangereuse.

Pour calculer la probabilité de panne dangereuse, chaque fonction de sécurité doit être décomposée en blocs fonctionnels, qui sont ensuite utilisés comme des sous-systèmes. La configuration de nombreuses fonctions de sécurité inclut un capteur connecté à un dispositif

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

logique, lui-même connecté à un actionneur. Ceci crée une disposition en série pour les sous-systèmes. Si nous pouvons déterminer la probabilité de panne dangereuse pour chaque sous-système et si nous connaissons son niveau SILCL, la probabilité de panne du système est facile à calculer en ajoutant la probabilité de panne des sous-systèmes. Ce concept est illustré ci-dessous.



= PFHD 1 + PFHD 2 + PFHD 3
= 1x10-7 + 1x10-7 + 1x10-7
= 3x10-7 c.-à-d., convenant à SIL2

Si, par exemple, nous voulons un niveau d'intégrité SIL2, chaque sous-système doit avoir une limite d'intégrité SIL CL d'au moins SIL2, et la somme des probabilités de panne dangereuse (PFHD) du système ne doit pas dépasser la limite autorisée dans le tableau précédent « Probabilité de panne dangereuse en fonction des niveaux SL ».

Le terme « sous-système » a une signification particulière dans la norme CEI/EN 62061. C'est le premier niveau de sous-division d'un système en sous-parties qui, lorsqu'elles sont défaillantes, entraînent une défaillance de la fonction de sécurité. Par conséquent, si deux interrupteurs redondants sont utilisés dans un système, aucun des interrupteurs n'est un sous-système. Le sous-système inclurait les deux interrupteurs et la fonction de diagnostic des pannes associée (le cas échéant).

Conception de sous-système – CEI/EN 62061

Si un concepteur de système utilise des composants « prêts à l'emploi » dans des sous-systèmes conformes à la définition de la norme CEI/EN 62061, les choses deviennent bien plus faciles parce que les exigences spécifiques à la conception des sous-systèmes ne s'appliquent pas. Ces exigences sont, en général, prises en charge par le fabricant du dispositif (sous-système) et sont bien plus complexes que celles requises pour la conception du système.

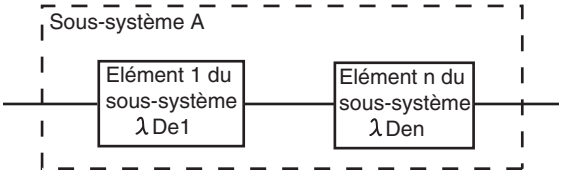
La norme CEI/EN 62061 requiert que les sous-systèmes complexes, comme les PLC de sécurité, se conforment à la norme CEI 61508. Ceci signifie que toute la rigueur de la norme CEI 61508 s'applique aux dispositifs qui utilisent des composants électroniques ou programmables complexes. Ceci peut s'avérer un processus très difficile. Par exemple, l'évaluation de la probabilité de panne dangereuse (PFH_D) réalisée par un sous-système

complexe peut être un processus très compliqué si l'on utilise des techniques comme le modèle de Markov, le schéma fonctionnel de fiabilité ou l'analyse d'arborescence de panne.

La norme CEI/EN 62061 définit des exigences pour la conception de sous-systèmes de moindre complexité. Généralement, cela inclut des composants électriques relativement simples, comme des dispositifs de verrouillage et des relais de surveillance de sécurité électromécaniques. Les exigences ne sont pas aussi complexes que celles de la norme CEI 61508, mais elles peuvent tout de même être très compliquées.

La norme CEI/EN 62061 fournit quatre architectures logiques de sous-système avec les formules associées, qui peuvent être utilisées pour évaluer la probabilité de panne dangereuse (PFHD) obtenue par un sous-système de faible complexité. Ces architectures sont des représentations purement logiques et ne doivent pas pensées comme des architectures physiques. Ces quatre architectures sont illustrées dans les quatre schémas suivants.

Pour une architecture de sous-système basique illustrée ci-dessous, les probabilités de pannes dangereuses sont simplement ajoutées les unes aux autres.



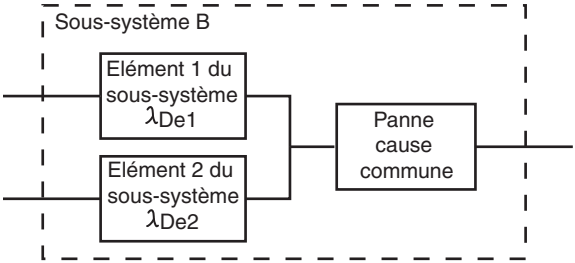
Architecture logique de sous-système A

$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$
$PFH_{DssA} = \lambda_{DssA} \times 1h$

λ, lambda est utilisé pour indiquer le nombre de pannes. L'unité utilisée pour le nombre de pannes est le nombre de pannes par heure. λ_D, lambda indice D est le nombre de pannes dangereuses. λ_{DssA}, lambda indice DssA est le nombre de pannes dangereuses du sous-système A. Lambda indice DssA est la somme des taux de pannes des éléments individuels, e1, e2, e3, jusqu'à et y compris en. La probabilité de panne dangereuse est multiplié par 1 heure pour créer la probabilité de panne en une heure.

Le schéma suivant montre un système tolérant une seule panne sans fonction de diagnostic. Lorsque l'architecture inclut la tolérance d'une seule panne, il existe un potentiel de panne d'origine commune qu'il faut prendre en considération. Le résultat de la panne d'origine commune est brièvement décrit plus loin dans ce chapitre.

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



Architecture logique de sous-système B

$\lambda_{DssB} = (1\text{-}ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2})/2$
$PFH_{DssB} = \lambda_{DssB} \times 1h$

Les formules de cette architecture prennent en considération la disposition en parallèle des éléments du sous-système et ajoutent les deux éléments suivants provenant du tableau précédent « Eléments à prendre en considération pour la classification SIL ».

ß – sensibilité aux pannes d'origine commune (bêta)

T1 – la plus petite valeur de l'intervalle entre essais de sûreté ou de l'autonomie. L'essai de sûreté est conçu pour détecter les pannes et les dégradations du sous-système de sécurité, afin que le sous-système puisse être restauré à son état de fonctionnement.

