Switchs Ethernet

Réglementation

Directives et législations européennes

Cette section a pour objectif de servir de guide pour toute personne qui se préoccupe de la sécurité des machines, particulièremnet des systèmes de protection dans l'Union européenne. Elle est destinée aux concepteurs et utilisateurs d'équipements industriels.

Pour promouvoir le concept d'un marché ouvert dans l'Espace économique européen (EEE) (qui comprend tous les états membres de l'UE plus trois autres pays), tous les états membres ont l'obligation de promulguer des lois qui définissent les exigences essentielles de sécurité pour les machines et leur utilisation.

Les machines non conformes à ces exigences ne peuvent pas être commercialisées dans les pays de l'EEE.

Il existe plusieurs directives européennes concernant la sécurité des machines et des équipements industriels, mais les deux les plus pertinentes sont les suivantes :

1. La Directive Machines
2. La directive sur l'utilisation par les travailleurs au travail d'équipements de travail

Ces deux directives sont directement liées puisque les exigences essentielles de santé et de sécurité (EHSR) de la Directive Machines peuvent être utilisées pour confirmer la sécurité de l'équipement utilisé dans la directive sur l'utilisation par les travailleurs au travail d'équipements de travail.

Cette section traite d'aspects de ces deux directives et il est fortement recommandé à toute personne concernée par la conception, la fourniture, l'acquisition ou l'utilisation d'équipements industriels dans l'EEE et dans certains autres pays européens de se familiariser avec ces exigences. La plupart des fournisseurs et utilisateurs de machines ne seront tout simplement pas autorisés à fournir ou à utiliser les machines dans ces pays si elles ne sont pas conformes à ces directives.

Il peut exister d'autres directives européenne pouvant traiter des machines. La plupart d'entre elles sont relativement spécialisées dans leur domaine d'application, elles n'entrent donc pas dans le champ de cette section mais il est important de noter que, le cas échéant, leurs exigences doivent également être respectées. Par exemple, la Directive CEM 2004/108/EC et la Directive ATEX 94/9/EC.

La Directive Machines de l'UE

La Directive Machines traite de la fourniture de nouvelles machines et équipements, notamment les composants de sécurité. Fournir des machines qui ne respectent pas les exigences de la directive dans l'Union européenne constitue une infraction.

La définition la plus large des « machines » donnée dans la directive est la suivante : un « ensemble équipé ou destiné à être équipé d'un système d'entraînement autre que la force humaine ou animale appliquée directement, composé de pièces ou d'organes liés entre eux dont au moins un est mobile et qui sont réunis de façon solidaire en vue d'une application définie ».

Des informations détaillées et des recommandations sur la définition et tous les aspects de la Directive Machines se trouvent sur le site officiel de l'UE :

http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_en.htm

La Directive Machines actuelle (2006/42/EC) a remplacé la version précédente (98/37/EC) fin 2009. Elle clarifie et amende mais n'introduit pas de modifications radicales aux exigences essentielles de santé et de sécurité (EHSR). Elle introduit quelques modifications pour tenir compte des évolutions technologiques et méthodologiques. Elle étend son champ d'application pour couvrir plus de types d'équipements (p. ex., les élévateurs pour site de construction). Il existe désormais une exigence explicite pour une évaluation des risques destinée à déterminer quelles exigences essentielles de santé et de sécurité sont applicables et des modifications ont été apportées aux procédures d'évaluation de la conformité pour les équipements décrit en annexe IV.

Les dispositions clés de la directive originale (98/37/EC) sont entrées en vigueur le 1er janvier 1995 pour les machines et le 1er janvier 1997 pour les composants de sécurité.

Les dispositions de la directive actuelle (2006/42/EC) sont entrées en vigueur le 29 décembre 2009. Il est de la responsabilité du fabricant ou de son représentant agréé de s'assurer que l'équipement fourni est conforme à la directive. Cela inclut :

Figure 1 : Marquage CE sur la machine

- vérifier que les exigences essentielles de santé et de sécurité (EHSR) applicables contenues en annexe I de la directive sont remplies ;
- une fiche technique est préparée ;
- une évaluation appropriée de la conformité est réalisée ;
- une "Déclaration de conformité CE" est fournie ;
- le marquage CE est indiqué ;
- des instructions pour une utilisation sécurisée sont fournies.

Exigences essentielles de santé et de sécurité (EHSR)

L'annexe 1 de la directive donne une liste des exigences essentielles de santé et de sécurité (appelées EHSR) auxquelles les machines doivent se conformer le cas échéant. L'objectif de cette liste est de s'assurer que la machine est sécurisée et qu'elle est conçue et fabriquées de sorte qu'elle puisse être utilisée, réglée et entretenue à toutes les étapes de sa vie, sans mise en danger des personnes. Le texte suivant fournit un aperçu rapide d'exigences typiques, mais il est important de prendre en considération toutes les exigences EHSR données en annexe 1.

Une évaluation des risques doit être réalisée afin de déterminer quelles exigences EHSR concernent l'équipement en question.

Les exigences essentielles de santé et de sécurité en annexe 1 fournissent une hiérarchie de mesures pour éliminer les risques :

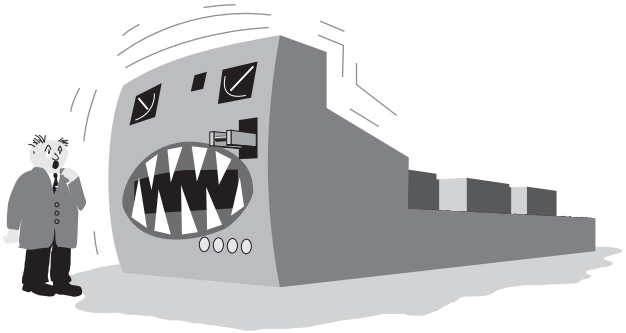


Figure 2 : La machine doit être conforme aux exigences EHSR

(1) Conception à sécurité intrinsèque – La conception elle-même doit si possible permettre d'éviter les dangers.

Lorsque cela n'est pas possible **(2) Des mesures de protection complémentaires** doivent être utilisées, p. ex., des protections avec points d'accès verrouillés, des barrières immatérielles comme des barrières lumineuses, des tapis de détection, etc.

Tout risque résiduel qui ne peut pas être éliminé par les méthodes précédentes doit être limité par l'utilisation de **(3) Equipement de protection individuelle et/ou une Formation**. Le fournisseur de la machine doit spécifier quels méthodes sont appropriées.

Des matériaux adaptés doivent être utilisés pour la construction et le fonctionnement. Un éclairage et des installations adéquates doivent être fournis. Les commandes et les systèmes de commande doivent être sécurisés et fiables. Les machines ne doivent pas pouvoir démarrer de façon imprévue et doivent généralement avoir au moins un dispositif d'arrêt d'urgence. Une attention

particulière doit être donnée aux installations complexes dans lesquelles les processus en amont et en aval peuvent affecter la sécurité d'une machine. La défaillance d'une alimentation ou d'un circuit de commande ne doit pas entraîner de situation dangereuse. Les machines doivent être stables et capables de supporter des contraintes prévisibles. Elles ne doivent pas comporter de bordures ou de surfaces susceptible de provoquer des blessures.

Des barrières ou des dispositifs de protection doivent être utilisés pour protéger des risques, notamment ceux présentés par les pièces mobiles. Ces protections doivent être d'une construction robuste et difficiles à contourner. Des barrières de protection fixes doivent être montées de façon à ce qu'elles ne puissent être retirées qu'avec des outils. Les barrières amovibles doivent être interconnectées. Les barrières réglables doivent être faciles à régler sans outils.

Les dangers dus à l'électricité et à d'autres sources d'énergie doivent être évités Il faut réduire au minimum les risques de blessures dues à la température, aux explosions, au bruit, aux vibrations, à la poussière, aux gaz et aux rayonnements. La maintenance et l'entretien doivent être correctement prévus. Un nombre suffisant de dispositifs de signalisation et d'avertissement doit être fourni. Les machines doivent être fournies avec des instructions permettant une installation, une utilisation, des réglages, etc. en toute sécurité.

La Directive Machines – Evaluation de la conformité et normes

Une norme européenne (EN) harmonisée listée dans le Journal officiel (JO) de l'Union européenne sous la Directive Machines, et dont la date de cessation de présomption de conformité n'a pas expirée, confère un caractère de présomption de conformité à certaines des exigences essentielles de santé et de sécurité (EHSR). (De nombreuses normes récentes listées dans leJO incluent une référence croisée identifiant les EHSR couvertes par la norme).

Par conséquent, lorsque l'équipement doit être conforme à de telles normes européennes harmonisées, l'obligation de démontrer la conformité à ces exigences EHSR est grandement simplifiée, et le fabricant bénéficie également de cette certitude juridique. Ces normes ne sont pas légalement imposées ; cependant, leur respect est fortement recommandé puisque les méthodes alternatives de mise en conformité peuvent être extrêmement complexes. Ces normes soutiennent la Directive Machines et sont produites par le CEN (Commité européen de normalisation) en coopération avec l'ISO et le CENELEC (Comité européen de normalisation électrotechnique) en coopération avec la CEI.

Une évaluation complète et documentées des risques doit être réalisée pour s'assurer que tous les dangers potentiels des machines sont pris en compte. Le fabricant doit s'assurer que toutes les exigences EHSR sont satisfaites, même celles qui ne sont pas couvertes par les normes EN harmonisées.

Fiche technique

Le fabricant ou son représentant doit préparer une fiche technique pour faire la preuve de la conformité avec les exigences essentielles de santé et de sécurité (EHSR). Cette fiche doit inclure toutes les informations pertinentes, comme les résultats de tests, les schémas, les caractéristiques, etc.

Il n'est pas essentiel que toutes les informations soient disponibles en permanences sous forme papier, mais la fiche technique doit pouvoir être mise à disposition en cas d'inspection par une autorité compétente (un organisme mandaté par un pays de l'UE pour vérifier la conformité des machines).

Une fiche technique doit comporter au moins les documents suivants :

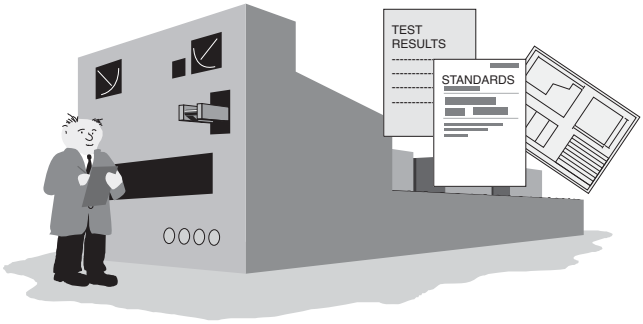


Figure 3 : Résultats des évaluations des documents

1. Schémas généraux de l'équipement, notamment les schémas du circuit de commande.
2. Les schémas détaillés, les calculs, les notes, les résultats de tests, etc. requis pour vérifier la conformité des machines avec les EHSR.
3. La documentation sur l'évaluation des risques, notamment une liste des exigences essentielles sur la santé et la sécurité auquelles sont soumises les machines et une description des mesures de protection mises en place.
4. Une liste des normes et autres caractéristiques techniques utilisées, indiquant les exigences essentielles de santé et de sécurité couvertes.
5. Une description des méthodes adoptées pour éliminer les dangers que présentent les machines.
6. Le cas échéant, tout rapport technique ou certificat obtenu auprès d'un laboratoire de test ou de tout autre organisme.
7. Si la conformité avec une norme européenne harmonisée est reconnue, tout rapport technique indiquant les résultats des tests correspondants.
8. Une copie des notices des machines.
9. Le cas échéant, la déclaration d'incorporation pour les machines partiellement complétées incluses et les notices d'assemblages correspondant à ces machines.
10. Le cas échéant, des copies de la déclaration de conformité CE des machines ou d'autres produits intégrés aux machines.
11. Une copie de la déclaration de conformité CE.

Pour la fabrication en série, les détails des mesures internes (systèmes de contrôle qualité, par exemple) utilisées pour assurer que toutes les machines produites sont conformes :

- Le fabricant doit réaliser les recherches ou les tests nécessaires sur les composants, les accessoires ou sur les machines complètes afin de déterminer si sa conception et sa construction lui permettent d'être installée et utilisée en toute sécurité.
- La fiche technique n'a pas besoin d'exister en tant que fichier individuel permanent, mais il doit être possible de regrouper tous les documents la composant pour la mettre à disposition dans un délai raisonnable. Elle doit être disponible pendant dix ans après la production de la dernière unité.

La fiche technique n'a pas besoin d'inclure des plans détaillés ou d'autres informations spécifiques sur les sous-ensembles utilisés pour la fabrication de la machine, sauf s'ils sont essentiels pour vérifier la conformité aux EHSR.

Evaluation de la conformité

Certains types d'équipements sont soumis à des mesures spéciales. Cet équipement est listé dans l'annexe IV de la directive et inclut des machines dangereuses, comme certaines machines à bois, presses, machines de moulage par injection, équipement souterain, systèmes de levage pour véhicules, etc.

L'annexe IV inclut également certains composants de sécurité comme les appareils de protection destinés à détecter la présence d'une personne (p. ex. les barrières immatérielles) et les unités logiques pour assurer les fonctions de sécurité.

Réglementations

Figure 4 : Evaluations de la conformité

Pour les machines décrites dans l'annexe IV qui ne sont pas totalement conformes avec les normes européennes harmonisées concernées, le fabricant ou son représentant agréé doit mettre en œuvre une des procédures suivantes :

1. **Examen de type CE**. Une fiche technique doit être préparée et un exemplaire de la machine doit être soumis à un organisme notifié (laboratoire de test) pour subir un examen de type CE. Si elle réussit les tests, la machine reçoit un certification d'examen de type CE. La validité du certificat doit être réévaluée tous les cinq ans par l'organisme notifié.
2. **Assurance qualité complète**. Une fiche technique doit être préparée et le fabricant doit avoir un système d'assurance de la qualité agréé pour la conception, la fabrication, l'inspection finale et les tests. Le système de contrôle qualité doit assurer la conformité de la machine avec les dispositions de cette directive. Ce système de qualité doit être évalué périodiquement par un organisme notifié.

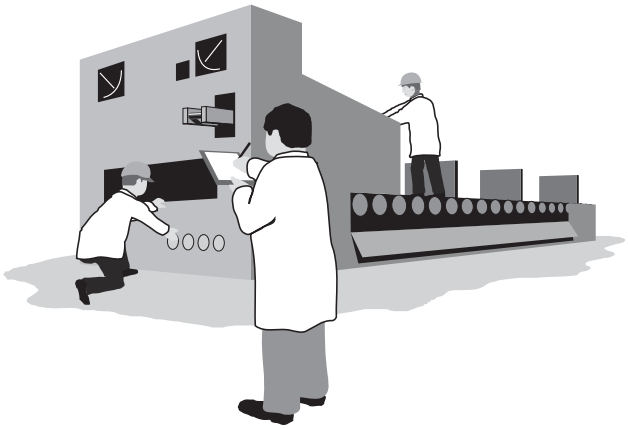


Figure 5 : Evaluations par un organisme notifié

Pour les machines qui ne sont pas incluses dans l'annexe IV ou pour les machines inlusent dans cette annexe mais qui sont totalement conformes aux normes européennes harmonisées concernées, le fabricant ou son représentant agréé peut également préparer la fiche technique et faire une auto évaluation et déclarer la conformité de l'équipement. Il doit y avoir des vérifications internes pour s'assurer que l'équipement fabriqué reste conforme.

Organismes notifiés

Un réseau d'organismes notifiés qui communiquent entre eux et travaillent sur des critères communs existe dans toute l'UE. Les organismes notifiés sont mandatés par les gouvernements (pas par l'industrie) et les informations concernant ces organismes peuvent être obtenues sur le site :
http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_en.htm

Procédure de déclaration de conformité CE

Le marquage CE doit être inscrit sur toutes les machines fournies. Les machines doivent également être fournies avec une Déclaration de conformité CE.

CE

Figure 6 : Marquage CE

Le marquage CE indique que la machine est conforme à toutes les directives européennes en vigueur et que les procédures d'évaluation de la conformité appropriées ont été réalisées. L'application du marquage CE pour la Directive Machines sur des machines qui ne sont pas conformes aux EHSR constitue une infraction.

La Déclaration de conformité CE doit contenir les informations suivantes :

- nom et adresse complète professionnelle du fabricant et, le cas échéant, le représentant agréé ;
- nom et adresse de la personne autorisée à compiler la fiche technique, qui doit être établi dans la Communauté (dans le cas d'un fabricant se trouvant hors de l'UE, cela peut être le « représentant agréé ») ;
- description et identification des machines, notamment la dénomination générique, la fonction, le modèle, le type, le numéro de série et le nom commercial ;
- une déclaration indiquant clairement que la machine remplit toutes les conditions pertinentes de cette directive et, le cas échéant, une déclaration similaire indiquant la conformité avec d'autres directives et/ou les dispositions pertinentes avec lesquelles la machine est conforme ;
- le cas échéant, une référence aux normes harmonisées utilisées ;
- le cas échéant, une référence aux autres normes et spécifications techniques utilisées ;
- (pour les machines soumises à l'annexe IV) le cas échéant, le nom, l'adresse et le numéro d'identification de l'organisme notifié qui a réalisé l'examen de type CE dont il est fait référence en annexe IX et le numéro du certificat d'examen de type CE ;
- (pour les machines soumises à l'annexe IV) le cas échéant, le nom, l'adresse et le numéro d'identification de l'organisme notifié qui a approuvé le système d'assurance de la qualité dont il est fait référence en annexe X ;
- le lieu et la date de la déclaration ;
- l'identité et la signature de la personne habilitée à établir la déclaration au nom du fabricant ou de son représentant agréé.

Déclaration d'intégration pour les quasi-machines CE

Lorsque l'équipement est fourni pour être assemblé avec d'autres composants afin de former une machine complète par la suite, une DECLARATION D'INTEGRATION doit être fournie avec. Le marquage CE ne doit pas être appliqué. La déclaration doit signaler que l'équipement ne doit pas être mis en service avant que la machine dans laquelle il a été incorporé a été déclarée conforme. Une fiche technique doit être préparée et la quasi-machine doit être fournie avec une documentation contenant une description des conditions devant être remplies pour l'incorporation correcte dans la machine finale, afin de ne pas compromettre la sécurité.

Cette option n'est pas disponible pour l'équipement pouvant fonctionner de façon autonome ou qui modifie le fonctionnement d'une machine.

La Déclaration d'intégration doit contenir les informations suivantes :

- nom et adresse complète professionnelle du fabricant de la quasit-machine et, le cas échéant, le représentant agréé ;
- nom et adresse de la personne autorisée à compiler la documentation technique pertinente, qui doit être établi dans la Communauté (dans le cas d'un fabricant se trouvant hors de l'UE, cela peut être le « représentant agréé ») ;
- description et identification des quasi-machines, notamment la dénomination générique, la fonction, le modèle, le type, le numéro de série et le nom commercial ;
- phrase indiquant quelles exigences essentielles de cette directive sont remplies et que la documentation technique pertinente est compilée conformément à la partie B de l'annexe VII, et, le cas échéant, une phrase indiquant la conformité des quasi-machines avec les directives en vigueur ;
- engagement à transmettre les informations pertinentes concernant les quasi-machines en réponse à une demande motivée de la part des autorités nationales ; Ceci doit inclure la méthode de transmission et doit se faire sans préjudice quant aux droits de propriété intellectuelle du fabricant de la quasi-machine ;
- déclaration indiquant que la quasi-machine ne doit pas être mise en service avant que la machine finale dans laquelle elle doit être intégreé n'ait été déclarée conforme aux dispositions de cette directive, le cas échéant ;
- le lieu et la date de la déclaration ;
- l'identité et la signature de la personne habilitée à établir la déclaration au nom du fabricant ou de son représentant agréé.