Prenons les valeurs suivantes comme exemple :

ß = 0,10
$\lambda_{De1} = 1 \times 10^{-6}$ pannes/heure
$\lambda_{De2} = 1 \times 10^{-6}$ pannes/heure
T1 = 87 600 heures (10 ans)

Le taux de panne du système est 1,70956E-07 pannes par heure (SIL2).

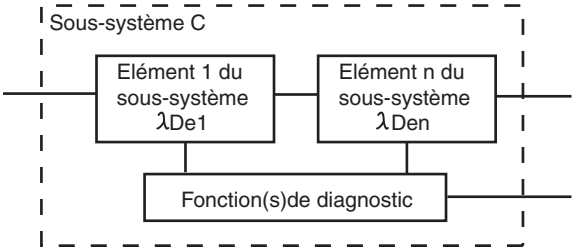
Effet de l'intervalle entre essais de sûreté

Voyons l'effet que l'intervalle entre essais de sûreté a sur le système. Supposons que l'intervalle entre essais de sûreté a été réduit à deux fois par an. Ceci réduit T1 à 4 380 heures et le taux de pannes dangereuses s'améliore pour donner 1,03548E-07 pannes par heure. Ceci n'est toujours que de niveau SIL2. Si l'intervalle entre essais de sûreté est réduit à une fois par mois (730 heures), le taux de pannes dangereuses s'améliore et passe à 1,0059E-07 pannes par heure. Ceci n'est toujours que de niveau SIL2. Il faut encore améliorer le taux de panne, l'intervalle entre essais de sûreté ou la panne d'origine commune pour obtenir un niveau SIL3. De plus, le concepteur doit garder à l'esprit que ce sous-système doit être combiné avec d'autres sous-systèmes pour calculer le nombre total de pannes dangereuses.

Effet de l'analyse des pannes d'origine commune

Voyons l'effet que les pannes d'origine commune ont sur le système. Supposons que nous prenions des mesures supplémentaires et que notre valeur bêta s'améliore à son meilleur niveau de 1 % (0,01), et que l'intervalle entre essais de sûreté reste à 10 ans. Le taux de pannes dangereuses augmente à 9,58568E-08. Le système est maintenant de niveau SIL3.

Le schéma suivant montre la représentation fonctionnelle d'un système ne tolérant aucune panne avec fonction de diagnostic. La couverture de diagnostic est utilisée pour diminuer la probabilité de pannes matérielles dangereuses. Les tests de diagnostic sont réalisé automatiquement. La couverture de diagnostic est le rapport entre le nombre de pannes dangereuses détectées et le nombre de toutes les pannes dangereuses. Le type et le nombre des pannes sans danger n'est pas pris en considération dans le calcul de la couverture de diagnostic ; c'est uniquement le pourcentage de pannes dangereuses détectées.



Architecture logique de sous-système C

$\lambda_{DssC} = \lambda_{De1} (1\text{-}DC_1) + \ldots + \lambda_{Den} (1\text{-}DC_n)$
$PFH_{DssC} = \lambda_{DssC} \times 1h$

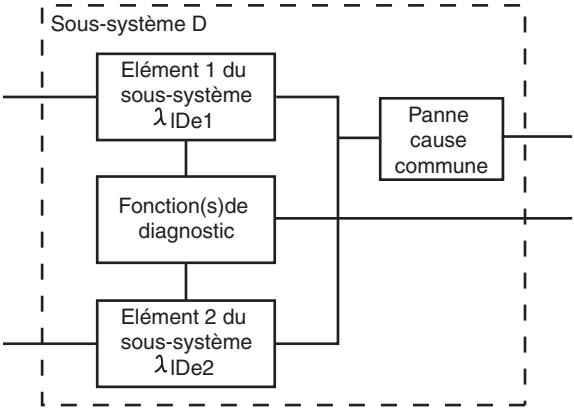
Ces formules incluent la couverture de diagnostic (DC) pour chaque élément de sous-système. Les taux de panne de chaque sous-système sont diminués de la couverture de diagnostic de chaque sous-système.

Ci-dessous se trouve le quatrième exemple d'architecture de sous-système. Ce sous-système tolère une seule panne et inclut une fonction de diagnostic. Le potentiel de panne d'origine commune doit également être pris en considération avec les systèmes tolérant une seule panne.

Si les éléments du sous-système sont identiques, les formules suivantes sont utilisées :

$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De}^2 \times 2 \times DC \times T_2/2 + \lambda_{De}^2 \times (1\text{-}DC) \times T_1 \} + ß \times \lambda_{De}$
$PFH_{DssD} = \lambda_{DssD} \times 1h$

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



Architecture logique de sous-système D

Si les éléments du sous-système sont différents, les formules suivantes sont utilisées :

$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2/2 + \lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \times T_1/2 \} + ß \times (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssD} = \lambda_{DssD} \times 1h$

Remarquez que les deux formules utilisent un paramètre supplémentaire, l'intervalle de diagnostic T2.

Pour exemple, prenons les valeurs suivantes pour l'exemple où les éléments du sous-système sont différents :

ß = 0,10
$\lambda_{De1} = 1 \times 10^{-6}$ pannes/heure
$\lambda_{De2} = 2 \times 10^{-6}$ pannes/heure
T1 = 87 600 heures (10 ans)
T2 = 876 heures
DC1 = 0,8
DC2 = 0,6

PFH_{DssD} = 2,36141E-07 pannes dangereuses par heure

Méthodologies de transition pour les catégories

Au cours de la rédaction de la norme CEI/EN 62061, le comité a pris conscience que toutes les données requises pour les systèmes et les dispositifs ne seraient pas disponibles avant longtemps. Deux tableaux ont été inclus pour faciliter la conversion des concepts de système existants basés sur les catégories d'origine et qui ont prouvé leur efficacité en utilisation. Ils fournissent une équivalence pour la probabilité de panne dangereuse (PFH_D) et les contraintes architecturales. Ces tableaux facilitent la transition vers les norme de sécurité fonctionnelle. Ils ont été légèrement simplifiés dans le présent document. En les étudiant, on constate que les architectures de nombreux exemples du système des catégories donnés dans les chapitres précédents peuvent être réutilisées pour la sécurité fonctionnel.

Catégorie	Tolérance aux pannes	Couverture de diagnostic	PFH_D pouvant être déclaré pour le sous-système
1	0	0 %	Voir CEI/EN 62061
2	0	60 % à 90 %	$\geq 10^{-6}$
3	1	60 % à 90 %	$\geq 2 \times 10^{-7}$
4	> 1	60 % à 90 %	$\geq 3 \times 10^{-8}$
	1	> 90 %	$\geq 3 \times 10^{-8}$

Probabilité de panne dangereuse (PFHD) basée sur les catégories

Le tableau précédent « Contraintes architecturales de la classification SIL », est une version simplifiée du tableau 7 de la norme. Utiliser ce tableau lorsqu'un sous-système basé sur les catégories devient un élément du système de commande de sécurité qui doit se conformer à la norme CEI/EN 62061. Pour plus de simplicité, le concepteur du système de sécurité peut déclarer une valeur PFH_D de 2×10^{-7} pour un système de catégorie 3 qui a une couverture de diagnostic de 60 %. Une solution alternative pour le concepteur du système de sécurité est d'effectuer une analyse complète pour déterminer si une meilleure valeur PFHD peut être déclarée.

Catégorie	Tolérance aux pannes	SFF	Limite SIL maximale selon les contraintes architecturales
1	0	< 60 %	Voir CEI/EN 62061
2	0	60 % à 90 %	SIL1
3	1	< 60 %	SIL1
	1	60 % à 90 %	SIL2
4	> 1	60 % à 90 %	SIL3

Contraintes architecturales des catégories

Le tableau « Probabilité de panne dangereuse (PFHD) basée sur les catégories » peut être utilisé pour déterminer la limite SIL d'un sous-système basé sur les catégories. La couverture de diagnostic du système basé sur les catégories doit être converti en fraction de panne sans danger.

En connaissant les valeurs PFH_D et SIL CL d'un système basé sur les catégories, le concepteur du système de sécurité peut appliquer ces valeurs à l'un des sous-systèmes illustrés antérieurement. Si le système basé sur les catégories est le système de commande de sécurité complet, des valeurs SIL et PFH_D sont déterminées par les tableaux « Contraintes architecturales de la classification SIL » et « Probabilité de panne dangereuse (PFHD) basée sur les catégories ». Le concepteur du système de sécurité doit également se conformer aux exigences de pannes d'origine commune, pannes systématiques et intervalle entre essais de sûreté. Le système de notation des pannes d'origine commune est légèrement différent pour chaque norme. Les concepts d'intégrité de sécurité systématique sont similaires dans les deux normes ; aucune des deux normes n'utilise de système de notation. L'intervalle entre essais de sûreté peut être considéré comme identique au temps de mission, ou un intervalle plus court peut être choisi.

Contraintes architecturales

Le niveau d'intégrité de sécurité qui peut être déclaré pour un système ou sous-système est limité par les caractéristiques architecturales. Les deux caractéristiques principales sont la tolérance aux pannes matérielles et la fraction de panne sans danger. Les caractéristiques secondaires incluent les pannes d'origine commune et l'exclusion de panne.

Lorsque l'on combine les sous-systèmes, le niveau SIL obtenu par le système de commande de sécurité est restreint et doit être inférieur ou égale à la limite SIL la plus basse de n'importe quel sous-système impliqué dans la fonction de commande de sécurité.

B10 et $B10_d$

Pour les sous-systèmes électromécaniques, la probabilité de panne doit être estimée en prenant en considération le nombre de cycles de fonctionnement déclaré par le fabricant, la charge et le cycle de travail. La probabilité de panne est exprimée comme valeur B10, qui est le délai prévisible après lequel 10 % de l'équipement sera défectueux. $B10_d$ est le délai prévisible après lequel 10 % de l'équipement présentera une panne avec danger.

Panne d'origine commune (CCF)

Un panne d'origine commune est un ensemble de pannes qui ont une cause identique et qui génèrent un danger. Les informations sur les pannes d'origine commune sont généralement requises uniquement par le concepteur du sous-système, typiquement le fabricant. Elle est utilisée dans les formules données pour l'estimation de la valeur PFHD d'un sous-système. Elle n'est généralement pas requise pour la conception du système. L'annexe F de la norme CEI/EN 62061 fournit une approche simple pour estimer la valeur CCF. Le tableau suivant montre un résumé du processus de notation.

N°	Mesure contre CCF	Note
1	Séparation/structuration	25
2	Diversité	38
3	Conception/application/expérience	2
4	Evaluation/analyse	18
5	Compétence/formation	4
6	Environnement	18

Notation des mesures contre les pannes d'origine commune

Des points sont attribués pour l'utilisation de mesures spécifiques contre les pannes d'origine commune. Les notes sont additionnées pour déterminer le facteur de panne d'origine commune, qui est indiqué dans le tableau suivant. Le facteur bêta est utilisé dans les modèles de sous-système pour « ajuster » le taux de pannes.

Note globale	Facteur de panne d'origine commune (ß)
< 35	10 % (0,1)
35 – 65	5 % (0,05)
65 – 85	2 % (0,02)
85 – 00	1 % (0,01)

Facteur bêta pour panne d'origine commune

Couverture de diagnostic (DC)

Des tests de diagnostic automatiques sont utilisés pour réduire la probabilité de pannes matérielles dangereuses. Etre capable de détecter 100 % des pannes matérielles dangereuses serait idéal, mais c'est un niveau souvent très difficile à atteindre.

La couverture de diagnostic est le rapport entre les pannes dangereuses détectées et toutes les pannes dangereuses.

$$DC = \frac{\text{Nombre de pannes dangereuses détectées, } \lambda_{DD}}{\text{Nombre total de pannes dangereuses, } \lambda_{DD}}$$

La valeur de la couverture de diagnostic est comprise entre zéro et un.