Machines ne provenant pas de l'UE – Représentants agréés

Si un fabricant situé en dehors de l'UE (ou de l'EEE) importe des machines dans l'UE, il doit mandater un représentant agréé.

Un représentant agréé est une personne physique ou juridique établie dans la Communauté européenne et qui a reçu un mandat écrit de la part du fabricant pour réaliser en son nom tout ou partie des obligations et formalités liées à la Directive Machines.

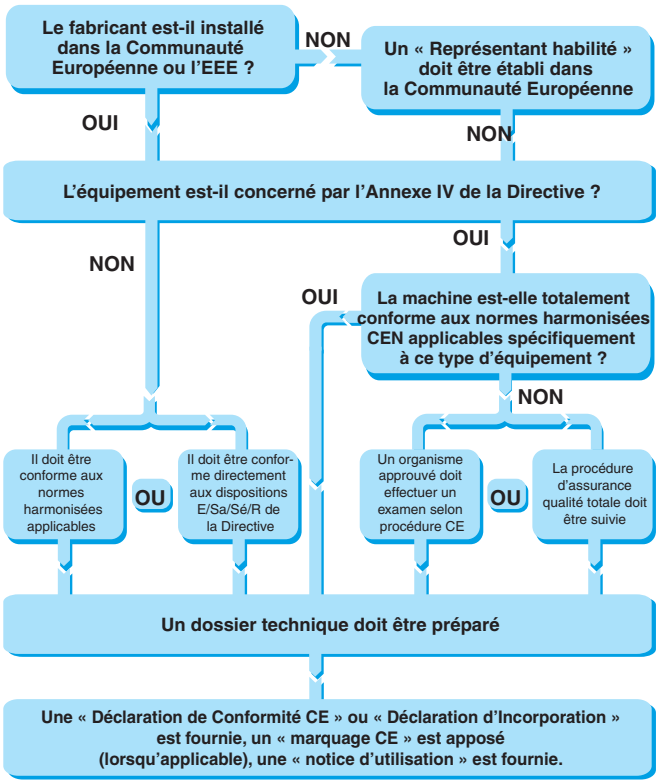


Figure 7 : Présentation des procédures pour la Directive Machines

Il est important d'étudier la directive (2006/42/CE) pour connaître tous les détails.

La directive européenne relative à l'utilisation d'équipements de travail (directive U.W.E.)

Alors que la Directive Machines est destinée aux fournisseurs, cette directive (89/655/CEE amandée par 95/63/CE, 2001/45/CRE et 2007/30/CE) est destinée aux utilisateurs des machines. Elle couvre tous les secteurs industriels et elle met les obligations générales du côté de l'employeur avec les exigences minimales pour la sécurité des équipements de travail. Tous les pays de l'UE promulguent leurs propres lois pour l'application de cette directive.

Par exemple, elle est appliquée au Royaume Uni sous le nom « The Provision and Use of Work Equipment Regulations » (souvent abrégé en P.U.W.E.R.). La mise en œuvre peut variée d'un pays à l'autre, mais l'objectif de la direcive reste inchangé.

Les articles de la directive décrivent en détail quels types d'équipements et de postes de travail sont courverts par la directive.

Ils rendent également les employeurs responsables des obligations générales, telles que la mise en place de systèmes de sécurité et la fourniture d'équipements adapatés et sécurisés correctement entretenus. Les opérateurs des machines doivent être correctement informés et formés sur l'utilisation sécuritaire des machines.

Les nouvelles machines (et les machines de seconde main dont la provenance se situe hors de l'UE) fournies après le 1er janvier 1993 doivent satisfaire à toutes les directives produits pertinentes ; p. ex., la Directive Machines(sous réserve d'arrangement transitoire). Les équipements de seconde main dont la provenance se situe dans l'UE fournies pour la première fois dans le lieu de travail doivent immédiatement se conformer aux exigences minimales indiquées dans l'annexe de la directive U.W.E.

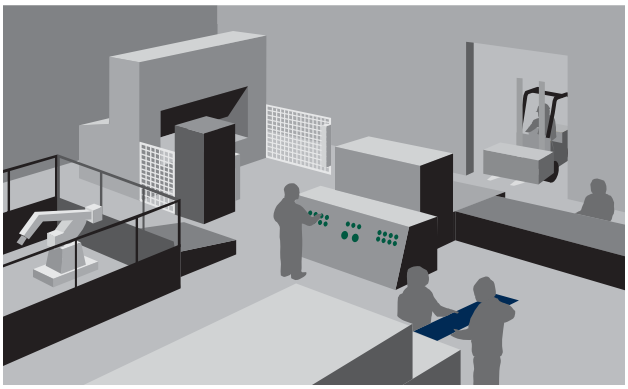


Figure 8 : La directive couvre l'utilisation des équipements

Remarque : les machines existantes ou de seconde main largement révisées ou modifiées sont classées comme nouvel équipement, le travail effectué dessus doit donc permettre la conformité avec la Directive Machines (même si c'est pour une utilisation par l'entreprise elle-même).

L'adéquation de l'équipement de travail est une exigence importante de la directive et elle souligne l'obligation faite à l'employeur de réaliser une évaluation des risques appropriée.

L'une des exigences est que les machines soient entretenues de façon adéquate. Cela signifie généralement qu'il doit y exister un calendrier de maintenance préventive planifié. Il est recommandé qu'un journal soit compilé et tenu à jour. Cela est particulièrement important dans les cas où la maintenance et l'inspection des équipements contribue à l'intégrité de la sécurité d'un dispositif ou d'un système de protection.

L'annexe de la directive U.W.E. décrit des exigences générales minimum pour les équipements de travail.

Si l'équipement est conforme aux directives produits pertinentes, p. ex. la Directive Machines, ils sont automatiquement conformes avec les exigences correspondantes sur la conception des machines indiquées dans les exigences minimales de l'annexe.

Les pays membres sont autorisés à promulguer des lois portant sur l'utilisation de l'équipement de travail qui vont au-delà des exigences minimales de la directive U.W.E.

De plus amples informations sur la directive relative à l'utilisation d'équipements de travail peuvent être obtenues sur le site Internet officiel de l'UE :
http://europa.eu/legislation_summaries/employment_and_social_policy/health_hygiene_safety_at_work/c11116_en.htm

Réglementations U.S.

Cette section présente certaines des réglementations de sécurité américaines pour la protection des machines industrielles. Il ne s'agit que d'un point de départ, le lecteur doit faire une recherche plus approfondie sur les exigences relatives son application spécifique et il doit prendre des mesures afin de s'assurer que sa conception, son utilisation, ses procédures de maintenance correspondent à la fois à ses propres besoins et aux réglementations et codes locaux et internationaux.

Il existe de nombreuses organisations qui font la promotion de la sécurité industrielle aux Etats-Unis. Notamment :

1. les sociétés, qui s'appuient sur des exigences établies et définissent leurs propres exigences internes ;
2. l'Occupational Safety and Health Administration (OSHA) ;
3. les organismes industriels comme la National Fire Protection Association (NFPA), la Robotics Industries Association (RIA), l'Association of Manufacturing Technology (AMT) et les fournisseurs de produits et solutions de sécurité, comme Rockwell Automation.

Occupational Safety and Health Administration

Aux Etats-Unis, l'un des moteurs de la sécurité est l'Occupational Safety and Health Administration (OSHA). L'OSHA a été créée en 1970 par une loi du Congrés américain. L'objectif de cette loi est de créer des conditions de travail à la fois saines et sécuritaires, et de protéger le personnel. Cette loi autorise le Ministère du travail à définir des normes obligatoires relatives à la sécurité et la santé au travail applicables aux entreprises impliquées dans le commerce inter-états. Cette loi s'applique au travail effectuer sur un lieu de travail situé dans un Etat, le district de Columbia, l'Etat libre de Porto Rico, les îles Vierges, Samoa américaine, l'île de Guam, le Territoire sous tutelle des îles du Pacifique, l'île de Wake, les terres du plateau continental extérieur définies dans la loi Outer Continental Shelf Lands Act, l'île Johnston et la zone du canal de Panama.

L'article 5 de la Loi définit les exigences de base. Chaque employeur doit fournir à chacun de ses employés un travail et un lieu de travail exempts de dangers connus pouvant provoquer le décès ou des blessures physiques sérieuses et doit se conformer aux normes relatives à la sécurité et la santé au travail promulguées dans cette Loi.

L'article 5 indique également que chaque employé doit se conformer aux normes relatives à la sécurité et la santé au travail et à toutes les règles, réglementations et ordres émis en vertu de cette Loi qui s'appliquent à ses propres actions et conduite.

La loi OSHA place la responsabilité sur l'employeur et sur l'employé. Ceci diffère significativement de la Directive Machines, qui impose aux fournisseurs de mettre sur le marché des machines exemptes de dangers. Aux Etats-Unis, un fournisseur peut vendre une machine sans aucun dispositif de protection. C'est à l'utilisateur d'ajouter les dispositifs de protection pour sécuriser la machine. Bien que cette pratique ait été courante lorsque la Loi a été approuvée, la tendance est désormais à ce que les fournisseurs proposent des machines avec des dispositifs de protection, ceci parce que l'intégration de la sécurité dès la conception de la machine est bien plus économique que son ajout après sa conception et sa fabrication. Les normes tentent désormais de favoriser la communication entre fournisseur et utilisateur sur les impératifs de protection afin de rendre les machines plus sûres mais également plus productives.

Le Ministère du travail est compétent pour promulguer une norme relative à la sécurité ou la santé au travail à partir d'une norme consensuelle, et de toute norme fédérale établie, sauf si la promulgation d'une telle norme n'aboutissait pas à une amélioration de la sécurité ou de la santé pour le personnel spécifiquement ciblé.

L'OSHA accomplit cette tâche par la plublication de normes dans le titre 29 dans le Code of Federal Regulation (29 CFR). Les normes relatives aux machines industrielles sont publiées par l'OSHA dans le Partie 1910 du titre 29 CFR. Elles sont accessibles librement sur le site Internet de l'OSHA : www.osha.gov. Contraiement à la plupart des normes, qui sont facultatives, les normes OSHA ont force de loi.

Certaines des parties importantes relatives à la sécurité des machines sont les suivantes :

A Généralités
B Adoption et extension des normes fédérales établies
C Dispositions générales sur la sécurité et la santé
H Matériaux dangereux
I Equipement de protection individuelle
J Dispositifs de contrôle de l'environnement – notamment condamnation/signalisation
O Machines et protection des machines
R Industries spéciales
S Electrique

Certaines normes OSHA renvoient à des normes facultatives. La conséquence juridique de l'incorporation par renvoi est que le matériel est traité comme s'il était entièrement publié dans le Federal Register. Lorsqu'une normes consensuelle nationale est incorporée par renvoi dans l'une des sous-parties, cette norme a force de loi. Par exemple, NFPA 70, une norme facultative connu sour le nom de US National Electric Code, est référencée dans la sous-partie S. Cela rend les exigences de la norme NFPA70 obligatoires.

29 CFR 1910.147, dans la sous-partie J, couvre la gestion des sources d'énergie présentant un danger. Ceci est généralement connu sous le nom de condamnation/signalisation (lockout/tagout). La normes fabultative équivalente est ANSI Z244.1. En résumé, cette norme impose que l'alimentation de la machine soit condamnée pour permettre l'entretien ou la maintenance. L'objectif est d'éviter la mise sous tension ou le démarrage imprévu de la machine, ce qui entraînerait des blessures corporelles.

Les employeurs doivent mettre en place un programme et des procédures afin d'installer des dispositifs de condamnation ou de signalisation appropriés sur les dispositifs d'isolation de l'alimentation, et de désactiver les machines ou l'équipement pour éviter la mise sous tension, le démarrage ou la libération d'énergie stockée de façon imprévue afin de prévenir les blessures corporelles.

Les réglages et les changements d'outils mineurs, et autres activités d'entretien mineures, qui se font pendant les opérations de production normales, ne sont pas couvertes par cette norme s'il s'agit d'activités de routine, répétitives et inhérentes à l'utilisation de l'équipement dans le cours normal de la production ; si toutefois ces activités sont effectuées à l'aide de mesures alternatives qui fournissent une protection adéquate. Par mesures alternatives, on entend des dispositifs de protection comme les barrières immatérielles, les tapis de sécurité, les dispositifs de verrouillage de porte et autres dispositifs similaires raccordés à un système de sécurité. Le défi pour le concepteur et pour l'utilisateur de la machine est de définir ce qui est « mineur » et ce qui est « routine, répétitif et inhérent ».

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

La norme 1910.212 est une norme OSHA générale pour les machines. Elle indique qu'une ou plusieurs méthodes de protection des machines doit être fournie afin de protéger l'opérateur et les autres personnes des dangers aux abords de la machine, par exemples les dangers présentés par le poste de travail, le point de pression, les pièces rotatives, les débris volants et les étincelles. Des protections doivent être installées sur la machine lorsque c'est possible et à un autre endroit lorsque cela n'est pas possible. La protection doit être telle qu'elle même ne présente pas un danger.

Le « poste de travail » est la zone de la machine où le travail est effectivement réalisé sur le matériau à traiter. Le poste de travail d'une machine, dont le fonctionnement expose un employé à un risque de blessure, doit être protégé. Le dispositif de protection doit être conforme au normes appropriées ou, en l'absence de normes spécifiques applicables, doit être conçu et fabriqué de sorte à empêcher qu'une partie du corps de l'opérateur puisse se trouver dans la zone dangereuse pendant le cycle de fonctionnement.

La sous-partie S (1910.399) définit les exigences électriques de l'OSHA. Une installation ou un équipement est acceptable par le sous-secrétariat du Ministère du travail, et approuvé dans le cadre de la définition de cette sous-partie S, si il ou elle est accepté, certifié, listé, étiqueté ou défini comme sécurisé de toute autre façon par un laboratoire d'essai agréé (NRTL).

Qu'est-ce qu'un équipement ? Il s'agit d'un terme générique qui inclut le matériel, les accessoires, les dispositifs, les appareils, les supports et autres éléments semblables utilisés comme composants, ou de façon connexe, d'une installation électrique.

Que signifie « listé » ? L'équipement est « listé » s'il fait partie d'un type mentioné dans une liste qui, (a) est publiée par un laboratoire agréé qui réalise des inspections périodiques de la production de cette équipement, et (b) indique que cet équipement est conforme aux normes nationales ou qu'il a réussi des tests prouvant qu'il est sécuritaire pour une utilisation particulière.

Depuis août 2009, les entreprises suivantes sont reconnues par l'OSHA comme étant des NRTL :
Association canadienne de normalisation (CSA)
Communication Certification Laboratory, Inc. (CCL)
Curtis-Straus LLC (CSL)
FM Approvals 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)
TÜV America, Inc. (TÜVAM)
TÜV Product Services GmbH (TÜVPSG)
TÜV Rheinland of North America, Inc. (TÜV)
Underwriters Laboratories Inc. (UL)
Wyle Laboratories, Inc. (WL)

Certains états ont adopté leurs propres normes OSHA. Vingt-quatre états, Puerto Rico et les îles Vierges possèdent des programmes d'état approuvés par l'OSHA et ont adopté leurs propres normes et règles d'application. Pour la plupart, ces états adoptent des normes identiques à celles de l'OSHA au niveau fédéral. Cependant, certains états ont adopté différentes normes relatives à ce sujet ou peuvent avoir différentes règles d'application.

Les employeurs doivent signaler les incidents à l'OSHA. L'OSHA compile les taux d'incidents, transmet ces informations à des bureaux locaux et les utilisent pour établir des priorités d'inspection. Les facteurs clés pour les inspections sont les suivants :

- Danger imminent
- Catastrophes et victimes
- Plaintes des employés
- Industries à haut risque
- Inspections locales planifiées
- Inspections de suivi
- Programmes nationaux et locaux

Les infractions aux normes OSHA peuvent entraîner des amendes. La classification de ces amendes est la suivante :

- Grave : jusqu'à 7 000 $ par infraction
- Autre que grave : discrétionnaire, mais inférieure à 7 000 $
- Répétitive : jusqu'à 70,000 $ par infraction
- Intentionnelle : jusqu'à 70,000 $ par infraction
- Infractions entraînant la mort : sanctions supplémentaires
- Non mise en conformité : 7 000 $/jour

Le tableau ci-dessous montre les 14 principales contraventions OSHA entre octobre 2004 et septembre 2005.

Norme	Description
1910.147	Contrôle de l'énergie dangereuse (condamnation/signalisation)
1910.1200	Communication relative au danger
1910.212	Prescriptions générales pour toutes les machines
1910.134	Protection respiratoire
1910.305	Méthodes, composants et équipement de câblage à usage général
1910.178	Chariots de manutention électriques
1910.219	Transmission mécanique de puissance
1910.303	Prescriptions générales
1910.213	Machines à bois
19102.215	Machines à meule abrasive
19102.132	Prescriptions générales
1910.217	Presses mécaniques
1910.095	Exposition au bruit dans le travail
1910.023	Protection des ouvertures et trous dans les sols et les murs

Tableau 1

Réglementations canadiennes

Au Canada, la sécurité industrielle est administrée au niveau provincial. Chaque province possède ses propres réglementations. Par exemple, l'Ontario a créé la Loi sur la santé et la sécurité au travail, qui définit les droits et les obligations de toutes les parties sur le lieu de travail. Son objectif principal est de protéger les travailleurs contre les risques pour la santé et la sécurité au travail. Cette loi définit les procédures de gestion des dangers au travail, ainsi que les dipositions d'application de la loi lorsque ses prescriptions ne sont pas appliquées volontairement.

La Loi contient le réglement 851, article 7, qui définit l'évaluation de la santé et la sécurité pré-démarrage. Cette évaluation est obligatoire en Ontario pour toute machine, qu'elle soit nouvelle, reconditionnée ou modifiée, et un rapport doit être généré par un ingénieur professionnel.

Introduction

Cette section fournit une liste de certaines des normes internationales et nationales relatives à la sécurité des machines. Il ne s'agit cependant pas d'une liste exhaustive mais d'un aperçu des enjeux sur la sécurité des machines qui font l'objet d'une normalisation.

Cette section doit être lue conjointement avec la section sur les réglementations.

Tous les pays du monde travaillent à une harmonization internationale des normes. Ceci est particulièrement évident dans le domaine de la sécurité des machines. Les normes de sécurité internationales sont gouvernées par deux organismes : ISO et CEI. Des normes régionales et nationales sont encore en vigueur et continuent à soutenir les obligations locales, mais de nombreux pays se tournent vers l'utilisation des normes internationales produites par l'ISO et la CEI.

Par exemple, les normes EN (normes européenne) sont utilisées dans tous les pays de l'EEE. Toutes les nouvelles normes EN sont alignées sur les normes ISO et CEI et, dans la plupart des cas, leur texte est identique.

La CEI s'occupe des questions électrotechniques et l'ISO aborde les autres questions. La plupart des pays industrialisés sont membre de la CEI et de l'ISO. Les normes relatives à la sécurité des machines sont écrites par des groupes de travail regroupant des experts provenant de la plupart des pays industrialisés.

Dans la plupart des pays, les normes peuvent être considérées comme facultatives, alors que les réglementations constituent des obligations légales. Cependant, les normes sont généralement utilisées comme une interprétation pratique des réglementations. Les domaines des normes et des réglementations sont donc étroitement liés.

ISO (Organisation internationale de normalisation)

L'ISO est une organisation non gouvernementale regroupant les organismes de normalisations nationaux de la plupart des pays du monde (157 pays au moment de la mise sous presse). Un Secrétariat central, situé à Genève en Suisse, coordonne le système. L'ISO définit des normes relatives à la conception, la fabrication et l'utilisation de machines plus efficaces, plus sûres et plus propres. Les normes facilitent également des échanges plus équilibrés entre pays.

Les normes ISO sont identifiables grâce aux trois lettres ISO.

Les normes ISO relatives aux machines sont organisées de la même façon que les normes EN, en trois niveaux : Types A, B et C (voir la section sur les normes européennes harminisées).

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

CEI (Commission électrotechnique internationale)

La CEI prépare et plublie des normes internationales relatives à l'électricité, l'électronique et autres technologies connexes. A travers ses membres, la CEI fait la promotion d'une coopération internationale sur toutes les questions liées à la normalisation électrotechnique et des 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

Ces normes sont communes à tous les pays de l'EEE et sont produites par les organismes de normalisation européens : CEN et CENELEC. Leur application est facultative, mais convevoir et fabriquer des équipements selon ces normes est la façon la plus directe se conformer aux EHSR définies par la Directive Machines.

Ces normes sont divisées en 3 types : A, B et C.

NORMES Type A : Couvrent des aspect concernant tous les types de machines.

NORMES Type B : Sous-divisées en 2 groupes.

NORMES Type B1 : couvrent des aspects particuliers relatifs à la sécurité et à l'ergonomie des machines.

NORMES Type B2 : couvrent les composants de sécurité et les dispositifs de protection.

NORMESType C : couvrent des types ou groupes spécifiques de machines.

Il est important de noter que la conformité à une norme C procure une présemption automatique de conformité avec les EHSR. En l'absence d'une norme C adaptée, les normes A et B peuvent être utilisées comme preuve partielle ou totale de conformité avec les EHSR par le renvoi à la conformité avec les sections pertinentes.

Des accords ont été passés pour une coopération entre le CEN/CENELEC et des organismes tels que l'ISO et la CEI. Cela devrait conduire à la production de normes internationales communes. Dans la plupart des cas, une norme EN a son équivalent CEI ou ISO. En général, les deux textes sont identiques et les divergences régionales sont indiquées dans le préambule de la norme.

Cette section liste certaines des normes EN, ISO, CEI et autres normes nationales et régionales relatives à la sécurité des machines. Lorsqu'une norme EN est indiquée entre crochets, elle est identique et très proche de la norme ISO ou CEI. Pour une liste complète des normes EN relatives à la sécurité des machines visitez : *http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_en.htm*

Normes ISO et EN (Type A)

EN ISO 12100

Sécurité des machines. Concepts de base ; principes généraux de conception. Parties 1 & 2

Il s'agit d'une norme de type A qui décrit tous les principes de base, notamment l'évaluation des risques, la protection, le verrouillage, l'arrêt d'urgence, les dispositifs de déclenchement, les distances de sécurité, etc. Elle renvoie à d'autres normes qui donnent plus de détails.

Dans un avenir proche, il est probable que EN ISO 12100 et EN ISO 14121 seront fusionnée en une seule norme.

EN ISO 14121

Principes de l'évaluation des risques.

La norme décrit les bases pour l'évaluation des risques au cours du cycle de vie de la machine. Elle récapitule les méthodes d'analyse du danger et d'estimation des risques.

Un rapport technique ISO : ISO/TR 14121-2, est également disponible. Il fait des recommandations et donne des exemples pratiques sur les méthodes d'évaluation des risques.

Normes ISO et EN (Type B)

EN ISO 11161

Sécurité des systèmes de fabrication intégrés – Prescriptions de base.

Cette norme a été publiée sous sa forme révisée en 2007. Elle a été largement mise à jour, ce qui la rend très utile pour les machines intégrées actuelles.

EN ISO 13849-1:2008 Composants de sécurité des systèmes de commande – Partie 1 : Principes généraux de conception

Cette norme est le résultat de la révision en profondeur de l'ancienne norme EN 954-1 (qui ne sera plus en vigueur fin 2011). Elle introduit de nombreux nouveaux aspects pour la sécurité fonctionnelle des systèmes de commande. Le terme « PL » (Performance Level ou niveau de performance) est utilisé pour décrire le niveau d'intégrité d'un système ou d'un sous-système.

Elle peut servir d'alternative à la norme CEI/EN 62061 (voir plus loin). Veuillez noter que la norme EN ISO 13849-1 couvre toutes les technologies des systèmes de commande, alors que la norme CEI/EN 62061 ne couvre que les technologies électriques.

EN ISO 13849-1 est destinées à fournir une transition directe pour les catégories de l'ancienne norme EN 954-1. Elle présente une méthodologie relativement simple comparée à la norme CEI/EN 62061, mais cela se fait au détriment de certaines contraintes et restrictions. Aussi bien la norme révisée ISO/EN 13849-1 que la CEI/EN 62061 peut être utilisée pour les systèmes de sécurité électrique des machines et l'utilisateur doit choisir celle qui est la mieux adaptée à ses besoins ; cependant, EN ISO 13849-1 est souvent préférée lorsqu'il y a transition de catégories.

Remarque : Peu de temps avant la publication de ce texte, le CEN (Comité européen de normalisation) a annoncé que la date finale pour la présomption de conformité à la norme EN 954-1 serait étendue jusque fin 2011 afin de faciliter la transition vers des normes plus récentes. Ceci remplace la date originale qui était fixée au 29 décembre 2009.

Pour les informations les plus récentes sur l'utilisation et l'état de la norme EN 954-1, visitez : *http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx*. En attendant, il est recommandé d'utiliser l'extension de la période de transition pour passer aux nouvelles normes (EN ISO 13849-1 ou CEI/EN 62061) en temps utile.

EN ISO 13849-2

Composants de sécurité des systèmes de commande – Partie 2 : Validation

Cette norme détaille la validation des composants de sécurité des sytèmes de commande. Elle possède des annexes qui donnent des détails sur les composants de sécurité, les principes de sécurité et l'exclusion des défauts.

EN ISO 13850

Dispositifs d'arrêt d'urgence, aspects fonctionnels – Principes de conception.

Décrit les principes et les exigences de conception.

ISO 13851 (EN 574)

Dispositifs à commande bimanuelle – Aspects fonctionnels – Principes de conception.

Décrit les exigences et les recommandations pour la conception et la sélection des dispositifs à commande bimanuelle, notamment la prévention du contournement et des défauts.

EN ISO 13857

Distances de sécurité afin d'éviter que le bras ou la jambe d'une personne ne puisse pénétrer dans une zone dangereuse.

Donne des indications pour le calcul des tailles d'ouverture et du positionnement des protections, etc.

ISO 13854 (EN 349)

Distances minimales afin d'éviter l'écrasement de parties du corps d'une personne.

Donne des indications pour le calcul des écartements de sécurité entre les pièces mobiles, etc.

ISO 13855 (EN 999)

Positionnement des équipements de protection par rapport aux vitesses d'approche des parties du corps d'une personne.

Décrit des méthodes de calcul pour les distances de sécurité minimales par rapport à un danger destinées à des dispositifs de sécurité spécifiques, en particulier pour les dispositifs électrosensibles (p. ex., les barrières immatérielles), les tapis sensibles à la pression et les commandes bimanuelles. Elle présente un principe de positionnement pour les dispositifs de sécurité basé sur la vitesse d'approche et le temps d'arrêt de la machine pouvant être extrapolé afin de couvrir les barrières de protection interconnectées sans gâche de sécurité.

ISO 13856-1 (EN 1760-1)

Dispositifs de sécurité sensibles à la pression – Partie 1 : Tapis & sols.

Décrit les exigences et les procédures de test.

ISO 13856-2 (EN 1760-2)

Dispositifs de sécurité sensibles à la pression – Partie 2 : Bourrelets & barres.

Décrit les exigences et les procédures de test.

ISO 14118 (EN 1037)

Prévention des démarrage intempestifs – Isolation et dissipation d'énergie

Définit les mesures destinées à isoler les machines des alimentations et à dissiper l'énergie accumulée afin de prévenir le démarrage intempestif des machines et de permettre une intervention en toute sécurité.

ISO 14119 (EN 1088)

Dispositifs d'interverrouillage associés aux barrière de protection – Principe de conception et de sélection.

Décrit les principes de conception et de sélection des dispositifs d'interverrouillage associés aux barrières de protection.

Afin de vérifier les interrupteurs mécaniques, elle renvoie à la norme CEI 60947-5-1 – Dispositif de commutation basse tension – Partie 5 : Dispositifs du circuit de commande et éléments de coupure – Article 1 : Dispositifs du circuit de commande électromécanique.

Pour vérifier les interrupteurs non mécaniques, elle renvoie à la norme CEI 60947-5-3 – Prescriptions particulières pour les dispositifs de proximité avec comportement défini en situation de défaut.

ISO 14120 (EN 953)

Prescriptions générales pour la conception et la construction des barrières de protection.

Donne des définitions, des descriptions et des exigences de conception pour les barrières de protection fixes et amovibles.

Normes ISO et EN (Type C)

Il existe de nombreuses normes de type C qui couvrent des types de machines spécifiques. Par exemple :

EN ISO 10218-1

Robots industriels

EN 415-4

Sécurité des machines d'emballage. Palettiseurs et dépalettiseurs.

Normes CEI et EN

CEI/EN 60204-1

Equipement électrique des machines – Partie 1 Prescriptions générales.

Cette norme est très importante qui décrit les recommandations de sécurité pour le câblage et l'équipement électrique des machines. Une version révisée en profondeur a été publiée en 2006. Cette version a éliminé la préférence précédente pour les circuits de sécurité électromécaniques.

CEI/EN 61508

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.

Cette norme est importante parce qu'elle contient les prescriptions et dispositions nécessaires à la conception de systèmes et sous-systèmes électroniques et programmables complexes. L'état générique cette norme n'est pas limitée au secteur des machines. Il s'agit d'un document long et complexe constitué de sept parties. Dans le secteur des machines, elle est principalement utilisée pour la conception d'appareils complexes, comme les automates de sécurité. Pour la conception et l'intégration du système des machines, les normes spécifiques au secteur, comme la norme CEI/EN 62061 ou EN ISO 13849-1, sont probablement mieux adaptées. CEI 61508 a préparé le chemin pour les normes spécifiques au secteur et aux produits de nouvelle génération qui apparaissent. Elle a introduit l'acronyme SIL (safety integrity level ou niveau d'intégrité de la sécurité) et définit 4 niveaux hiérarchiques SIL utilisés pour la fonction de sécurité. Le niveau SIL 1 est le plus faible et le niveau SIL 4 est le plus élevé. SIL 4 ne s'applique généralement pas au secteur des machines parce qu'il est prévu pour des niveaux de risque très élevés plus souvent associés aux secteurs comme la pétrochimie ou le nuclaire.

CEI 62061 (EN 62061)

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.

Cette norme est une norme de nouvelle génération qui utilise l'acronyme SIL (safety integrity level). Il s'agit en fait de la version de la norme CEI/EN 61508 spécifiquement destinée aux machines. Elle définit les exigences et fait des recommandations pour la conception, l'intégration et la validation des systèmes de commande de sécurité des machines. Cette norme fournit une approche alternative à la norme EN ISO 13849-1 et elle est prévue pour être utilisée pour les fonctions de sécurité de plus en plus complexes requises par les machines actuelles et futures. Pour les fonctions de sécurité moins complexe, EN ISO 13849-1 peut être plus facile à mettre en place. L'utilisation de ces normes nécessite la disponibilité de données telles que PFH_D (probabilité de défaillance dangereuse par heure) ou MTTFd (durée moyenne de fonctionnement avant défaillance dangereuse).

CEI 61496 (EN 61496)

Equipement de protection électro-sensible Partie 1 :Prescriptions générales et tests.

Prescriptions générales et tests.

Partie 2 : Prescriptions particulières pour l'équipement utilisant des appareils de protection optoélectronique actif.

La partie 1 définit les exigences et les procédures de test pour la commande et la surveillance de l'équipement de protection électrosensible. Les parties suivantes traitent des aspects particuliers liés à la partie détection du système. La partie 2 définit les exigences particulières liés aux barrières immatérielles de sécurité.

CEI 61800-5-2 (EN 61800-5-2)

Sécurité fonctonnelle des systèmes à variateur de puissance.

Cette norme traite des variateurs avec fonctions de sécurité.

Normes américaines

Normes OSHA

Lorsque c'est possible, l'OSHA promulgue des normes consensuelles nationales ou des normes fédérales établies en normes de sécurité. Les dispositions obligatoires des normes, incorporées par référence, ont la même force et les mêmes effets que les normes listées dans la partie 1910. Par exemple, la norme consensuelle nationale NFPA 70 est listée comme document de référence dans l'annexe A de la sous-partie S-Electrique de la partie 1910 de 29 CFR. NFPA 70 est une norme facultative qui a été élaborée par la National Fire Protection Association (NFPA). NFPA 70 est également connue sous le nom National Electric Code (NEC). Par incorporation, toutes les exigences obligatoires du NEC sont obligatoires selon l'OSHA.

Ce qui suit est une liste contenant différentes normes OSHA relatives à la sécurité des machines :

1910 sous-partie O - Machines et protection des machines

1910.211 - Définitions.

1910.212 - Prescriptions générales de toutes les machines.

1910.213 - Prescriptions pour les machines à bois.

1910.214 - Machines pour la tonnellerie. [Réservé]

1910.215 - Machines à meule abrasive.

1910.216 - Machines rotatives dans les industries du caoutchouc et du plastique.

1910.217 - Presses mécaniques.

1910.217 Annexe A - Prescriptions obligatoires pour la certification/validation des systèmes de sécurité pour l'initialisation par dispositif de détection de présence des presses électriques mécaniques.

1910.217 Annexe B - Recommandations non obligatoires pour la certification/validation des systèmes de sécurité pour l'initialisation par dispositif de détection de présence des presses électriques mécaniques.

1910.217 Annexe C - Prescriptions obligatoires pour la reconnaissance par l'OSHA des organisations de validation tierces pour la norme PSDI.

1910.217 Annexe D - Informations supplémentaires non obligatoires.

1910.218 - Machines à forger.

1910.219 - Puissance mécanique.

1910.255 - Soudage par résistance.

1910 Sous-partie R - Industries spéciales.

1910.261 - Usines de pâte à papier, papier et carton.

1910.262 - Textiles.

1910.263 - Equipement de boulangerie.

1910.264 - Machines et opérations de blanchissage.

1910.265 - Scieries.

1910.266 - Opérations forestières.

Normes ANSI

Le National Standards Institute (ANSI) sert d'administrateur et de coordinateur pour le système de normalisation volontaire du secteur privé aux Etats-Unis. C'est un association mutuelle privée à but non lucratif soutenue par un groupement varié d'organisations des secteurs privé et public.

L'ANSI n'élabore pas de normes mais aide à l'élaboration de normes en créant un consensus entre des groupes qualifiés. L'ANSI assure également que les principes directeurs du consensus, le suivi des procédures et la transparence sont respectés par les groupes qualifiés. Ci-dessous est présentée une liste partielle des normes de sécurité industrielle pouvant être obtenue en contactant l'ANSI.

Ces normes sont classées comme normes d'application ou comme normes de construction. Les normes d'application définissent comment instaurer la protection sur les machines. Par exemple, ANSI B11.1 fournit des informations sur l'utilisation des protections machine sur les presses électriques et ANSI/RIA R15.06 décrit l'utilisation des protections sur les robots.

National Fire Protection Association

La National Fire Protection Association (NFPA) a été créée en 1896. Sa mission consiste à réduire le fardeau que fait peser le feu sur la qualité de vie en encourageant des normes et des codes consensuels basés sur des faits scientifiques, ainsi que des recherches et une informations sur le feu et autres questions de sécurité connexes. NFPA promeut de nombreuses normes qui l'aident à accomplir sa mission. Deux normes très importantes liées à la sécurité industrielle et à la protection sont le National Electric Code (NEC) et l'Electrical Standard for Industrial Machinery.

La National Fire Protection Association a joué le rôle de promoteur pour le NEC depuis 1911. Le document original établissant le code a été élaboré en 1897 à la suite des efforts communs de divers groupes d'intérêts dans les domaines de l'assurance, de l'électricité, de l'architectuer et connexes. Le NEC a depuis été remanié de nombreuses fois ; il est révisé environ tout les trois ans. L'article 670 du NEC aborde certains aspects des machines industrielles et renvoie le lecteur à l'Electrical Standard for Industrial Machinery, NFPA 79.

NFPA 79 concerne les équipements, les appareils et les systèmes électriques/électroniques des machines industrielles fonctionnant sur une tension nominale de 600 volts ou moins. L'objectif de la norme NFPA 79 est de fournir des informations détaillées sur l'utilisation des équipements, appareils ou systèmes électriques/électroniques faisant partie des machines industrielles et qui promeuvent la sécurité des personnes et des équipements. NFPA 79, qui a été adoptée officiellement par l'ANSI en 1962, a un contenu très semblable à celui de la norme CEI 60204-1.

Les machines, qui ne sont pas couvertes par des normes OSHA spécifiques, doivent être dépourvues de tout dangers reconnus pouvant entraîner le décès ou des blessures sérieuses. Ces machines doivent être conçues et entretenues de façon à être conforme ou à dépasser les exigences des normes industrielles en vigueur. NFPA 79 est une norme qui s'applique aux machines qui ne sont pas spécifiquement couvertes par les normes OSHA.