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

Tolérance aux pannes matérielles

La tolérance aux pannes matérielles représente le nombre de pannes qu'un sous-système peut subir avant de provoquer une panne dangereuse. Par exemple, une tolérance aux pannes matérielles de 1 signifie que 2 pannes peuvent entraîner la perte de la fonction de commande de sécurité, mais pas une seule panne.

Gestion de la sécurité fonctionnelle

La norme définit des exigences pour la commande des activités de gestion et techniques nécessaires pour obtenir un système de commande de sécurité électrique.

Probabilité de panne dangereuse (PFH_D)

Une partie des exigences à mettre en œuvre pour procurer une capacité SIL à un système ou à un sous-système est d'obtenir des données sur la valeur PFH_D (probabilité de panne dangereuse par heure) en raison des pannes matérielles aléatoires.

Ces données sont fournies par le fabricant. Les données pour les composants et les systèmes récents de Rockwell Automation (GuardLogix, GuardPLC, SmartGuard et Kinetix avec GuardMotion, dispositifs de verrouillage, dispositifs d'arrêt d'urgence, etc.) sont déjà disponibles.

La norme CEI/EN 62061 dit également clairement que des manuels de données de fiabilité peuvent être utilisés le cas échéant.

Pour les dispositifs électromécaniques peu complexes, le mécanisme de panne est généralement lié au nombre et à la fréquence des opérations plutôt qu'uniquement au temps. Par conséquent, pour ces composants les données sont dérivées d'une forme de test d'autonomie (p. ex., test B10). B10 est le nombre d'opérations. Les informations basées sur l'application, comme le nombre prévisible d'opérations par an, est alors requis pour convertir les données $B10_d$ ou similaires en valeur $MTTF_d$ (durée moyenne de fonctionnement avant défaillance dangereuse). Ceci est ensuite converti en valeur PFH_D.

En règle générale, on peut supposer l'égalité suivante :

$$PFH_D = 1/MTTF_d$$

Et, pour les dispositifs électromécaniques :

$MTTF_d = B_{10d}/(0{,}1 \times \text{nombre moyen d'opérations par an})$

La formule de la valeur $MTTF_d$ est basée sur l'hypothèse d'un nombre de pannes constant. La répartition cumulée des pannes est $F(t) = 1 - \exp(-\lambda dt)$.

Intervalle entre essais de sûreté

L'intervalle entre essais de sûreté représente le délai après lequel le sous-système doit être soit totalement vérifié ou remplacé pour assurer qu'il est dans un état « comme neuf ». En pratique, dans le secteur des machines, ceci est obtenu par remplacement. L'intervalle entre essais de sûreté est donc généralement la même chose que l'autonomie. La norme EN ISO 13849-1:2008 appelle cela le Temps mission.

Un essai de sûreté est une vérification pouvant détecter les pannes et les dégradations d'un système de commande de sécurité pour que ce système puisse être restauré dans un état aussi proche que possible de son état « comme neuf ». L'essai de sûreté doit détecter 100 % des pannes dangereuses. Les voies séparées doivent être testées séparément.

A l'inverse des tests de diagnostic, qui sont automatiques, les essais de sûreté sont généralement réalisés manuellement et hors ligne. Etant automatiques, les tests de diagnostic sont réalisés souvent, alors que les essais de sûreté sont conduits de façon peu fréquente. Par exemple, les circuits allant vers un dispositif de verrouillage sur une barrière de protection peuvent être testés automatiquement pour détecter les courts-circuits et les circuits ouverts en utilisant un test de diagnostic (p. ex., impulsion).

L'intervalle entre essais de sûreté doit être déclaré par le fabricant. Parfois, le fabricant fournit différents intervalles entre essais de sûreté. L'intervalle entre essais de sûreté approprié est déterminé en évaluant la formule correspondant à l'architecture sélectionnée. En général, plus l'intervalle entre essais de sûreté est court, plus le nombre de pannes est bas.

Fraction de panne sans danger (SFF)

La fraction de panne sans danger est similaire à la couverture de diagnostic mais elle prend également en compte toute tendance inhérente à tomber en panne sans création de danger. Par exemple, lorsqu'un fusible grille, il y a une panne mais il est très probable que la panne sera un circuit ouvert qui, dans la plupart des cas, est une panne « sans danger ». La fraction de panne sans danger est (la somme des pannes « sans danger » plus le nombre de pannes dangereuses détectées) divisé par (la somme de pannes « sans danger » plus le nombre de pannes dangereuses détectées et non détectées). Il est important de comprendre que les seuls types de pannes pris en considération sont ceux qui ont un effet sur la fonction de sécurité.

La plupart des dispositifs mécaniques peu complexes, comme les boutons d'arrêt d'urgence et les dispositifs de verrouillage, ont (par eux-même) une fraction de panne sans danger inférieure à 60 % ; mais la plupart des dispositifs électroniques de sécurité sont conçus avec redondance et surveillance, une fraction supérieure à 90 % est donc habituelle. La valeur SFF est normalement indiquée par le fabricant.

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

La fraction de panne sans danger (SFF) peut être calculée à l'aide de l'équation suivante :

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$$

où

λ_S = le nombre de pannes sans danger

$\Sigma\lambda_S + \Sigma\lambda_D$ = le nombre total de pannes

λ_{DD} = le nombre de pannes dangereuses détectées

λ_D = le nombre de pannes dangereuses

Défaillance systématique

La norme définit des exigences destinées à réguler et éviter les défaillances systématiques. Les défaillances systématiques sont différentes des pannes matérielles aléatoires qui sont des pannes qui se produisent à n'importe quel moment, et qui résultent généralement d'une dégradation de pièces matérielles. Les types les plus courants de défaillance systématique sont les erreurs de conception de logiciel, les erreurs de conception du matériel, les erreurs dans les spécifications exigées et les procédures de fonctionnement. Voici quelques exemples de mesures à prendre pour éviter les défaillances systématiques :

- sélection, combinaison, disposition, assemblage et installation corrects des composants ;
- utilisation de bonnes pratiques d'ingénierie ;
- respect des spécifications et des instructions d'installation du fabricant ;
- assurer la compatibilité entre les composants ;
- résistance aux conditions ambiantes ;
- utilisation des matériaux appropriés.