ANSI/NFPA 70
US National Electrical Code

ANSI/NFPA 70E
Prescriptions pour la sécurité électrique sur le lieu de travail

ANSI/NFPA 79
Norme électrique pour les machines industrielles

Association for Manufacturing Technology

ANSI B11.1
Machines-outils - Presses mécaniques - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.2
Machines-outils - Presses hydrauliques - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.3
Freins de presse électrique - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.4
Machine-outils - Cisailles - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.5
Machines-outils - Equipement sidérurgique - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.6
Tours - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.7
Machines-outils - Machine à matricer et former à froid - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.8
Perceuses, fraiseuse et aléseuse - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.9
Meuleuse - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.10
Machine à scier le métal -Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.11
Machine à tailler les engrenages - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.12
Machines-outils - Laminoir à profilés et cintreuse à galets - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.13
Machines-outils - Décolleteuses mono et multi-broche automatique et machines à mandrins - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.14
Machines-outils - Machines à refente bobine - Exigences de sécurité pour la construction, l'entretien et l'utilisation – Retirée et intégrée à B11.18

ANSI B11.15
Cintreuses pour tuyau, tube et de mise en forme - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.16
Presses à compacter la poudre métallique - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.17
Machines-outils - Presses hydrauliques à extrusion horizontales - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.18
Machines-outils - Machines et équipements pour le traitement de bandes, feuilles ou plaques à partir de configurations en serpentin - Machines and Machinery Systems

ANSI B11.19
Machines-outils - Protection lorsque référencée par d'autres normes B11 relatives à la sécurité des machines - Critères de performance pour la conception, la construction, l'entretien et l'utilisation

ANSI B11.20
Machines-outils - Systèmes/cellules de fabrication – Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B11.21
Machines-outils - Machines-outils utilisant des lasers pour le traitement des matériaux - Exigences de sécurité pour la conception, la construction, l'entretien et l'utilisation

ANSI B11.TR3
Evaluation des risques et réduction des risques – Guide servant à estimer, évaluer et limiter les risques liés aux machines-outils

ANSI B11.TR4
Ce rapport technique aborde l'utilisation des automates programmables dans les applications de sécurité.

ANSI B11.TR6
Ce rapport technique, en cours d'élaboration, fournit des exemples de circuits des fonctions de sécurité pour différents niveaux de réduction des risques.

ANSI ISO 12100
Machines de sécurité. Concepts de base ; principes généraux de conception. Parties 1 et 2
La norme ISO 12100 a été adoptée aux Etats-Unis par l'AMT sous la forme d'une norme ANSI identique. ISO 12100 est une norme sur les principes de base applicable dans le monde entier qui constitue le cadre de travail pour la plupart des normes ISO, CEI et EN relatives à la sécurité des machines. Elle a une approche basée sur l'évaluation des risques, et non une approche normative et restrictive. L'objectif est d'éviter les problèmes de coût et les entraves commerciale provoqués par une multiplicité de normes nationales couvrant le même sujet de différentes façons.

Robot Industries Association
ANSI RIA R15.06
Exigences de sécurité pour les robots industriels et les systèmes robotisés
ANSI RIA R15.06
Exigences de sécurité pour les robots industriels et les systèmes robotisés

Packaging Machinery Manufacturer's Institute
ANSI PMMI B155.1
Exigences de sécurité pour les machines de conditionnement et les machines de conversion liée au conditionnement
La norme sur le conditionnement a été récemment révisée afin d'inclure l'évaluation des risques et la réduction des risques.

American Society of Safety Engineers
Z224.1
Contrôle de l'énergie dangereuse, condamnation/signalisation et méthodes alternatives
Cette norme est similaire à la norme OSHA 1910.147. Elle fournit une approche (évaluation des risques) pour déterminer la méthode alternative appropriée lorsque l'énergie ne peut pas être condamnée.

Society of Plastics Industry
ANSI B151.1
Machines à injecter horizontales – Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B151.15
Machines de moulage par extrusion-soufflage – Exigences de sécurité

ANSI B151.21
Machines de moulage par injection-soufflage – Exigences de sécurité

ANSI B151.26
Machines à matières plastiques - Réaction dynamique – Macines à injection - Exigences de sécurité pour la construction, l'entretien et l'utilisation

ANSI B151.27
Machines à matières plastiques - Robots utilisés avec les machiens à injection horizontales - Exigences de sécurité pour l'intégration, l'entretien et l'utilisation

ANSI B151.28
Machines à matières plastiques - Machines à découper, fendre ou polir la mousse plastique - Exigences de sécurité pour la construction, l'entretien et l'utilisation

Normes canadiennes
Les normes CSA reflètent une consensus entre producteurs et utilisateurs – notamment les fabricants, consommateurs, détaillants, syndicats, organisations professionnelles et agences gouvernementales. Les normes sont largement utilisées dans l'industrie et le commerce, et sont souvent adoptées par les administrations municipales, provinciales et fédérales dans leurs réglementations, particulièrement dans les domaines de la santé, la sécurité, la construction et l'environnement.

Les individus, les entreprises et les associations partout au Canada montrent leur soutien à l'élaboration des normes CSA en donnant de leur temps et en apportant leurs compétences au travail du Comité CSA et soutiennent les objectifs de l'Association en devenant membres donateurs. Les plus de 7 000 volontaires du comité et les 2 000 membres donateurs constituent l'ensemble de membres du CSA.

Le Conseil canadien des normes est l'organisme coordonateur du système des normes nationales, une fédération d'organisations autonomes et indépendantes qui travaille à l'élaboration et à l'amélioration des normes dans l'intérêt national.

CSA Z432-04
Sécurité des machines

CSA Z434-03
Robots industriels et systèmes robotiques - exigences générales de sécurité

CSA Z460-05
Maîtrise des énergies dangereuses - Cadenassage et autres méthodes

CSA Z142-02
Code régissant l'opération des presses : Exigences concernant la santé, la sécurité et la protection

Normes australiennes

La plupart de ces normes sont étroitement alignées sur les normes équivalentes ISO/CEI/EN

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
Télécopie : +61 2 8206 6001
Courriel : mail@sai-global.com
Site Internet : www.saiglobal.com/shop

AS 4024.1-2006

Protection des machines. Partie 1 : Principes généraux

AS 4024.1101-2006	Terminologie – Généralités
AS 4024.1201-2006	Terminologie et méthodologie de base
AS 4024.1202-2006	Principes techniques
AS 4024.1301-2006	Principes d'évaluation des risques
AS 4024.1302-2006	Réduction des risques pour la santé et la sécurité provenant des substances dangereuses émises par les machines
AS 4024.1401-2006	Principes de conception – Terminologie et principes généraux
AS 4024.1501-2006	Conception des composants de sécurité des systèmes de commande - Principes généraux
AS 4024.1502-2006	Conception des composants de sécurité des systèmes de commande - Validation
AS 4024.1601-2006	Exigences générales pour la conception et la construction des protections fixes et amovibles
AS 4024.1602-2006	Principes de conception et de sélection des dispositifs de verrouillage
AS 4024.1603-2006	Prévention et démarrage imprévisible
AS 4024.1604-2006	Arrêt d'urgence – Principes de conception
AS 4024.1701-2006	Mesures du corps humain pour la conception technologique
AS 4024.1702-2006	Principes pour la détermination des dimensions requises pour les ouvertures permettant l'accès du corps entier dans la zone de la machine
AS 4024.1703-2006	Principes pour la détermination des dimensions requises pour les ouvertures d'accès
AS 4024.1704-2006	Données anthropométriques
AS 4024.1801-2006	Distances de sécurité – Membres supérieurs
AS 4024.1802-2006	Distances de sécurité – Membres inférieurs
AS 4024.1803-2006	Espacements minimum pour éviter l'écrasement de parties du corps humain
AS 4024.1901-2006	Principes généraux pour l'interaction humaine avec les afficheurs et les actionneurs
AS 4024.1902-2006	Afficheurs
AS 4024.1903-2006	Actionneurs
AS 4024.1904-2006	Exigences pour les signaux visuels, sonores et tactiles
AS 4024.1905-2006	Exigences pour le marquage
AS 4024.1906-2006	Exigences pour le positionnement et l'utilisation des actionneurs
AS 4024.1907-2006	Systèmes de signaux de danger sonores et visuels et signaux d'information

AS4024.2-1998
Protection des machines. Partie 2 : Exigences d'installation et de mise en service pour systèmes electro-sensibles – Dispositifs optoélectroniques
La base de cette norme est la norme CEI 61496-1 et -2. La partie 2 couvre l'installation et la mise en service de barrières immatérielles spécialement adaptées à la sécurité des machines.

AS 4024.3-1998
Protection des machines. Partie 3 : Exigences de fabrication et de test pour systèmes electro-sensibles – Dispositifs optoélectroniques
La base de cette norme est la norme CEI 61496-1 et -2. La partie 3 couvre la fabrication et les tests des barrières immatérielles spécialement adaptées à la sécurité des machines.

AS4024.4-1998
Protection des machines. Partie 4 : Exigences d'installation et de mise en service pour systèmes electro-sensibles – Dispositifs sensibles à la pression
La base de cette norme est la norme EN 1760-1 et EN 1760-2. La partie 4 couvre l'installation et la mise en service de tapis, bourrelets et barres utilisés avec les machines, quelle que soit l'énergie utilisée.

AS 4024.5-1998
Protection des machines. Partie 5 : Exigences de fabrication et de test pour systèmes electro-sensibles – Dispositifs sensibles à la pression
La base de cette norme est la norme EN 1760-1 et EN 1760-2. La partie 5 couvre la fabrication et lest tests des tapis, bourrelets et barres utilisés avec les machines, quelle que soit l'énergie utilisée.

Stratégie de sécurité

D'un point de vue purement fonctionnel, plus une machine est efficace dans l'accomplissement de sa tâche, meilleure elle est. Mais, pour qu'une machine soit viable, elle doit également être sécurisée. En effet, la sécurité doit être considérée comme un critère essentiel.

Afin de concevoir une stratégie de sécurité adaptée, deux étapes doivent être combinées, comme dans la figure 9.

Evaluation des risques, basée sur une bonne compréhension des limites et des fonctions de la machine et des tâches devant être réalisées sur la machine tout au long de la durée d'utilisation.

Réduction des risques, est alors réalisée si besoin et des mesures de sécurité sont sélectionnée sur la base des informations dérivées de l'étape d'évaluation des risques.

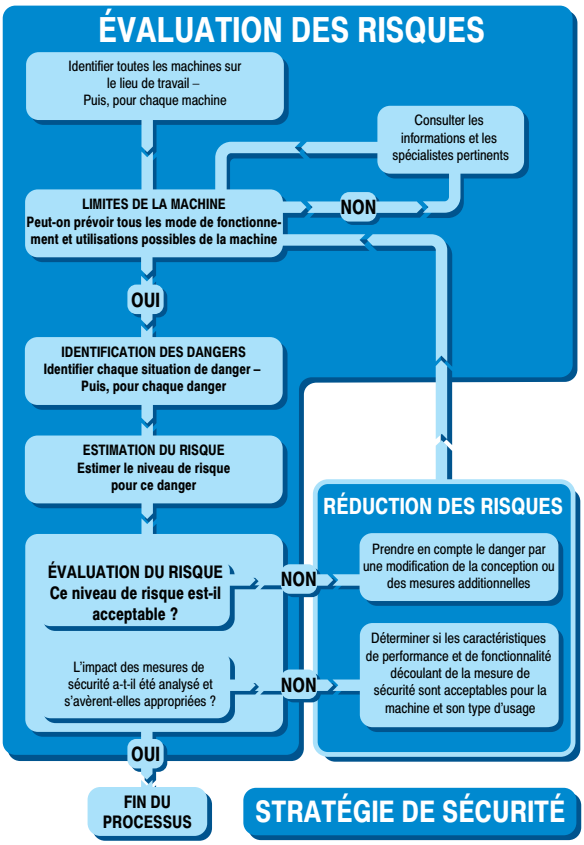


Figure 9 : Stratégie de sécurité

La façon dont cela est fait constitue la base de la stratégie de sécurité pour les machines.

Il nous faut une liste de vérification pour faire un suivi et s'assurer que tous les aspects sont pris en compte et que le principe de départ ne se trouve pas perdu dans les détails. Tout le processus doit être documenté. Cela permet non seulement d'assurer un travail plus rigoureux, mais également de mettre les résultats à disposition pour que d'autres protagonistes puissent les vérifier.

Cette section concerne à la fois les fabricants de machines et les utilisateurs de machines. Le fabricant doit s'assurer que sa machine peut être utilisée en toute sécurité. L'évaluation des risques doit être commencée dès la conception de la machine et elle doit prendre en considération toutes les tâches prévisibles qui devront être effectuées sur la machine. Cette approche basée sur les tâches dès les premières étapes de l'évaluation des risques est très importante. Par exemple, il peut être nécessaire de régler des pièces mobiles de la machine à intervalle régulier. Il doit être possible d'inclure dans la phase de conception des mesures qui permettront de réaliser ce processus en toute sécurité. Si cela n'est pas fait dès les premières étapes, il peut être difficile, voire même impossible, de les mettre en place lors des étapes suivantes. Le conséquence peut être que le réglage des pièces mobiles doit tout de même être fait, mais qu'il doive se faire d'une façon non sécurisée ou inefficace (voire les deux). Une machine sur laquelle toutes les tâches ont été prises en compte au cours de l'évaluation des risques est une machine plus sûre et plus efficace.

L'utilisateur (ou l'employeur) doit s'assurer que les machines se trouvant sur le lieu de travail sont sécurisées. Même si une machine a été déclarée sécurisée par le fabricant, son utilisateur doit tout de même réaliser une évaluation des risques afin de déterminer si l'équipement est sécurisé dans son environnement spécifique. Les machines sont souvent utilisées dans des situations non prévues par le fabricant. Par exemple, une fraiseuse utilisée dans un atelier scolaire doit faire l'objet d'une plus grande attention qu'une fraiseurse utilisée dans un atelier industriel.

Il ne faut pas aussi oublier qu'une entreprise utilisatrice qui acquiert plusieurs machines indépendantes et les intègre dans un unique procédé, devient le fabricant de la machine combinée qui en résulte.

Considérons maintenant les étapes essentielles qui conduisent à une stratégie de sécurité adaptée. Ce qui suit peut être appliqué à une installation industrielle existante ou à une seule nouvelle machine.

Evaluation des risques

Il ne faut pas considérer l'évaluation des risques comme une charge. Il s'agit d'un processus utile qui fournit des informations vitales et permet à l'utilisateur ou au concepteur de prendre des décisions logiques sur la façon d'obtenir un niveau de sécurité.

Il existe différentes normes qui traitent de ce sujet. Les normes ISO 14121 : « Principes de l'évaluation des risques » et ISO 12100: « Sécurité des machines – Principes de base » contiennent les recommandations les plus utilisées dans le monde.

Quelle que soit la technique utilisée pour évaluer les risques, une équipe pluridisciplinaire permet généralement d'obtenir des résultats dont la couverture est plus large et qui sont plus équilibrés qu'avec une seule personne.

L'évaluation des risques est un processus itératif ; elle est réalisée à différentes étapes tout au long du cycle de vie de la machine. Les informations disponibles varient selon l'étape dans le cycle de vie. Par exemple, lorsqu'il réalise une évaluation des risques, un constructeur de machines aura accès à tous les détails des mécanismes de la machine et des matériaux de construction, mais n'aura probablement qu'un aperçu approximatif de l'environnement dans lequel la machine sera utilisée. Lorsqu'il réalise une évaluation des risques, l'utilisateur de la machine n'a pas forcément accès à tous les détails techniques mais il a toutes les informations sur l'environnement dans lequel elle sera utilisée. Idéalement le résultat d'une itération sera le point de départ le l'itération suivante.

Déterminer les limites de la machine

Ceci implique une collecte et une analyse des informations concernant les pièces, les mécanismes et les fonctions d'une machine. Il est également nécessaire de prendre en considération tous les types d'interactions du personnel avec la machine et l'environnement dans lequel la machine est utilisée. L'objectif est d'obtenir une bonne compréhension de la machine et de son utilisation.

Lorsque des machines distinctes sont reliées entre elles, de façon mécanique ou par des systèmes de commande, elles doivent être considérées comme une seule machine, sauf si elles sont divisées en zones par des mesures de protection appropriées.

Il est important de prendre en compte toutes les limites et les étapes du cycle de vie d'une machine, notamment l'installation, la mise en service, la maintenance, la mise hors service, l'utilisation et le fonctionnement corrects, ainsi que les conséquences d'une mauvaise utilisation ou d'un dysfonctionnement raisonnablement prévisibles.

Identification des tâches et des dangers

Tous les dangers liés à la machine doivent être identifés et listés en fonction de leur nature et de leur localisation. Les types de danger incluent l'écrasement, le cisaillement, l'enchevêtrement, l'éjection de pièces, les fumées, le rayonnement, les substances toxiques, la chaleur, le bruit, etc.

Les résultats de l'analyse des tâches doivent être comparés avec les résultats de l'identification des dangers. Cela montre à quels endroits il existe un risque de convergence entre une source de danger et une personne, c.-à-d. une situation à risque. Toutes les situations à risque doivent être listées. Il est possible que le même danger produise différents types de situations à risque selon la nature de la personne ou de la tâche. Par exemple, la présence d'un technicien de maintenance hautement qualifié et compétent peut avoir des implications différentes que la présence d'un agent 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 l'agent de nettoyage. Si les cas ne sont pas listés et abordés séparément, le cas le plus défavorable doit être utilisé et le technicien de maintenance ainsi que l'agent de nettoyage sont couverts par les mêmes mesures de protection.

Il est parfois nécessaire de réaliser une évaluation générale des risques sur une machine existante qui a déjà des mesures de protection (p. ex., une machine avec des parties mobiles dangereuses protégée par une barrière de protection interconnectée). Les parties mobiles dangereuses constituent un danger potentiel qui peut devenir un danger réel en cas de défaillance du système de verrouillage. Sauf si ce système de verrouillage a déjà été validé (p. ex., par une évaluation des risques ou pour une conception conforme à une norme appropriée), sa présence ne doit pas être prise en compte.

Estimation des risques

Il s'agit d'un des aspects les plus fondamentaux de l'évaluation des risques. Il existe de nombreuses façons d'aborder ce sujet et les pages suivantes en illustrent les principes de base.

Toute machine pouvant potentiellement créer une situation dangereuse présente un risque d'événement dangereux (c.-à-d., de blessure). Plus le risque est grand, plus il est important de faire quelque chose pour l'éviter. Avec un danger donné, le risque peut être si faible qu'il est possible de le tolérer et de l'accepter, mais pour un autre danger, le risque peut être si élevé qu'il faut prendre des mesures extrêmes pour s'en protéger. Par conséquent, pour décider s'il convient de faire quelque chose à propos de ce risque, et dans ce cas ce qu'il faut faire, il est nécessaire de pouvoir le quantifier.

Le risque est souvent évalué uniquement en fonction de la gravité des blessures qu'il peut provoquer en cas d'accident. La gravité des blessures potentielles ET la probabilité de leur apparition doivent être prises en compte pour estimer le niveau du risque.

La suggestion faite sur les pages suivantes pour l'estimation des risques n'est pas préconisée comme LA méthode étant donné que les situations individuelles peuvent dicter une approche différente. SON OBJECTIF EST DE SERVIR DE GUIDE GÉNÉRAL POUR ENCOURAGER A LA CRÉATION D'UNE STRUCTURE MÉTHODIQUE ET DOCUMENTÉE.

Le système de points n'a été calibré pour aucun type particulier d'application, il n'est donc pas nécessairement adapté à toute application spécifique. ISO TR (rapport technique) 14121-2 « Evaluation des risques – Recommandations pratiques et exemples de méthodes » fournit des recommandations pratiques et décrit des méthodes différentes pour mesurer les risques.

Les facteurs suivants sont pris en compte :

- LA GRAVITE D'UNE BLESSURE POTENTIELLE.
- LA PROBABILITE DE SON APPARITION.

La probabilité d'apparition inclut deux facteurs :

- FREQUENCE D'EXPOSITION.
- PROBABILITE DE BLESSURE.

En abordant chaque facteur individuellement, nous allons attribuer des valeurs à chacun d'eux.

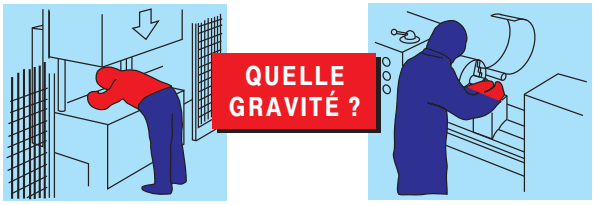
Utilisez toutes les données et les compétences à votre disposition. Vous prenez en compte toutes les étapes du cycle de vie de la machine, donc pour éviter une trop grande complexité, basez vos décisions sur le cas le plus défavorable pour chaque facteur.

Il est également important de garder son bon sens. Les décisions doivent prendre en compte ce qui est faisable, réaliste et plausible. C'est là qu'une approche basée sur une équipe pluridisciplinaire est utile.

N'oubliez pas que pour cet exercice vous ne devez généralement pas prendre en compte les systèmes de protection existants. Si l'estimation des risques montre qu'un système de protection est requis, il existe des méthodologies indiquées plus loin dans ce chapitre qui peuvent être utilisées pour déterminer les caractéristiques requises.

1. Gravité des blessures potentielles

Dans cet exemple, nous supposons que l'accident ou l'incident qui s'est produit, est peut-être la conséquence des dangers illustrés sur la figure 10. Une étude précise du danger indique quelle est la blessure la plus grave pouvant se produire.



Dans cet exemple, la blessure la plus grave serait de type « fatale ».

Dans cette exemple, la blessure la plus grave à attendre serait de type « sérieuse » avec possibilité de contusion, fracture, amputation d'un doigt ou blessure causée par l'éjection de la clé du mandrin, etc.

Figure 10 : Blessure potentielle

Remarque : dans cet exemple, nous supposons qu'une blessure est inévitable et nous ne nous attachons qu'à sa gravité. Partez du principe que l'opérateur est exposé au mouvement ou procédé dangereux.

La gravité de la blessure doit être évaluée comme :

- **MORTELLE :** décès
- **MAJEURE** : (normalement irréversible) handicap permanent, perte de la vue, amputation d'un membre, trouble respiratoire, etc.
- **GRAVE** : (normalement réversible) perte de conscience, brûlure, fractures, etc.
- **MINEURE** : ecchymoses, coupures, écorchures légères, etc.

Chaque description peut se voir attribuer une valeur de points (illustré à la figure 11).

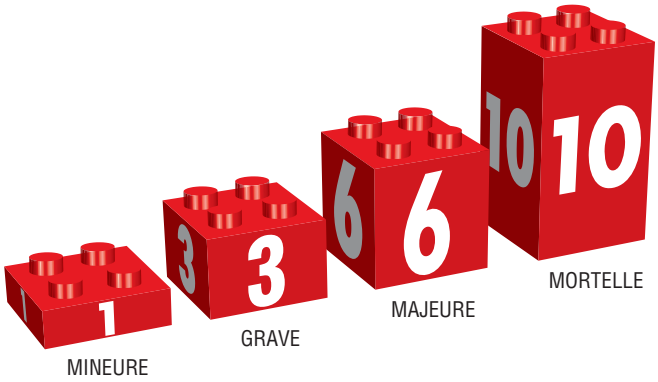


Figure 11 : Points attributés selon la gravité

2. Fréquence d'exposition

La fréquence d'exposition répond à la question : à quelle fréquence l'opérateur ou le personnel de maintenance est-il exposé au danger (Figure 12).

Figure 12 : Fréquence d'exposition

La fréquence d'exposition au danger peut être classée comme :

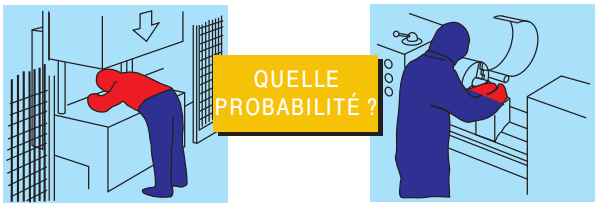
- **FREQUENTE** : plusieurs fois par jour
- **OCCASIONNELLE** : quotidiennement
- **RAREMENT** : une fois par semaine ou moins

Chaque description peut se voir attribuer une valeur de points (illustré à la figure 13).

Figure 13 : Points attribués selon la fréquence d'exposition

3. Probabilité de blessure

Vous devez partir du principe que l'opérateur est exposé au mouvement ou au procédé dangereux (Figure 14).



Dans cet exemple, la probabilité de blessure peut être considérée comme « certaine » en raison de la proportion du corps engagée dans la zone de danger et de la vitesse de fonctionnement de la machine.

Dans cet exemple, la probabilité de blessure peut être considérée comme « possible » car l'exposition de l'opérateur au danger est minimale et qu'il a le temps de s'écarter du danger.

Figure 14 : Probabilité

En prenant en compte la façon dont l'opérateur interagit avec la machine, ainsi que d'autres facteurs (vitesse de démarrage, par exemple), la probabilité de blessure peut être classée comme :

- Improbable
- Probable
- Possible
- Certaine

Chaque description peut se voir attribuer une valeur de points (illustré à la figure 15).

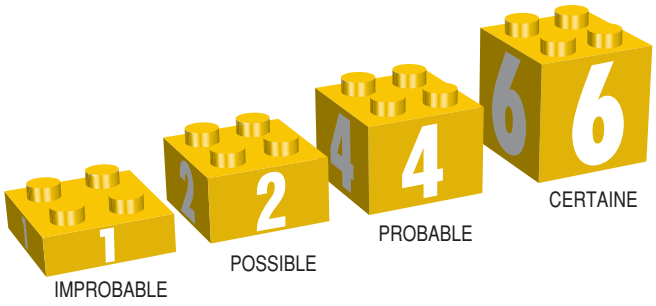


Figure 15 : Points attribués selon la probabilité de blessure

Tous les facteurs ont reçu une valeur et sont additionnés pour donner une estimation initiale. La figure 16 montre que le total des trois facteurs donne 13. Mais nous devons prendre en considérations quelques facteurs supplémentaires.

Figure 16 : Estimation initiale

(**Remarque** : ceci n'est pas forcément basé sur les images de l'exemple précédent.)

L'étape suivante consiste à ajuster l'estimation initiale par la prise en compte de facteurs supplémentaires comme ceux indiqués dans le tableau 2. Il est fréquent qu'ils ne puissent être pris en compte correctement que lorsque la machine est installée dans son environnement permanent.

Facteur typique	Action suggérée
Plusieurs personnes exposées au danger	Multiplier la gravité par le nombre de personnes
Durée prolongée dans la zone dangereuse sans isolement complet de l'alimentation	Si la durée de chaque accès est supérieure à 15 minutes, ajouter 1 point au facteur de fréquence
L'opérateur n'est pas qualifié ou formé	Ajouter 2 points au total
Intervalles très longs (p. ex., un an) entre les accès. (Il peut y avoir des défaillances progressives et non détectées, particulièrement dans les systèmes de surveillance.)	Ajouter le nombre de points équivalent au facteur de fréquence maximum

Tableau 2 : critères supplémentaires pour l'estimation des risques

Les résultats des facteurs supplémentaires sont ajoutés au total précédent, comme montré sur la figure 17.

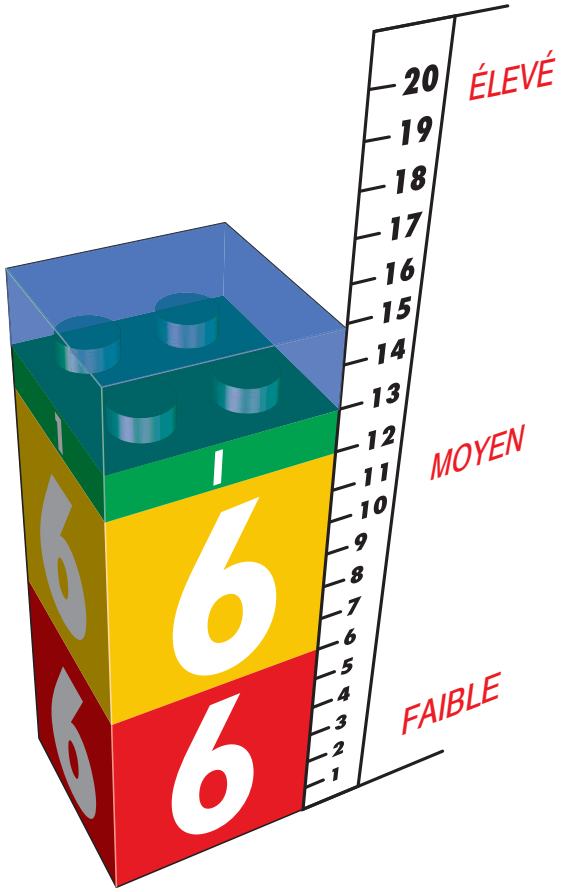


Figure 17 : Valeur final avec ajustements

Réduction des risques

Nous devons maintenant prendre en considération chaque machine et leurs risques respectifs, puis prendre des mesures pour gérer les dangers.

Le tableau illustré sur la figure 18 est une suggestion pour une partie du processus documenté de prise en compte de tous les aspects de sécurité de la machine utilisée. Il constitue un guide pour les utilisateurs de machines, mais les fabricants et fournisseurs de machines peuvent également utiliser le même principe pour vérifier que tous les équipements ont été évalués. Il constitue également un index pour des rapports plus détaillés sur l'évaluation des risques.

Il montre que lorsqu'une machine porte le marquage CE, le processus est simplifié puisque les dangers présentés par la machine ont déjà été évalués par le fabricant et les mesures nécessaires ont été prises. Même avec un équipement marqué CE, il peut exister des dangers non prévus par le fabricant en raison de la nature de son utilisation ou des matériaux qu'il transforme.

Hiérarchie des mesures pour la réduction des risques

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

1. Eliminer ou réduire les risques autant que possible (conception et construction de machines à sécurité intrinsèque).
2. Installation des systèmes et des mesures de protection nécessaires (p. ex. protections interconnectées, barrières immatérielles, etc) selon les risques qui ne peuvent pas être éliminés lors de la conception.
3. Informer les utilisateurs des risques résiduels dus à des insuffisances des mesures de protection adoptées, indiquer si une formation spécifique est requise et spécifier s'il faut fournir un équipement de protection individuelle.

Chaque mesure de la hiérarchie doit être prise en compte à partir du haut et utilisée lorsque c'est possible. Cela entraîne en générale l'utilisation d'une combinaison de mesures.

Société – MAYKIT WRIGHT LTD
Bâtiment – Atelier d'outillage – Secteur est.
Date – 29/08/95
Profil opérateur – En apprentissage/Expérimenté.

Réf. équipement et date d'installation	Conformité aux Directives	Numéro de rapport d'évaluation de risque	Historique des accidents	Remarques	Identification du danger	Type de danger	Action corrective	Effectué et vérifié – Référence
Tour parallèle Bloggs. N° de série 8390726 Date install. : 1978	Non concerné	RA302	Aucun	Équipement électrique conforme à BS EN 60204 Arrêts d'urgence en place (remplacés : 1989)	Rotation du mandrin avec grille ouverte	Entraînement par les parties en mouvement Coupures	Installation interrupteur d'interverrouillage sur grille	25/11/94 (J. Kershaw – Rapport n° 9567)
					Fluide de coupe	Toxicité	Remplacer par qualité non toxique	30/11/94 (J. Kershaw – Rapport n° 9714)
					Nettoyage copeaux	Coupures	Fournir des gants	30/11/94 (J. Kershaw – Rapport n° 9715)
Fraiseuse à tourelle Bloggs N° de série 17304294 Date fabric. : 1995 Date install. : Mai 1995	Dir. Machine Dir. CEM	RA416	Aucun		Déplacement du banc (vers le mur)	Écrasement	Déplacer machine pour avoir un dégagement suffisant	13/04/95 (J. Kershaw – Rapport n° 10064)

Figure 18 : Modèle d'évaluation des risques

Conception à sécurité intrinsèque

Lors de la conception de la machine, il est possible d'éviter de nombreux dangers potentiels simplement par une prise en compte de facteurs tels que les matériaux, les impératifs d'accès, les surfaces chaudes, les méthodes de transmission, les points pièges, niveaux de tension, etc.

Par exemple, s'il n'est pas nécessaire d'accéder à une zone dangereuse, la solution consiste à la protéger de l'intérieur du corps de la machine ou par une barrière englobante fixe.

Systèmes et mesures de protection

Si l'accès est requis, les choses sont un peu plus complexes. Il est nécessaire de s'assurer que l'accès n'est possible que lorsque la machine est sécurisée. Des mesures de protection comme les barrières de protection interconnectées et/ou les systèmes de déclenchement sont requis. Le choix du dispositif ou du système de protection doit être fait en grande partie selon les caractéristiques de fonctionnement de la machine. Ceci est très important parce qu'un système qui nuit à l'efficacité de la machine se trouve soumis au retrait ou au contournement non autorisé.

Dans ce cas, la sécurité de la machine dépend de l'application et de l'utilisation correctes du système de protection, même en situation de défaut.

L'utilisation correcte du système doit maintenant être abordée. Dans chaque type, il est probable qu'il existe un choix de technologies présentant des degrés divers de performance dans la surveillance, la détection et la prévention des défauts.

Dans un monde idéal, chaque système de protection serait parfait sans possiblité de défaillance en situation de danger. Dans le monde réel, cependant, nous sommes restreints par les limites actuelles des connaissances et des matériaux. Une autre contrainte très réelle est celle du coût. Sur la base de ces facteurs, il devient évident qu'un sens de la mesure est nécessaire. Le bon sens nous dit qu'il serait ridicule d'insister pour que l'intégrité du système de sécurité d'une machine qui pourrait, au pire, causer des écrochures légères soit la même que celle du système requis pour garder un avion gros porteur en l'air. Les conséquences d'une défaillance sont radicalement différentes, nous devons donc avoir un moyen de mettre en adéquation l'étendue des mesures de protection avec le niveau de risque obtenu lors de l'étape d'estimation des risques.

Quel que soit le dispositif de protection choisi, il ne faut pas oublier qu'un "système de sécurité" peut contenir de nombreux éléments, notamment le dispositif de protection, le câblage, le commutateur de puissance et parfois des parties du système de commande de la machine. Tous ces éléments du système (notamment les gâches, les supports, le câblage, etc.) doivent avoir des caractéristiques de performance adaptées à leur principe de conception et à leur technologie. CEI/EN 62061 et EN ISO 13849-1 classent les niveaux hiérarchiques de performance des composants de sécurité des systèmes de commande et ils fournissent des méthodes d'évaluation des risques dans leurs annexes afin de déterminer les impératifs d'intégrité pour un système de protection.

ISO 13849-1:2006 fournit un graphique des risques amélioré dans son annexe A. Ce graphique est illustré à la figure 19.

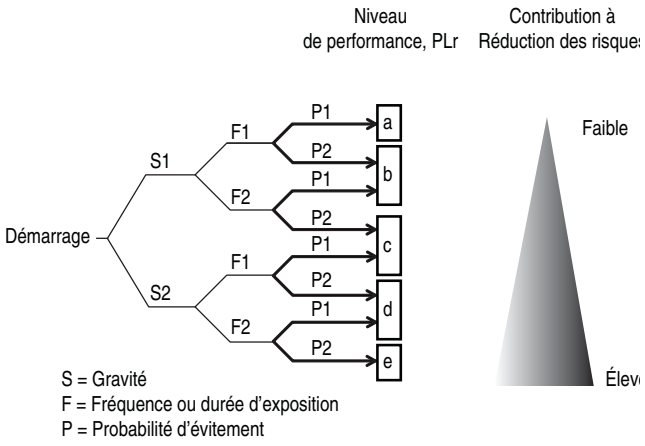


Figure 19 : Graphique des risques pour déterminer le niveau de performance requis pour une fonction de sécurité – tiré de ISO 13849-1:2006

CEI 62061 fournit également une méthode dans son annexe A, illustrée dans la figure 20.

Les deux méthodes ci-dessus donnent des résultats équivalents. Chaque méthode est prévue pour prendre en compte le contenu détaillé de la norme dont elle dépend.

Dans les deux cas, il est extrêmement important que les recommandations fournies dans le texte de la norme soient appliquées. Le graphique ou le tableau des risques ne doit pas être utilisé de façon isolée ou d'une manière trop simpliste.

Evaluation

Lorsque la mesure de protection a été choisie et avant de la mettre en œuvre, il est important de refaire une estimation des risques. Cette procédure est souvent oubliée. Si une mesure de protection est installée, l'opérateur peut se sentir totalement protégé contre les risques envisagés à l'origine. Et, parce qu'il n'a plus la même conscience du danger qu'au début, il peut intervenir sur la machine d'une façon différente. Il peut, par exemple, se trouver exposé au danger plus souvent, ou il peut pénétré plus profondément dans la machine. Cela signifie que si la mesure de protection est défaillante, il court un plus grand risque que celui envisagé à l'origine. C'est ce risque que nous devons estimer. Par conséquent, l'estimation des risques doit être refaite en prenant en considération tout changement prévisible dans la façon dont les personnes peuvent interagir avec la machine. Le résultat de cette activité est utilisé pour vérifier si les mesures de protection proposées sont réellement adaptées. Pour de plus amples informations, consulter l'annexe A de la norme CEI/EN 62061.

Formation, équipement de protection individuelle, etc.

Il est important que les opérateurs aient la formation adéquate sur les méthodes de travail en toute sécurité relatives à une machine. Cela ne veut pas dire que les autres mesures peuvent être négligées Il n'est pas acceptable de simplement dire à un opérateur de ne pas s'approcher des zones dangereuses (plutôt que de les protéger).

Il peut également être nécessaire pour un opérateur d'utiliser des équipements comme des gants spéciaux, des lunettes de protection, un appareil respiratoire, etc. Le concepteur de la machine doit préciser quels types d'équipements sont requis. L'utilisation d'un équipement de protection individuelle ne constitue généralement pas la méthode de protection principale, mais elle complète les mesures indiquées ci-dessus.

Évaluation des risques et mesures de sécurité

Document N° : _____
Partie de : _____

Produit : _____
Fourni par : _____
Date : _____

☐ Évaluation des risques pro
☐ Évaluation des risques intermédiaire
☐ Évaluation des risques complémentaire

Zone noire – mesures de sécurité nécessaires
Zone grise – mesures de sécurité recommandées

Conséquences Décès, perte d'un œil ou d'un bras	Gravité Se	Classe Cl 3-4	5-7	8-10	11-13	14-15	Fréquence et durée, Fr		Probabilité d'incident dangereux, Pr		Évitement, Av	
Permanentes, perte de doigts	4	SIL2	SIL2	SIL2	SIL3	SIL3	<=1 heure	5	Commun	5		
Réversibles, intervention médicale	3		OM	SIL1	SIL2	SIL2	> 1 heure – <+ jour	5	Probable	4		
Réversibles, premier secours	2			OM	SIL1	SIL2	> 1 jour – <= 2 sem.	4	Possible	3	Impossible	5
	1				OM	SIL1	> 2 sem. – <= 1 an	3	Rarement	2	Possible	3
							> 1 an	2	Négligeable	1	Probable	1

Ser. N°	Dgr. N°	danger	Se	Fr	Pr	Av	Cl	Mesure de sécurité	Sécurité

Commentaires

Figure 20 : Tableau servant à déterminer le niveau d'intégrité de la sécurité requis pour une fonction de sécurité – tiré de CEI 62061

Normes

De nombreuses normes et rapports techniques fournissent des recommandations pour l'évaluation des risques. Certains s'adressent à des applications générales et d'autres à des applications spécifiques. La liste suivante présente des normes qui contiennent des informations sur l'évaluation des risques.