La norme fournit d'autres exigences plus détaillées nécessaires pour éviter les défaillances systématiques. Elle n'inclut cependant pas de système de notation pour déterminer quel pourcentage des défaillances systématiques potentielles sont couvertes. Pour être conforme aux exigences SIL3, le concepteur doit répondre à toutes les exigences pour éviter les défaillances systématiques. Si toutes les exigences ne sont pas satisfaites, la limite SIL doit être réduite.

Conception du système selon la norme EN ISO 13849-1:2008

Une étude complète de la norme EN ISO 13849-1:2008 est nécessaire avant de pouvoir l'appliquer correctement. Ce qui suit est une brève présentation.

Cette norme définit des exigences pour la conception et l'intégration des pièces de sécurité du système de commande, notamment certains aspects logiciels. Elle s'applique aux systèmes de sécurité mais peut également être appliquée aux composants du système. Cette norme a également un champ d'application très large puisqu'elle concerne toutes les technologies, notamment électricité, hydraulique, pneumatique et mécanique. Bien que la norme ISO 13849-1 s'applique aux systèmes complexes, elle renvoie le lecteur aux normes CEI 62061 et CEI 61508 pour les systèmes logiciels intégrés complexes.

Avec cette norme, l'intégrité de sécurité d'un système est classée selon 5 niveaux de performance (PL). PLa est le niveau le plus faible d'intégrité et PLe est le niveau le plus élevé. Ils sont évalués en prenant les facteurs suivants en considération :

Structure (architecture). Ces facteurs sont directement liés aux catégories décrites précédemment dans ce document.

Temps mission – durée de fonctionnement prévisible
MTTFd – durée moyenne de fonctionnement avant défaillance dangereuse
DC – couverture de diagnostic
CCF – pannes d'origine commune
Comportement en présence d'une panne
Logiciel
Défaillances systématiques
Conditions ambiantes

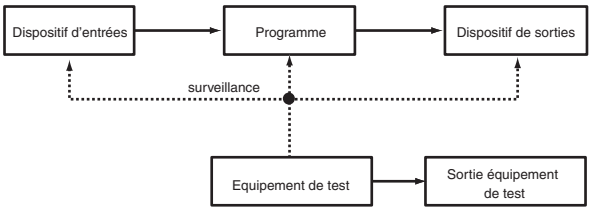
Architectures de système de sécurité (structures)

La norme définit une procédure simplifiée basée sur les catégories pour estimer le niveau de performance (PL). L'objectif de cette approche est de fournir un chemin de transition reconnaissable entre la norme d'origine basée sur les catégories et la version 2006 basée sur les niveaux de performance. La norme définit 5 architectures, comme illustré ci-dessous. Elles correspondent aux 5 catégories B, 1, 2, 3 et 4 existantes. Ces schémas doivent être étudiés attentivement. Ils sont présentés dans l'article 6 de la norme où les exigences, les différences et les hypothèses sont expliquées. Les schémas des architectures des catégories B et 1 et également 3 et 4 peuvent sembler identiques, mais la norme explique en détail les différences en termes d'exigences, notamment la couverture de diagnostic, etc.

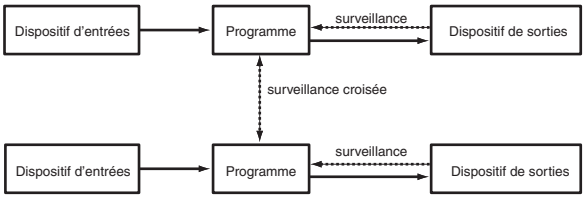
Il est également utile d'étudier les explications sur les catégories données dans ce document qui aborde les catégories en détail avec des exemples pratiques de leur mise en œuvre. Les trois schémas suivants montrent les schémas fonctionnels des 5 architectures de catégories, comme indiquées dans la norme ISO/EN 13849-1.

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

Architecture pour les catégories B et 1



Architecture pour la catégorie 2



Architecture pour les catégories 3 et 4

Temps mission

Le temps mission représente la durée maximale pendant laquelle un sous-système (ou un système) peut être utilisé. A la fin de cette durée, il doit être remplacé. Le temps mission doit être indiqué par le fabricant des composants. Le temps mission est généralement le même que l'« intervalle entre essais de sûreté » utilisé dans la norme CEI/EN 62061. Le concepteur du système de sécurité doit prendre en considération le temps mission des composants afin de déterminer le temps mission de chaque fonction de sécurité.

Durée moyenne de fonctionnement avant défaillance dangereuse ($MTTF_d$)

La durée moyenne de fonctionnement avant défaillance dangereuse ($MTTF_d$) est utilisée directement dans la norme EN ISO 13849-1:2008 dans l'estimation du niveau de performance (PL). La norme propose trois méthodes pour déterminer la valeur $MTTF_d$: 1) utiliser les données du fabricant, 2) utiliser les annexes C et D qui fournissent des taux de pannes pour les composants ou 3) utiliser une valeur par défaut de 10 ans. Choisir la valeur par défaut limite le potée à Moyen, comme le montre le tableau suivant.

Classement MTTFd pour chaque voie	Plage MTTFd pour chaque voie
Faible	3 ans <= MTTFd < 10 ans
Moyen	10 ans <= MTTFd < 30 ans
Elevé	30 ans <= MTTFd < 100 ans

Niveaux de $MTTF_d$

Lorsque le système de sécurité a un lien avec la norme CEI 62061, la valeur $MTTF_d$ doit être convertie en valeur PFH_D. Pour cela, on utilise l'égalité suivante :

$$PFH_D = 1/MTTF_d$$

Et, pour les dispositifs électromécaniques :

$$MTTF_d = B_{10d}/(0{,}1 \times \text{nombre moyen d'opérations par an})$$

Cela est également requis dans certains cas pour déterminer la valeur PFH_D. Elle est fournie par les fabricants. Les valeurs $MTTF_d$ et PFH_D sont généralement dérivées des mêmes données de test ou d'analyse. Pour les dispositifs électromécaniques peu complexes, le mécanisme de panne est généralement lié au nombre et à la fréquence des opérations plutôt qu'uniquement au temps. Par conséquent, pour ces composants les données sont dérivées d'une forme de test d'autonomie (p. ex., test B10). Des informations d'application, comme le nombre prévisible d'opérations par an, sont alors requises pour convertir la valeur $B10_d$, ou des données similaires, en valeur $MTTF_d$.