ANSI B11.TR3 : Evaluation et réduction du risque – Un guide pour estimer, évaluer et réduire les risques associés aux machines-outils.

ANSI PMMI B155.1 : Critères de sécurité pour les machines de conditionnement et les machines de conversion apparentées au conditionnement.

ANSI RIA R15.06 : Impératifs de sécurité pour les robots industriels et les systèmes robotisés.

AS 4024.1301-2006 : Principes de l'évaluation du risque.

CSA Z432-04 : Protection des machines

CSA Z434-03 : Robots industriels et systèmes robotisés – Critères généraux de sécurité

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

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

EN ISO 13849-1 : Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1 : principes généraux de conception

EN ISO 14121-1 : Sécurité des machines – Appréciation du risque – Partie 1 : principes

EN TR 14121-2 : Sécurité des machines – Appréciation du risque – Partie 2 : lignes directrices pratiques et exemples de méthodes

Mesures de protection et équipement complémentaire

Lorsque l'évaluation des risques montre qu'une machine ou un procédé présente un risque de blessure, le danger doit être éliminé ou limité. La façon dont cela est réalisé dépend de la nature de la machine et du danger. Les mesures de protection combinées à un dispositif de protection empêchent l'accès à la source du danger ou suppriment le mouvement dangereux lorsque l'accès est possible. Les barrières de protection interconnectées, les barrières immatérielles, les tapis de sécurité, les commandes bimanuelles et les poignées de sécurité sont des exemples de mesures de protection typiques.

Les dispositifs et systèmes d'arrêt d'urgence sont associés aux systèmes de commande de sécurité mais ce ne sont pas des systèmes fournissant une protection directe, ils ne doivent être considérés que comme des mesures de protection complémentaires.

Empêcher l'accès

Barrières englobantes fixes

Si le danger se trouve sur une partie de la machine à laquelle il n'est pas nécessaire d'accéder, une protection doit être fixée de façon permanente sur la machine, comme illustré à la figure 21. Ces types de protections doivent nécessiter des outils pour leur retrait. Les protections fixes doivent pouvoir 1) résister à leur environnement d'utilisation, 2) contenir les projectiles lorsque c'est nécessaire et 3) ne pas créer de danger, en ayant par exemple des bords tranchants. Les protections fixes peuvent avoir des ouvertures aux points de contact avec la machine ou des ouvertures lorsque du treillis métallique est utilisé pour l'armoire.

Les fenêtres constituent des moyens pratiques pour surveiller le fonctionnement de la machine, lorsque l'accès à cette partie de la machine n'est pas possible. Le matériau doit être choisi avec précaution parce que les interactions des produits chimiques avec les liquides de coupe, les rayons ultra-violets et également le vieillissement peuvent entraîner une dégradation des matériaux de la fenêtre avec le temps.

Mesures de protection et équipement complémentaire

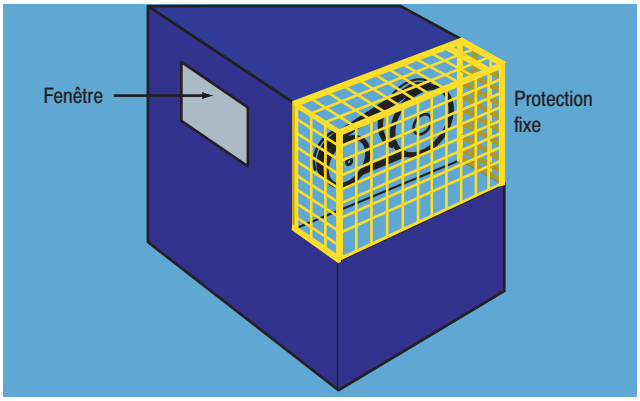


Figure 21 : Protections fixes

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

Détection d'accès

Des mesures de protection peuvent être utilisées pour détecter l'accès à une zone dangereuse. Lorsque la détection est choisie 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 fournit pas le niveau de réduction des risques nécessaire.

Ce système de sécurité est généralement constitué de trois blocs : 1) un dispositif d'entrée qui détecte l'accès à la zone dangereuse, 2) un dispositif logique qui traite les signaux du dispositif de détection, vérifie l'état du système de sécurité et active ou désactive les dispositifs de sortie, et 3) un dispositifs de sortie qui commande l'actionneur (par exemple un moteur). La figure 22 montre le schéma fonctionnel d'un système de sécurité simple.

Figure 22 : Schéma fonctionnel d'un système de sécurité simple

Dispositifs de détection

De nombreux dispositifs alternatifs existent pour détecter la présence d'une personne pénétrant ou déjà présente dans la zone dangereuse. Le meilleur choix pour une application spécifique dépend de plusieurs facteurs.

- Fréquence d'accès
- Temps d'arrêt de la source du danger
- Importance à terminer le cycle de la machine
- Confinement des projectiles, liquides, pulvérisations, vapeurs, etc.

Les protections amovibles adaptées peuvent être interconnectées afin de fournir une protection contre les projectiles, les liquides, les pulvérisations et autres types de dangers ; elles sont également souvent utilisées lorsque l'accès à la zone dangereuse est peu fréquent. Les barrières de protection interconnectées peuvent également être verrouillées afin d'empêcher l'accès lorsque la machine est en milieu de cycle et lorsqu'elle prend beaucoup du temps pour s'arrêter.

Les dispositifs de détection de présence, comme les barrières immatérielles, les tapis et les scrutateurs, permettent un accès rapide et facile à la zone dangereuse et sont souvent choisis lorsque les opérateurs doivent souvent accéder à cette zone dangereuse. Ces types de dispositifs ne fournissent pas de proctection contre les projectiles, les vaporisations, les liquides et autres types de danger.

Le meilleur choix en matière de mesure de protection est un dispositif ou un système qui fournit le maximum de protection avec le minimum de gêne pour le fonctionnement normal de la machine. Tous les aspects de l'utilisation de la machine doivent être pris en considération ; ceci parce que l'expérience montre qu'un système difficile à utiliser a plus de chance d'être retiré ou contourné.

Dispositifs de détection de présence

Lors du choix de la méthode retenue pour protéger une zone ou un périmètre, il est important d'avoir une bonne connaissance des fonctions de sécurité qui sont requises.

En général il y a au moins deux fonctions.

1. Coupure ou désactivation de l'alimentation lorsqu'une personne pénètre dans la zone dangereuse.
2. Empêcher l'enclenchement ou l'activation de l'alimentation lorsqu'une personne se trouve dans la zone dangereuse.

A première vue, ces deux fonctions sembles identiques, mais bien qu'elles soient clairement liés, et sont bien souvent mises en application avec les mêmes équipements, ce sont en réalité deux fonctions séparées. Pour la première fonction, il est nécessaire d'utiliser un actionneur quelconque. En d'autres termes, un dispositif qui détecte qu'une partie du corps d'une personne a dépassé un certain point et qui envoie un signal pour couper l'alimentation. Si la personne peut alors continuer au delà de ce point de déclenchement et si sa présence n'est plus détectée, alors la deuxième fonction (prévention de l'activation) ne peut pas être réalisée.

La figure 23 donne un exemple d'accès de tout le corps avec une barrière immatérielle montée verticalement comme actionneur. Les barrières de protection interconnectées peuvent également être considérées comme un dispositif de déclenchement uniquement lorsque rien n'empêche la barrière d'être refermée après la pénétration.

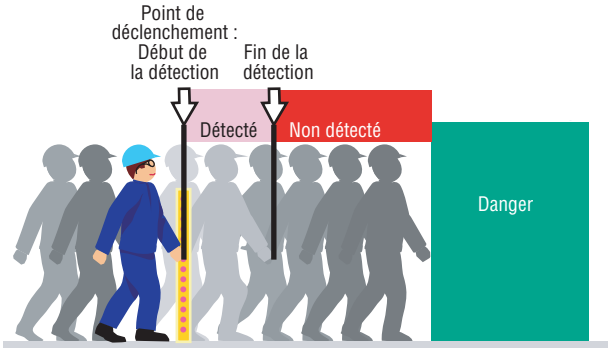


Figure 23 : Accès du corps entier

Si l'accès de tout le corps n'est pas possible, lorsqu'une personne ne peut pas continuer après le point de déclenchement, sa présence est toujours détectée et la deuxième fonction (empêcher l'enclenchement) est réalisée.

Pour les applications ne concernant qu'une partie du corps, comme sur la figure 24, les mêmes types de dispositifs réalisent le déclenchement et la détection de présence. La seule différence étant le type d'application.

Les dispositifs de détection de présence sont utilisés pour détecter la présence de personnes. Les dispositifs incluent les barrières immatérielles de sécurité, les sépartateurs de sécurité à un faisceau, les scrutateurs de zone de sécurité, les tapis de sécurité et les bourrelets de sécurité

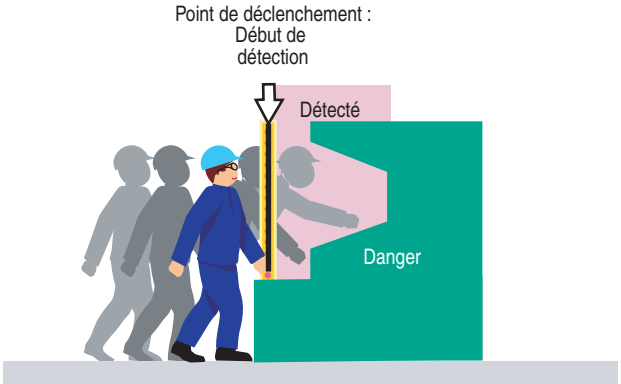


Figure 24 : Accès d'une partie du corps

Barrières immatérielles de sécurité

Les barrières immatérielles de sécurité peuvent simplement être décrites comme des détecteurs de présence photoélectriques spécialement conçus pour protéger le personnel des blessures liées au mouvement dangereux d'une machine. Egalement appelées dispositifs protecteurs optoélectroniques actifs (AOPD - Active Opto-electronic Protective Device) ou équipement de protection électro-sensible (ESPE - Electro Sensitive Protective Equipment), les barrières immatérielles offrent une sécurité optimale, tout en permettant une meilleure productivité et en étant plus ergonomiques que les protections mécaniques. Elles sont particulièrement bien adaptées aux applications dans lesquelles le personnel doit fréquemment accéder à une zone dangereuse.

Les barrières immatérielles sont conçues et testées en conformité avec la norme CEI 61496-1 et -2. Il n'existe pas de version EN harmonisée de la partie 2, l'annexe IV de la directive européenne relatives aux machines requiert donc une certification tierce pour les barrières immatérielles avant qu'elles ne soient mises sur le marché dans l'Union européenne. Les organismes tiers testent les barrières immatérielles afin de se conformer à cette norme internationale. Underwriter's Laboratory a adopté la norme CEI 61496-1 sous la forme d'une norme nationale américaine.

Fonctionnement

Les barrières immatérielles sont composées d'un émetteur et d'un récepteur qui crée une barrière multi-faisceaux de lumière infrarouge devant, ou autour, d'une zone dangereuse. L'émetteur est synchronisé avec le récepteur par le faisceau photoélectrique le plus proche d'une extrémité du boîtier. Pour éliminer la sensibilité aux déclenchements intempestifs liés à la lumière ambiante et aux interférences (diaphonie) des autres dispositifs optoélectroniques, les voyants à DEL de l'émetteur sont pulsés à une fréquence spécifique (modulation de fréquence), avec chaque DEL pulsée séquentiellement de façon à ce qu'un émetteur ne puisse affecter que le récepteur qui lui est spécifiquement associé. Lorsque tous les faisceaux ont été vérifiés, la scrutation recommence. Un exemple de barrière immatérielle de base est illustré figure 25.

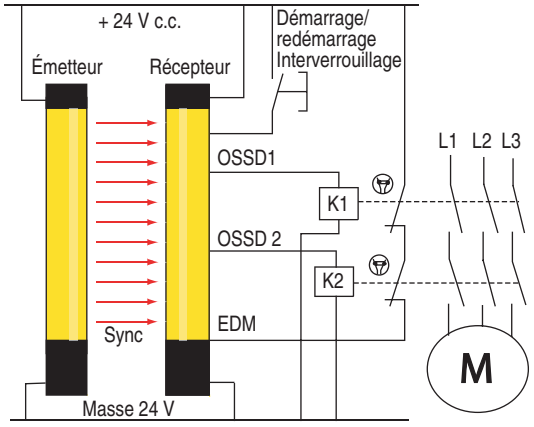


Figure 25 : Barrière immatérielle de sécurité de base

Lorsque l'un des faisceaux est interrompu par une intrusion dans le champ de détection, le circuit de commande de la barrière immatérielle désactive ses signaux de sortie. Le signal de sortie doit être utilisé pour désactivé le danger. La plupart des barrières immatérielles ont des sorties OSSD (dispositif de commutation de signal de sortie). Les OSSD sont des transistors de type PNP avec protection contre les courts-circuits, les surcharges et détection des défauts transversaux (voie à voie). Ils peuvent commuter des dispositifs alimentés en c.c., comme des contacteurs de sécurité et des relais de commande de sécurité, généralement jusqu'à 500 mA.

Verrouillage du démarrage/redémarrage : Les barrières immatérielles sont conçues pour dialoguer directement avec des actionneurs machine de faible puissance ou des dispositifs logiques, comme des relais de surveillance ou des automates de sécurité programmables. Lorsque les actionneurs machine sont commutés directement, l'entrée de verrouillage du démarrage/redémarrage de la barrière immatérielle doit être utilisée. Cela empêche la barrière immatérielle de réinitialiser la source du danger lorsque la barrière immatérielle est mise sous tension ou lorsqu'elle est remise à zéro.

Contrôle des contacteurs commandés (EDM) : Les barrières immatérielles ont également une entrée qui leur permet de surveiller les actionneurs de la machine. Cela s'appelle la surveillance des contacteurs commandés ou EDM pour « external device monitoring ». Lorsque la barrière immatérielle est remise à zéro, elle détermine si l'actionneur externe est désactivé avant d'activer un redémarrage.

L'émetteur et le récepteur peuvent également être interfacés avec un bloc logique de sécurité qui fournit le programme logique, les sorties, les diagnostics système et les fonctions supplémentaires (inhibition, masquage, initialisation par dispositif de détection de présence) nécessaires pour l'application.

La barrière immatérielle doit pouvoir envoyer un signal d'arrêt à la machine, même en cas de défaillance d'un composant. Les barrières immatérielles ont deux sorties surveillées transversales qui doivent changer d'état lorsque le champ de détection de la barrière immatérielle de sécurité est interrompu. Si l'une des sorties est défaillante, l'autre sortie répond et envoie un signal d'arrêt à la machine commandée et, dans le cadre du système de surveillance transversal, détecte que l'autre sortie n'a pas changé d'état ou répondu. La barrière immatérielle se met alors en état de condamnation, ce qui empêche la machine de fonctionner jusqu'à ce que la barrière immatérielle de sécurité soit réparée. Le réarmement de la barrière immatérielle de sécurité ou sa remise sous tension ne réinitialise pas la condition de condamnation.

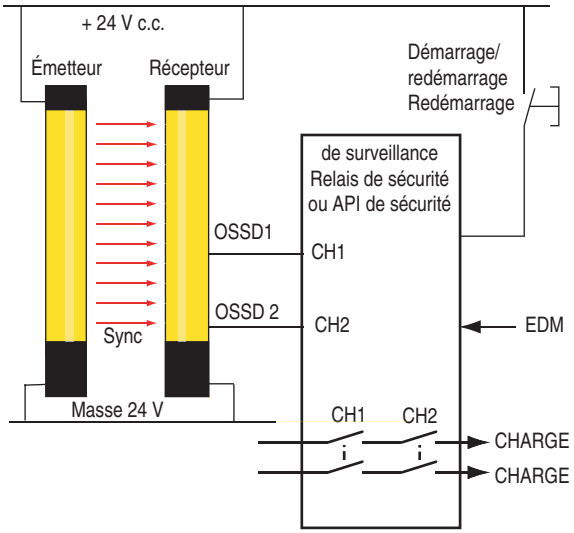


Figure 26 : Barrière immatérielle interfacée avec relais de surveillance ou automate de sécurité

Les barrières immatérielles sont souvent intégrées dans le système de sécurité en les raccordant à un relais de surveillance (MSR - Monitoring safety relais) ou un automate de sécurité, comme illustré sur la figure 26. Dans ce cas, le MSR ou l'automate de sécurité gère la coupure des charges, le verrouillage du démarrage/redémarrage et la surveillance du dispositif externe. Cette approche est utilisée pour les fonctions de sécurité complexes et pour la coupure de charges importantes. Ceci réduit également le câblage de la barrière immatérielle.

Résolution :

L'un des critères de sélection important pour les barrières immatérielles est sa résolution. La résolution est la taille maximale théorique que doit avoir un objet pour toujours déclencher la barrière immatérielle. Les résolutions souvent utilisées sont de 14 mm (couramment utilisée pour la détection des doigts), 30 mm (couramment utilisée pour la détection de la main) et 50 mm (couramment utilisée pour la détection d'une cheville). Des valeurs plus élevées sont utilisées pour la détection de tout le corps.

La résolution est l'un des facteurs qui détermine la distance minimale à laquelle la barrière immatérielle peut être placée par rapport au danger. Voir la section sur le « Calcul de la distance de sécurité ».

Mesures de protection et équipement complémentaire

Applications verticales :

Les barrières immatérielles sont le plus souvent utilisées dans des applications à montage vertical. La barrière immatérielle doit être placée à une distance suffisante pour empêcher qu'une personne ne puisse atteindre le danger avant son arrêt.

Dans les applicastions qui nécessite un franchissement, l'interruption de la barrière immatérielle initie une commande d'arrêt du danger. Lorsqu'il franchit la barrière, pour charger ou décharger les pièces par exemple, l'opérateur est protégé parce que certaines parties de son corps bloquent la barrière immatérielle et empêchent le redémarrage de la machine.

Les barrières fixes ou les protections supplémentaires doivent empêcher l'opérateur de franchir la barrière immatérielle, que ce soit en passant par dessus, par dessous ou sur les côtés. La figure 27 montre un exemple d'application verticale.