Couverture de diagnostic (DC)

La couverture de diagnostic (DC) représente l'efficacité de la fonction de surveillance des pannes d'un système ou d'un sous-système. La couverture de diagnostic est le rapport entre le nombre de pannes dangereuses détectées et le nombre de toutes les pannes dangereuses. Les normes EN ISO 13849-1:2008 et CEI 61508 fournissent des tableaux pouvant être utilisés pour déduire la valeur DC et, dans certains cas, cette valeur DC peut être fournie par le fabricants.

Panne d'origine commune (CCF)

Un panne d'origine commune (CCF) est un ensemble de pannes qui ont une cause identique et qui génèrent un danger. Ce sont les pannes de différents éléments, qui résultent d'un même événement. Les pannes ne sont pas des conséquences les unes des autres. L'annexe F de la norme EN ISO 13849-1:2008 fournit une méthode qualitative simplifiée pour déterminer la valeur CCF. Le tableau suivant montre un résumé du processus de notation.

N°	Mesure contre CCF	Note
1	Séparation/structuration	15
2	Diversité	20
3	Conception/application/expérience	20
4	Evaluation/analyse	5
5	Compétence/formation	5
6	Environnement	35

Notation des pannes d'origine commune

Une note d'au moins 65 doit être obtenue pour prétendre à la conformité aux catégories 2, 3 et 4.

Défaillance systématique

Les normes définissent des exigences destinées à réguler et éviter les défaillances systématiques. Les types les plus courants de défaillance systématique sont les erreurs de conception de logiciel, les erreurs de conception du matériel et les erreurs dans les spécifications exigées.

Les défaillances systématiques sont différentes des pannes matérielles aléatoires qui sont des pannes qui se produisent à n'importe quel moment, et qui résultent généralement d'une dégradation de pièces matérielles. L'annexe G de la norme EN ISO 13849-1:2008 décrit des mesures destinées à contrôler et éviter les défaillances systématiques.

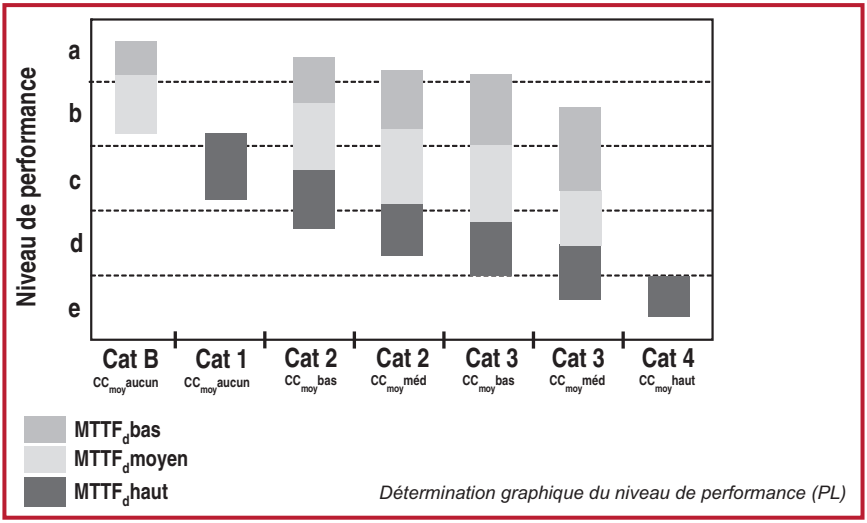
Niveau de performance (PL)

Lorsque les critères de conception du tableau précédent « Niveaux de $MTTD_d$ » sont évalués, un niveau de performance est attribué au système de commande de sécurité. Le niveau de performance est un niveau discret qui définit la capacité des pièces de sécurité du système de commande à exécuter une fonction de sécurité.

Pour évaluer le niveau de performance obtenu par la mise en œuvre de l'une des 5 architectures, les données suivantes sont requises pour le système (ou le sous-système) :

- $MTTF_d$ (durée moyenne de fonctionnement avant défaillance dangereuse de chaque voie)
- DC (couverture de diagnostic)
- Architecture (la catégorie)

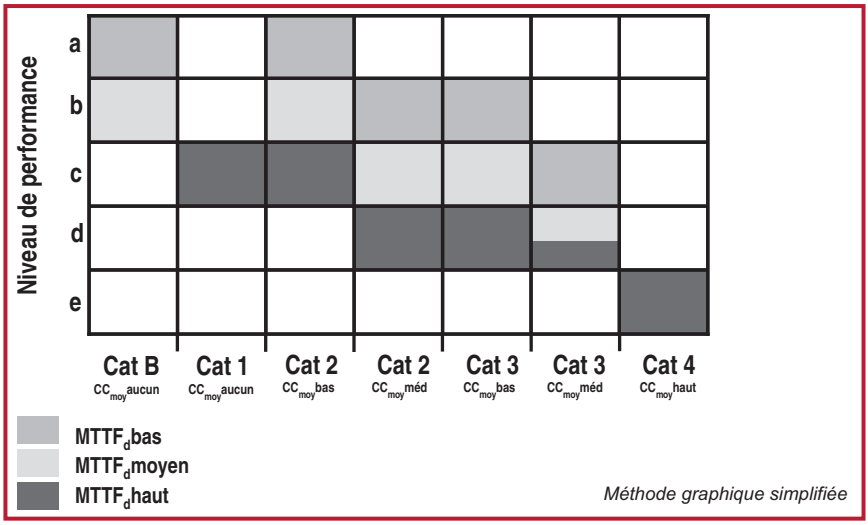
Le schéma suivant présente une méthode graphique pour déterminer le niveau de performance (PL) à partir d'une combinaison de ces facteurs. Le tableau à la fin de cette section montre les résultats tabulaires de différents modèles de Markov qui sont à la base de la création de ce schéma. Consultez le tableau lorsqu'une détermination plus précise est nécessaire.