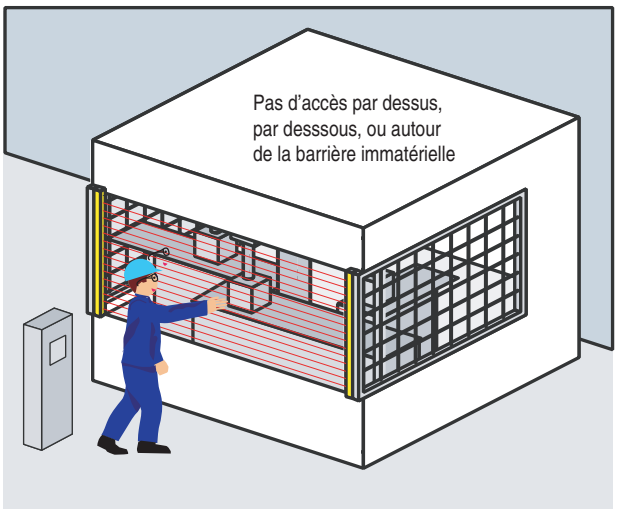


Figure 27 : Application verticale

En cascade

L'installation en cascade est une technique utilisée pour raccorder un jeu de barrières immatérielles directement à un autre, comme sur la figure 28. Un jeu agit comme l'hôte, l'autre agit comme un auxiliaire. Une troisième barrière immatérielle peut être ajoutée comme deuxième auxiliaire. Cette approche réduit les coûts de câblage et les bornes d'entrée sur le dispositif logique. En contre-partie, le temps de réponse des barrières immatérielles en cascade est plus long puisque plus de faisceaux doivent être vérifiés à chaque scrutation des barrières immatérielles.

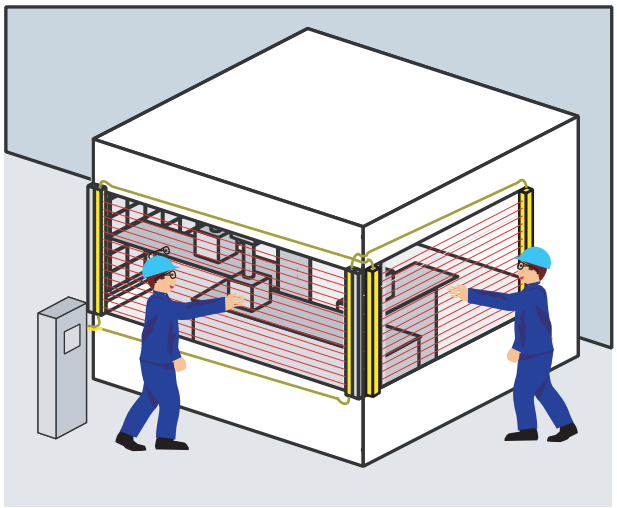


Figure 28 : Barrières immatérielles en cascade

Masquage fixe

Le masquage permet à des parties du champ de détection d'une barrière immatérielle d'être désactivée afin de laisser passer les objets généralement associés au processus. Ces objets doivent être ignorés par la barrière immatérielle, qui doit continuer à fournir une détection de l'opérateur.

La figure 29 montre un exemple où l'objet est stationnaire. Les accessoires de montage, les éléments de la machine, les outils ou le convoyeur sont dans la partie désactivée de la barrière immatérielle. Appelé masquage fixe surveillé, cette fonction nécessite que l'objet se trouve dans la zone définie à tout moment. Si l'un des faisceaux programmés pour être « masqué » n'est pas bloqué par l'accessoire ou la pièce de travail, un signal d'arrêt est envoyé à la machine.

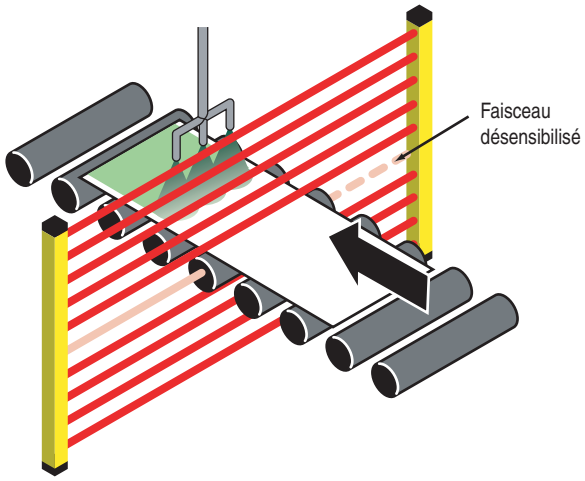


Figure 29 : Barrière immatérielle masquée où le convoyeur est installé

Masquage flottant

Le masquage flottant permet à un objet, comme la matière première, de pénétrer dans le champ de détection en tout point sans arrêter la machine. Pour cela, un ou deux faisceaux sont désactivés dans le champ de détection. Au lieu de créer une fenêtre fixe, les faisceaux désactivés se déplacent de haut en bas, ou « flottent », en fonction des besoins.

Le nombre de faisceaux pouvant être désactivés dépend de la résolution. Deux faisceaux peuvent être désactivés avec une résolution de 14 mm, mais un seul faisceau peut être désactivé avec une résolution de 30 mm. Cettre restriction permet de garder une ouverture plus petite afin d'empêcher l'opérateur de franchir les faisceaux désactivés.

N'importe quel faisceau du champ de détection peut être bloqué, sauf le faisceau de synchronisation, sans que le système envoie un signal d'arrêt à la machine protégée. Un frein de presse, illustré à la figure 30, en est un bon exemple. Lorsque le piston descend, la feuille de métal se plie et se déplace dans la barrière immatérielle, n'interrompant qu'un ou deux faisceaux adjacents à la fois.

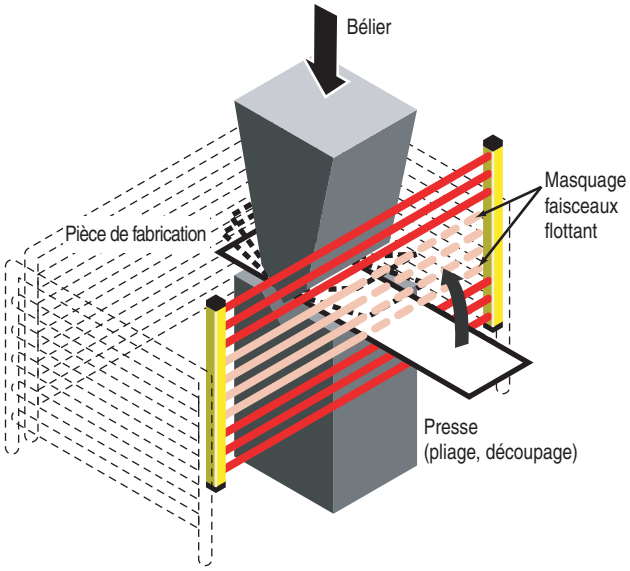


*Figure 30 : Masquage*flottant

Lorsque le masquage fixe ou flottant est utilisé, la distance de sécurité (distance minimale entre la barrière immatérielle et le danger pour que l'opérateur ne puisse atteindre la source du danger avant que la machine ne soit arrêtée) est affectée. Puisque le masquage augmente la taille minimale des objets pouvant être détectés, la distance de sécurité minimale doit également être augmentée selon la formule utilisée pour calculer la distance de sécurité minimale (voir la section sur le calcul de la distance de sécurité).

Applications horizontales

Après avoir calculé la distance de sécurité, le concepteur peut découvrir que l'opérateur de la machine peut franchir l'espace entre la barrière immatérielle et le danger. Si cet espace est supérieur à 300 mm (12 in.), des précautions supplémentaires doivent être envisagées. Une solution consiste à monter une deuxième barrière immatérielle en position horizontale. Cela peut être deux jeux de barrières immatérielles indépendants ou deux barrières immatérielles en cascade. Une autre solution consiste à monter une barrière immatérielle plus longue avec un angle par rapport à la machine. Ces solutions sont illustrées à la figure 31. Dans les deux solutions, les barrières immatérielles doivent être placées à une distance suffisante du danger pour la sécurité.

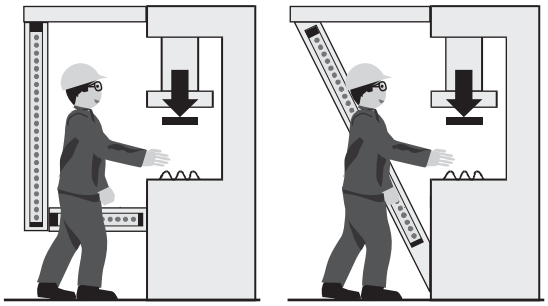


Figure 31 : Solutions alternatives pour l'espacement entre la barrière immatérielle et le danger

Pour les distances de sécurité plus longues ou pour la détection périmétrique, les barrières immatérielles peuvent être montées horizontalement, comme illustré sur la figure 32. Les barrières immatérielles ne doivent pas être montées trop près du sol pour qu'elles ne s'encrassent pas, et pas trop hautes pour qu'une personne ne puisse pas se glisser dessous. Une distance de 300 mm (12 in.) au-dessus du sol est fréquente. De plus, la barrière immatérielle ne doit pas être utilisée comme marchepied pour accéder au périmètre. La résolution de la barrière immatérielle doit être sélectionnée de façon à détecter au moins la cheville d'une personne. Pour la détection d'une cheville, la résolution ne doit pas être supérieure à 50 mm. Si la barrière immatérielle ne protège pas toute la cellule, une fonction de réarmement manuel doit être utilisée. Le bouton de réarmement doit être situé en dehors de la cellule avec une vue complète de celle-ci.

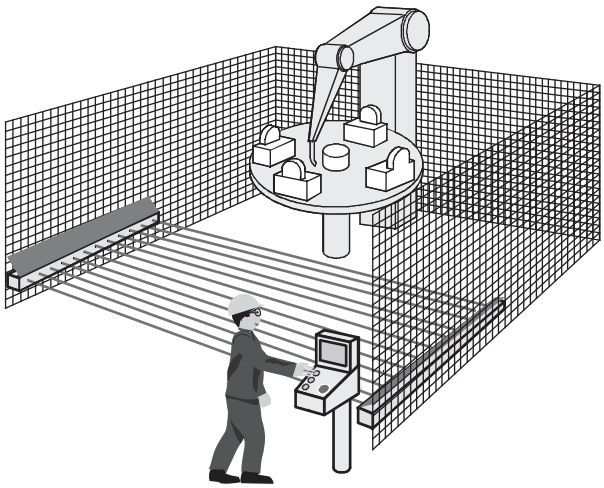


Figure 32 :Installation horizontale d'une barrière immatérielle

Contrôle d'accès périmétrique ou de zone

Le contrôle d'accès périmétrique est souvent utilisé pour détecter l'accès sur le contour extérieur d'une zone dangereuse. Les barrières immatérielles utilisées pour détecter l'accès périmétrique ont des résolutions permettant de détecter le corps entier, comme illustré à la figure 33. Cela peut être obtenu de différentes façons. Des barrières immatérielles multi-faisceaux avec deux ou trois faisceaux ou un dispositif à un faisceau qui se reflète dans des miroirs afin de créer un schéma à deux faisceaux sont souvent utilisés. Dans les deux cas, le faisceau le plus bas doit être à 300 mm (12 in.) au dessus du sol, et le faisceau le plus haut doit empêcher une personne de simplement passer par dessus la barrière immatérielle.

Les miroirs peuvent être utilisés afin de dévier le faisceau lumineux autour d'une cellule. La distance que la barrière lumineuse peut couvrir est limitée par les pertes dues aux reflexions dans les miroirs. L'alignement de la barrière immatérielle est plus difficile et un outil d'alignement avec laser visible est souvent nécessaire pour l'installation.

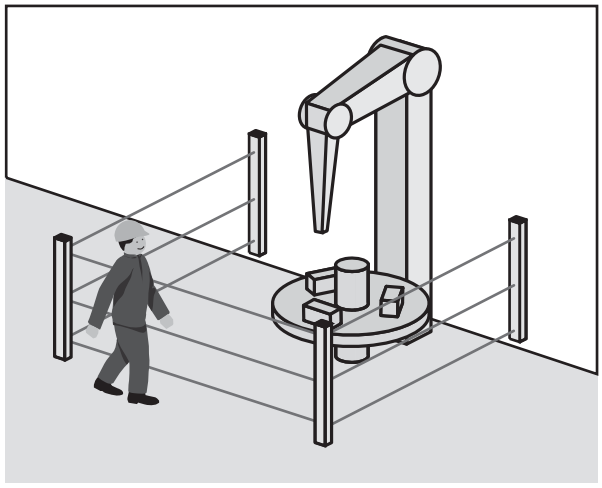


Figure 33 : Des miroirs créent le périmètre

Les miroirs peuvent être utilisés afin de dévier le faisceau lumineux autour d'une cellule. La distance que la barrière lumineuse peut couvrir est limitée par les pertes dues aux reflexions dans les miroirs. L'alignement de la barrière immatérielle est plus difficile et un outil d'alignement avec laser visible est souvent nécessaire pour l'installation.

Mesures de protection et équipement complémentaire

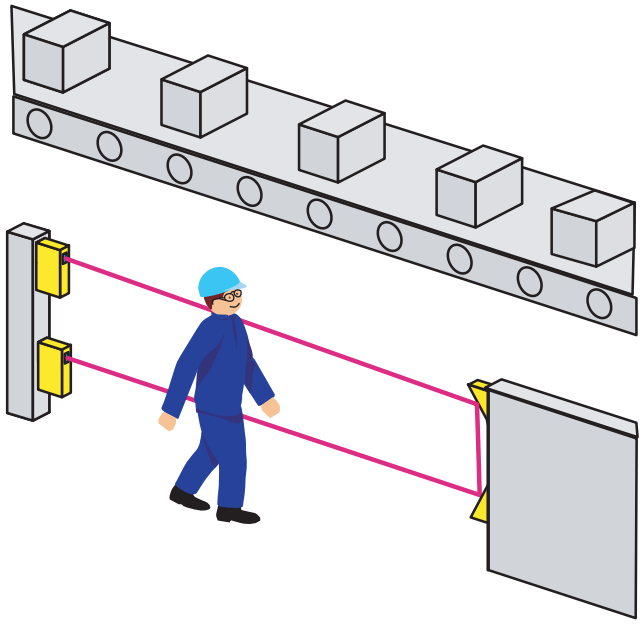


Figure 34 : Dispositifs à un faisceau pour les applications dont le risque est faible

Certains dispositifs à un faisceau présentent de longues distances de détection (jusqu'à 83 m ou 275 pieds). Cela permet à un dispositif à un faisceau de créer une barrière protectrice autour des machines dangereuses. Etant donné que seul un agencement à un ou deux faisceaux est possible, cette approche est limitée aux applications dont le risque est faible. La section sur le "Calcul de la distance de sécurité" (page) aborde le positionnement et l'espacement des faisceaux afin d'obtenir des champs de protection adéquats. La figure 34 montre un exemple d'application à un faisceau. Cette approche est généralemnet utilisée dans les applications dont le risque est faible, en raison de l'espacement plus grand entre les faisceaux. L'interruption du faisceau entraîne l'arrêt du mouvement dangereux de la machine.

Scrutateurs laser de sécurité

Les scrutateurs laser de sécurité utilisent un miroir rotatif pour refléter les impulsions lumineuses sur un arc, ce qui crée un plan de détection. L'emplacement de l'objet est déterminé par l'angle de rotation du miroir. En utilisant une technique basée sur la « vitesse de la lumière » d'un faisceau de lumière invisible réfléchi, le scrutateur peut également détecter la distance entre l'objet et le scrutateur. En prenant la distance mesurée et l'emplacement de l'objet, le scrutateur laser détermine la position exacte de l'objet.

Les scrutateurs laser créent deux zones : 1) une zone d'alarme et 2) une zone de protection. La zone d'alarme fournit un signal qui n'arrête pas la source du danger mais informe les personnes qu'ils approchent de la zone de protection, comme illustré à la figure 35. Les objets qui pénètrent ou qui sont à l'intérieur de la zone de protection provoquent l'envoi d'une commande d'arrêt par le scrutateur laser, les sorties OSSD sont désactivées.

La forme et la taille de la zone protégée est configurée par un logiciel chargé dans le scrutateur. Le calcul de la distance de sécurité doit être utilisée pour déterminer la taille appropriée pour la zone de protection.

Un des avantages du scrutateur laser par rapport aux barrières immatérielles horizontales ou aux tapis, est la capacité de reconfiguration de la zone. La figure 35 montre un exemple du champ d'alarme configuré pour ignorer les objets structurels.

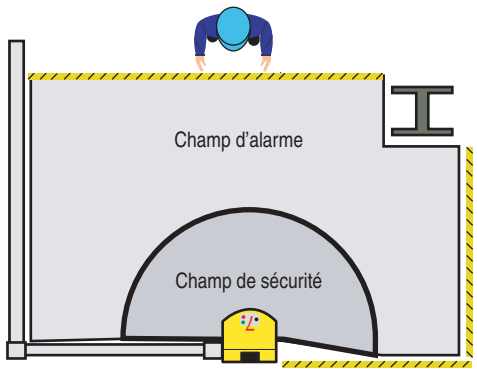


Figure 35 : Champ d'alarme configuré autour des objets structurels

Les avancées de la technologie des scrutateurs laser permettent à un seul scrutateur de couvrir plusieurs zones. Dans la figure 36, le scrutateur laser permet l'accès de l'opérateur par un côté (montré dans le cas 1) alors que le robot fonctionne de l'autre côté (cas 2).

Les scrutateurs plus anciens possèdent des sorties électromécaniques. Les scrutateurs plus récents adoptent les mêmes principes que les barrières immatérielles et permettent des sorites OSSD avec vérification transversale, la surveillance de dispositif externe et le verrouillage de redémarrage pour une utilisation autonome. Les sorties OSSD peuvent également être raccordées aux dispositifs logiques lorsque c'est nécessaire pour un système plus étendu.

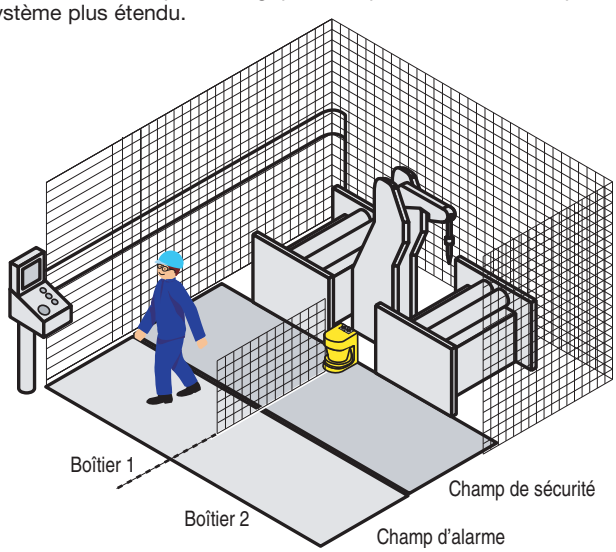


Figure 36 : Application multizone d'un scrutateur laser

Inhibition

L'inhibition est caractérisée comme la suspension temporaire et automatique d'une fonction de sécurité. Parfois, le processus nécessite que la machine soit arrêtée lorsque des personnes pénètrent dans la zone, mais qu'elle continue de fonctionner lorsque des matériaux sont alimentés automatiquement dans la zone. Dans ce cas, une fonction d'inhibition est nécessaire. L'inhibition est autorisée pendant la portion non dangereuse du cycle de la machine ou elle ne doit pas exposer les personnes à un danger.

Des détecteurs sont utilisés pour initier la fonction d'inhibition. Les détecteurs peuvent être classés comme détecteurs de sécurité ou non. Les types, le nombre et le positionnement des détecteurs d'inhibition doivent être sélectionnés afin de répondre aux exigences de sécurité définies par l'évaluation des risques.