Détermination graphique du niveau de performance (PL)

Le lecture remarquera qu'il existe un chevauchement au niveau des lignes de séparation des niveaux PL. Si la valeur MTTF n'est donnée qu'en terme de catégorie (comme bas, moyen ou élevé), utilisez le schéma suivant pour déterminer le niveau de performance (PL).

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 exemple, l'application utilise l'architecture de la catégorie 3. Si la couverture de diagnostic (DC) est comprise entre 60 % et 90 %, et que la valeur $MTTF_d$ de chaque voie est comprise entre 10 et 30 ans, alors, selon la figure 10.7, le niveau PLd est obtenu.

D'autres facteurs doivent également être présents pour satisfaire au niveau de performance requis. Ces exigences incluent les prescriptions pour les pannes d'origine commune, les défaillances systématiques, les conditions ambiantes et le temps mission.

Si la valeur PFH_D du système ou du sous-système est connue, le tableau 10.4 (annexe K de la norme) peut être utilisé pour déduire le niveau PL.

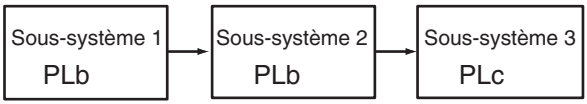
Conception et combinaisons de sous-systèmes

Les sous-systèmes conformes à un niveau de performance peuvent être combinés simplement dans un système en utilisant le tableau 10.3. Les fondements de ce tableau sont clairs. Premièrement, la valeur du système est celle de son sous-système le plus faible. Deuxièmement, plus il y a de sous-systèmes, plus la possibilité de pannes est grande.

PL_{low}	N_{low}	PL
a	> 3	non autorisé
	≤ 3	a
b	> 2	a
	≤ 2	b
c	> 2	b
	≤ 2	c
d	> 3	c
	≤ 3	d
e	> 3	d
	≤ 3	e

Calcul du niveau de performance (PL) pour sous-systèmes combinés en série

Dans le système illustré dans le schéma, les niveaux de performances les plus faibles sont ceux des sous-systèmes 1 et 2. Les deux ont un niveau PLb. Par conséquent, dans le tableau, en suivant la ligne b (dans la colonne PL_{low}), puis la ligne 2 (dans la colonne N_{low}), nous trouvons le niveau de performance obtenu par le système comme étant b (dans la colonne PL). Si les trois sous-systèmes étaient PLb, le PL obtenu serait PLa.



Combinaison de sous-systèmes en série comme système PLb

Validation

La validation jouent un rôle très important dans les processus d'élaboration et de mise en service du système de sécurité. La norme ISO/EN 13849-2:2003 définit les exigences de validation pour les systèmes conçus selon la norme originale ISO 13849-1 (EN 954-1). On prévoit que cette norme sera révisée pour l'aligner avec la norme EN ISO 13849-1:2008. La validation prévue par la norme ISO 13849-2 fait appel à un plan de validation et aborde la validation par le biais de tests et de techniques d'analyse, comme l'analyse de l'arborescence de pannes et les modes de panne, analyse des effets et analyse critique. La plupart de ces exigences s'appliquent au fabricant du sous-système plutôt qu'à l'utilisateur du sous-système.

Mise en service de la machine

Pendant la phase de mise en service du système ou de la machine, la validation des fonctions de sécurité doit être exécutée dans tous les modes de fonctionnement et doit couvrir toutes les situations normales et anormales prévisibles. Les combinaisons d'entrées et de séquences de fonctionnement doivent également être prises en considération. Cette procédure est importante parce qu'il est toujours nécessaire de vérifier que le système est adapté aux caractéristiques de fonctionnement et aux conditions ambiantes réelles.

Certaines de ces caractéristiques peuvent être différentes de celles prévues au moment de la conception.

Exclusion de panne

L'un des principaux outils d'analyse des systèmes de sécurité est l'analyse des pannes. Le concepteur et l'utilisateur doivent comprendre comment le système de sécurité fonctionne en présence de pannes. De nombreuses techniques sont disponibles pour faire cette analyse. Par exemple, l'analyse de l'arborescence des pannes, les modes de pannes, l'analyse des effets et l'analyse critique, l'analyse de l'arborescence des événements et enfin les évaluations de la force de charge.

Au cours de l'analyse, il est possible de découvrir certaines pannes qui ne peuvent pas être détectées par le test de diagnostic automatique sans induire des coûts économiques exagérés. De plus, la probabilité d'apparition de ces pannes peut être rendue extrêmement faible grâce à l'utilisation de méthodes d'atténuation pour la conception, la construction et les tests. Dans ces conditions, les pannes peuvent être ignorées. L'exclusion de pannes consiste à écarter une panne parce que la probabilité d'apparition de cette panne du système de commande de sécurité est négligeable.

La norme EN ISO 13849-1:2008 autorise l'exclusion de pannes sur la base de l'improbabilité technique de son apparition, de l'expérience technique généralement reconnue et des exigences techniques relatives à l'application. La norme ISO 13849-2:2003 fournit des exemples et des justifications pour l'exclusion de certaines pannes des systèmes électriques, pneumatiques, hydrauliques et mécaniques. Les exclusions de pannes doivent être déclarées et justifiées de façon détaillée dans la documentation technique.

L'exclusion de pannes peut conduire à un niveau de performance (PL) très élevé. Des mesures appropriées pour permettre cette exclusion doivent être mises en œuvre tout au long du temps mission. Il n'est pas toujours possible d'évaluer le système de commande de sécurité sans partir du principe que certaines pannes peuvent être exclues. Pour plus d'informations sur l'exclusion de pannes, voir la norme ISO 13849-2.

MTTFd pour chaque voie en années	Probabilité moyenne de panne dangereuse par heure (1/h) et niveau de performance correspondant (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = aucune		DC_{avg} = aucune		DC_{avg} = faible		DC_{avg} = moyenne		DC_{avg} = faible		DC_{avg} = moyenne		DC_{avg} = élevée	
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-5}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-5}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}31 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		

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

MTTFd pour chaque voie en années	Probabilité moyenne de panne dangereuse par heure (1/h) et niveau de performance correspondant (PL)															
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = aucune		DC_{avg} = aucune		DC_{avg} = faible		DC_{avg} = moyenne		DC_{avg} = faible		DC_{avg} = moyenne		DC_{avg} = élevée	
18	$6,34 \times 10^{-6}$	b			$3,68 \times 10^{-6}$	b	$2,37 \times 10^{-6}$	c	$1,41 \times 10^{-6}$	c	$5,67 \times 10^{-7}$	d		
20	$5,71 \times 10^{-6}$	b			$3,26 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,22 \times 10^{-6}$	c	$4,85 \times 10^{-7}$	d		
22	$5,19 \times 10^{-6}$	b			$2,93 \times 10^{-6}$	c	$1,82 \times 10^{-6}$	c	$1,07 \times 10^{-6}$	c	$4,21 \times 10^{-7}$	d		
24	$4,76 \times 10^{-6}$	b			$2,65 \times 10^{-6}$	c	$1,62 \times 10^{-6}$	c	$9,47 \times 10^{-7}$	d	$3,70 \times 10^{-7}$	d		
27	$4,23 \times 10^{-6}$	b			$2,32 \times 10^{-6}$	c	$1,39 \times 10^{-6}$	c	$8,04 \times 10^{-7}$	d	$3,10 \times 10^{-7}$	d		
30			$3,80 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,21 \times 10^{-6}$	c	$6,94 \times 10^{-7}$	d	$2,65 \times 10^{-7}$	d	$9,54 \times 10^{-8}$	e
33			$3,46 \times 10^{-6}$	b	$1,85 \times 10^{-6}$	c	$1,06 \times 10^{-6}$	c	$5,94 \times 10^{-7}$	d	$2,30 \times 10^{-7}$	d	$8,57 \times 10^{-8}$	e
36			$3,17 \times 10^{-6}$	b	$1,67 \times 10^{-6}$	c	$9,39 \times 10^{-7}$	d	$5,16 \times 10^{-7}$	d	$2,01 \times 10^{-7}$	d	$7,77 \times 10^{-8}$	e
39			$2,93 \times 10^{-6}$	c	$1,53 \times 10^{-6}$	c	$8,40 \times 10^{-7}$	d	$4,53 \times 10^{-7}$	d	$1,78 \times 10^{-7}$	d	$7,11 \times 10^{-8}$	e
43			$2,65 \times 10^{-6}$	c	$1,37 \times 10^{-6}$	c	$7,34 \times 10^{-7}$	d	$3,87 \times 10^{-7}$	d	$1,54 \times 10^{-7}$	d	$6,37 \times 10^{-8}$	e
47			$2,43 \times 10^{-6}$	c	$1,24 \times 10^{-6}$	c	$6,49 \times 10^{-7}$	d	$3,35 \times 10^{-7}$	d	$1,34 \times 10^{-7}$	d	$5,76 \times 10^{-8}$	e
51			$2,24 \times 10^{-6}$	c	$1,13 \times 10^{-6}$	c	$5,80 \times 10^{-7}$	d	$2,93 \times 10^{-7}$	d	$1,19 \times 10^{-7}$	d	$5,26 \times 10^{-8}$	e
56			$2,04 \times 10^{-6}$	c	$1,02 \times 10^{-6}$	c	$5,10 \times 10^{-7}$	d	$2,52 \times 10^{-7}$	d	$1,03 \times 10^{-7}$	d	$4,73 \times 10^{-8}$	e
62			$1,84 \times 10^{-6}$	c	$9,06 \times 10^{-7}$	d	$4,43 \times 10^{-7}$	d	$2,13 \times 10^{-7}$	d	$8,84 \times 10^{-8}$	e	$4,22 \times 10^{-8}$	e
68			$1,68 \times 10^{-6}$	c	$8,17 \times 10^{-7}$	d	$3,90 \times 10^{-7}$	d	$1,84 \times 10^{-7}$	d	$7,68 \times 10^{-8}$	e	$3,80 \times 10^{-8}$	e
75			$1,52 \times 10^{-6}$	c	$7,31 \times 10^{-7}$	d	$3,40 \times 10^{-7}$	d	$1,57 \times 10^{-7}$	d	$6,62 \times 10^{-8}$	e	$3,41 \times 10^{-8}$	e
82			$1,39 \times 10^{-6}$	c	$6,61 \times 10^{-7}$	d	$3,01 \times 10^{-7}$	d	$1,35 \times 10^{-7}$	d	$5,79 \times 10^{-8}$	e	$3,08 \times 10^{-8}$	e
91			$1,25 \times 10^{-6}$	c	$5,88 \times 10^{-7}$	d	$2,61 \times 10^{-7}$	d	$1,14 \times 10^{-7}$	d	$4,94 \times 10^{-8}$	e	$2,74 \times 10^{-8}$	e
100			$1,14 \times 10^{-6}$	c	$5,28 \times 10^{-7}$	d	$2,29 \times 10^{-7}$	d	$1,01 \times 10^{-7}$	d	$4,29 \times 10^{-8}$	e	$2,47 \times 10^{-8}$	e

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
Asie Pacifique : Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tél. : +852 2887 4788, Fax : +852 2508 1846

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, 1860, 32e Avenue, Lachine, Québec, H8T 3J7, Tél: +1 (514) 780-5126, Fax: +1 (514) 636-6156, www.rockwellautomation.ca
France : Rockwell Automation SAS – 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
Suisse : Rockwell Automation AG, Buchserstrasse 7, CH-5001 Aarau, Tél.: +41 (62) 889 77 77, Fax: +41 (62) 889 77 11

Publication : SAFEBK-RM002A-FR-P – Février 2009