La figure 37 montre une installation typique d'inhibition avec deux détecteurs pour convoyeur de matériau. Les détecteurs sont positionnés selon un schéma en X. Certains dispositifs logiques nécessitent un ordre précis pour le blocage des détecteurs. Lorsque l'ordre est important, le schéma en X doit être asymétrique. Pour les dispositifs logiques qui utilisent les entrées du détecteur par paire, le schéma en X peut être symétrique. Des cellules photoélectriques réflex polarisées sont souvent utilisées pour empêcher les réflexions parasites d'initier de façon injustifiée la fonction d'inhibition, ou de provoquer des déclenchements intempestifs. D'autres technologies de détection, comme les détecteurs à induction et les interrupteurs de fin de course, peuvent être employées.

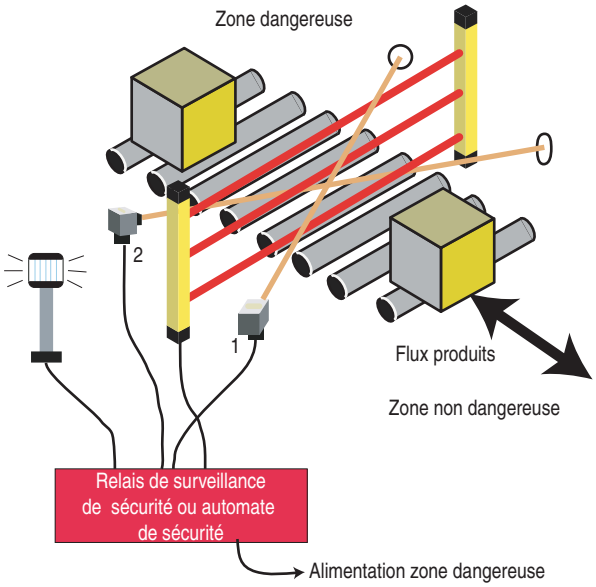


Figure 37 : Inhibition à 2 détecteurs pour convoyeur

Une autres approche couramment utilisée est l'utilisation de quatre détecteurs, comme illustré à la figure 38. Deux détecteurs sont montés du côté du danger et deux de l'autre côté. Les détecteurs sont orientés directement vers le côté opposé du convoyeur. La forme et la position de l'objet est moins importante dans cette approche. La longueur de l'objet est importante puisque l'objet doit bloquer les quatre détecteurs.

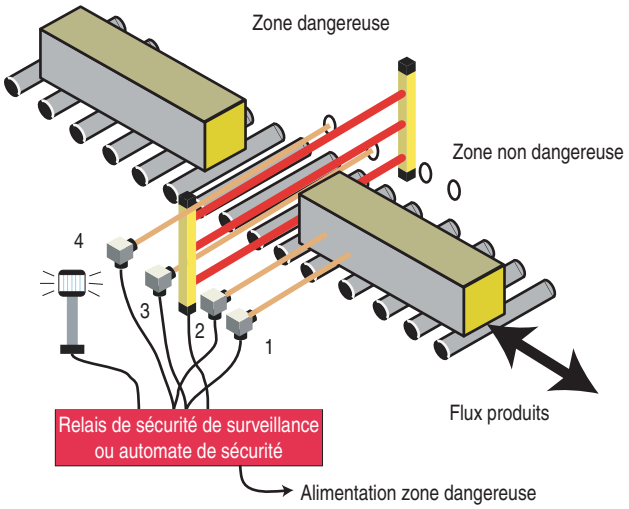


Figure 38 : Inhibition à 4 détecteurs pour convoyeur

L'accès d'un chariot-élévateur au convoyeur est une application courante. Pour inhiber la barrière immatérielle, le chariot-élévateur doit être détecté par les détecteurs. Le défi consiste à positionner les détecteurs pour qu'ils détectent le chariot-élévateur et non une personne. La figure 39 montre un exemple de cette application.

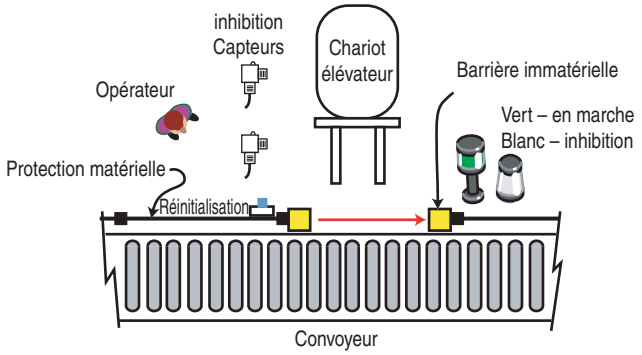


Figure 39 : Inhibition à 2 détecteurs pour chariot-élévateur

L'accès aux cellules robotisées se fait également par inhibition. Comme illustré à la figure 40, des interrupteurs de fin de course situés à la base du robot indiquent la position du robot. Les dispositifs de protection (les barrières immatérielles et les tapis de sécurité) sont inhibés lorsque le robot n'est pas dans une position dangereuse.

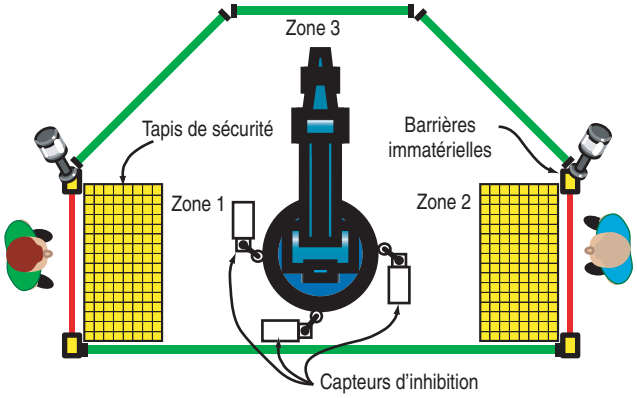


Figure 40 : Inhibition d'une cellule robotisée

Initialisation par dispositif de détection de présence (PSDI)

Egalement appelée mode de fonctionnement à une coupure, à deux coupures ou pas à pas, la PSDI implique l'utilisation d'une barrière immatérielle non seulement comme dispositif de sécurité, mais également comme dispositif de contrôle pour le fonctionnement de la machine. PSDI initie un cycle machine sur la base du nombre de fois que le champ de détection a été coupé. Par exemple, lorsqu'un opérateur avance le bras vers la source de danger pour insérer une pièce à travailler, l'interruption des faisceaux arrête immédiatement la machine ou empêche son redémarrage jusqu'à ce que l'opérateur retire sa main de la zone, la machine initie alors immédiatement un nouveau cycle. Ce processus peut être réalisé grâce à des dispositifs logiques de sécurité programmables ou des relais de surveillance spécialement conçus pour cette fonction.

L'auto-initialisation permet à la machine de démarrer et de s'arrêter en fonction du nombre de fois où les faisceaux de la barrière immatérielle ont été interrompus et rétablis. Le mode d'auto-initialisation à deux coupures (après la séquence de démarrage initiale) est illustré sur les figures 41 à 43.

A l'étape 1, l'opérateur coupe la barrière immatérielle. La machine est arrêtée et l'opérateur retire le matériau traité. L'opérateur se dégage de la barrière immatérielle, ce qui provoque la première coupure.

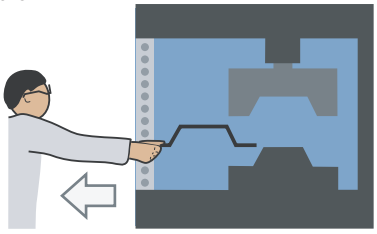


Figure 41 : Etape 1 de PSDI à deux coupures

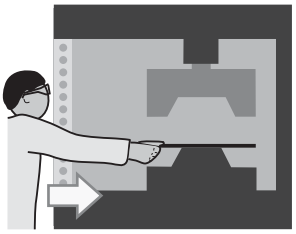


Figure 42 : Etape 2 de PSDI à deux coupures

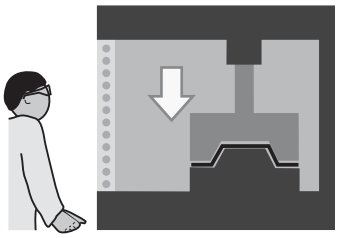


Figure 43 : Etape 3 de PSDI à deux coupures

A l'étape 2, l'opérateur coupe la barrière immatérielle une deuxième fois et charge le nouveau matériau. La machine reste arrêtée.

A l'étape 3, la machine démarre automatiquement lorsque la barrière immatérielle a été dégagée pour la deuxième fois.

Tapis de sécurité sensibles à la pression

Ces dispositifs sont utilisés pour fournir une protection d'un périmètre au sol autour d'une machine, comme illustré à la figure 44. Une matrice de tapis interconnectés est placée autour de la zone dangereuse et une pression exercées sur le tapis (p. ex., lorsqu'un opérateur marche sur le tapis) provoque la coupure de l'alimentation de la source de danger par le bloc logique de sécurité du tapis.

Plusieurs technologies sont utilisées pour créer des tapis de sécurité. Une des technologies les plus populaires consiste à utiliser deux plaques de métal parallèles, comme illustré à la figure 45. Les plaques sont séparées par des entretoises. Ces plaques et entretoises sont enveloppés d'un matériau non conducteur avec une surface antidérapante.

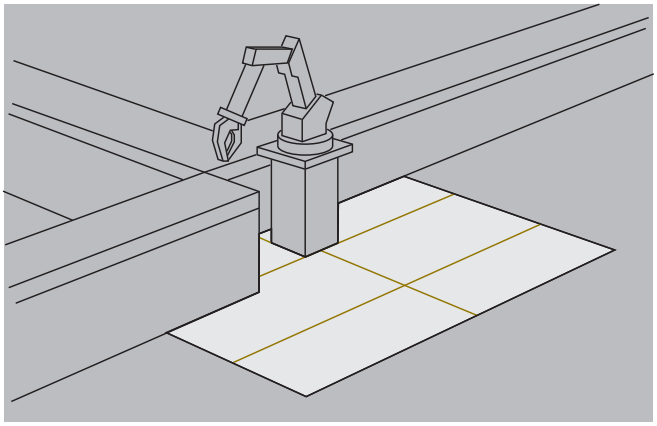


Figure 44 : Tapis de sécurité entourant un robot

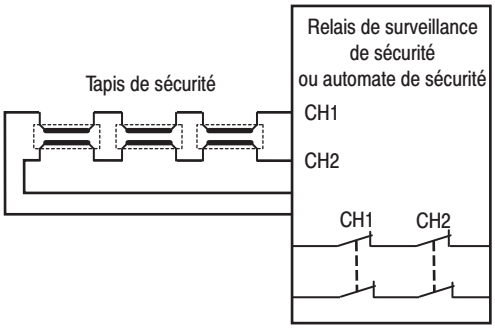


Figure 45 : Interfaçage de tapis de sécurité

Pour s'assurer que le tapis de sécurité est prêt à être utilisé, un courant électrique circule dans les deux plaques. Si un défaut de circuit ouvert se produit, le système de sécurité s'arrête. Pour intégrer les plaques parallèles dans un système de sécurité, deux ou quatre conducteurs sont utilisés. Si deux conducteurs sont utilisés, une résistance de terminaison est utilisée pour différencier les deux plaques. L'utilisation de quatre conducteurs est plus courante.Deux conducteurs, connectés à la plaque du haut sont attribués à une voie. Deux conducteurs, connectés à la plaque du bas sont attribués à une deuxième voie. Lorsqu'une personne marche sur le tapis, les deux plaques créent un court-circuit entre la voie 1 et la voie 2. Le dispositif logique de sécurité doit être conçu pour permettre ce court-circuit. La figure 46 montre un exemple de la façon dont plusieurs tapis à 4 fils sont raccordés en série afin de s'assurer que les tapis de sécurité sont prêts à être utilisés.

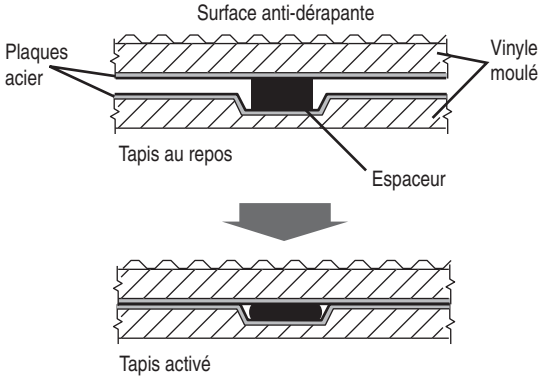


Figure 46 : Construction typique d'un tapis de sécurité

Les tapis sensibles à la pression sont souvent utilisés dans une zone fermée contenant plusieurs machines ; par exemple, fabrication flexible ou cellules robotisés. Lorsque l'accès à la cellule est nécessaire (par exemple pour le réglage ou l'"apprentissage" du robot), ils empêchent un mouvemnet dangereux si l'opérateur s'écarte de la zone de sécurité, ou s'il doit passer derrière un équipement, comme illustré à la figure 47.

La taille et la position du tapis doit prendre en compte la distance de sécurité (voir le calcul de la distance de sécurité).

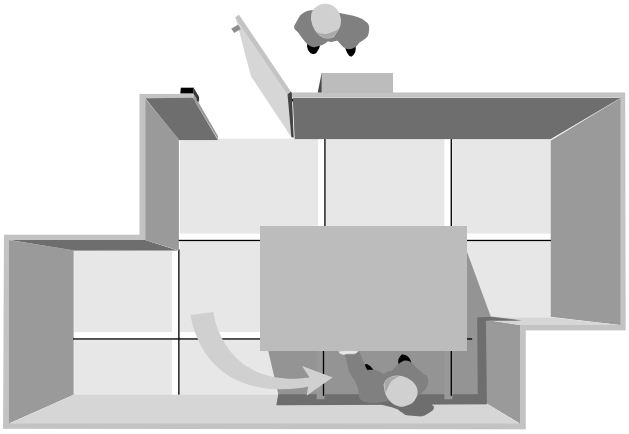


Figure 47 : Le tapis de sécurité détecte l'opérateur derrière l'équipement

Bourrelets sensibles à la pression

Ces dispositifs sont des bordures flexibles pouvant être montées sur le bord d'une pièce mobile, comme le plateau d'une machine ou une porte électrique, qui présente un risque d'écrasement ou de cisaillement, comme illustré à la figure 48.

Si la pièce mobile touche l'opérateur (ou vice versa), le bourrelet flexible s'enfonce et envoie une commande d'arrêt à la source d'alimentation du danger. Les bourrelets sensibles à la pression peuvent également être utilisés pour protéger les machines lorsqu'il y a un risque d'enchevêtrement de l'opérateur. Si un opérateur se trouve coincé par une machine, le contact avec le bourrelet sensible coupe l'alimentation de la machine.

Plusieurs technologies sont utilisées pour créer des bourrelets de sécurité. Une technologie souvent utilisée consiste à insérer ce qui est essentiellement un long interrupteur dans le bourrelet. Cette approche fournit des bourrelets droits et repose généralement sur la technique du raccordement à quatre fils.

Figure 48 : Bourrelet sur plateau de machine et porte électrique

Le Safedge Guardmaster d'Allen-Bradley utilise un caoutchouc conducteur, avec deux fils qui courent le long du bourrelet (figure 49). A l'extrémité du bourrelet, une résistance de terminaison est utilisée pour terminer le circuit. L'enfoncement du caoutchouc réduit la résistance du circuit.

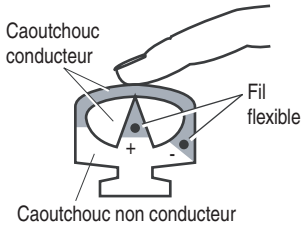


Figure 49 : Bourrelet de sécurité avec caoutchouc conducteur

Etant donné qu'un changement de résistance doit être détecté, le relais de surveillance doit être conçu pour détecter cet changement. Un exemple de câblage de cette conception à deux fils avec résistance de terminaison est illustrée à la figure 50. Un avantage de la technologie à caoutchouc conducteur est qu'elle fournit des coins actifs.

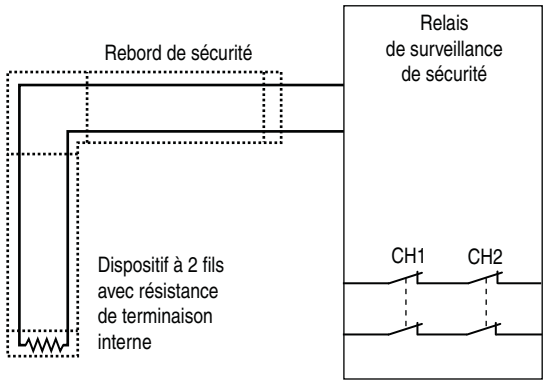


Figure 50 : Circuit du bourrelet de sécurité avec caoutchouc conducteur

Les barrières immatérielles, les scrutateurs, les tapis et les bourrelets sensibles sont classés comme "dispositifs de déclenchement". Ils ne limitent pas l'accès mais le "détectent". Ils reposent entièrement sur leur capacité de détection et de commutation pour fournir une sécurité. En général, ils sont adaptés uniquement pour les machines dont le temps d'arrêt après la coupure de l'alimentation est relativement court. Etant donné qu'un opérateur peut pénétrer directement dans la zone dangereuse, il est évident qu'il faut que le temps d'arrêt du mouvement soit inférieur au temps nécessaire à l'opérateur pour atteindre le danger après avoir déclencher le dispositif.

Interrupteurs de sécurité

Lorsque l'accès à la machine est peu fréquent, des protections amovibles sont préférées. La protection est interconnectée avec l'alimentation de la source du danger d'une façon qui permet de s'assurer que lorsque la grille de protection n'est pas fermée l'alimentation de la source de ce danger est coupée. Cette approche implique l'utilisation d'un interrupteur de sécurité installé sur la grille de protection. La commande de l'alimentation de la source du danger est acheminées à travers la section de commutation du dispositif. L'alimentation est généralement électrique, mais peut également être pneumatique ou hydraulique. Lorsqu'un mouvement de la grille de protection (ouverture) est détecté, l'interrupteur de sécurité envoie une commande pour isoler l'alimentation de la source du danger, directement ou via un contacteur d'alimentation (ou une vanne).

Certains interrupteurs de sécurité incorporent également un dispositif de verrouillage qui bloque la grille de protection en position fermée et qui ne la libère pas tant que la machine n'est pas en condition de sécurité. Pour la majorité des applications, la combinaison d'une protection mobile et d'un interrupteur de sécurité avec ou sans verrouillage de la protection, est la solution la plus fiable et la plus économique.

Interrupteurs de sécurité à broche

Les interrupteurs à broche requièrent qu'un actionneur à broche soit inséré et retiré de l'interrupteur. Lorsque la broche est insérée, les contacts de sécurité internes se ferment et permettent à la machine de fonctionner. Lorsque la broche est retirée, les contacts de sécurité internes s'ouvrent et envoient une commande d'arrêt aux composants de sécurité du système de commande. Les interrupteurs à broche sont polyvalents puisqu'ils peuvent être utilisés sur des protections coulissantes, sur charnière ou amovibles, comme illustré sur la figure 51.

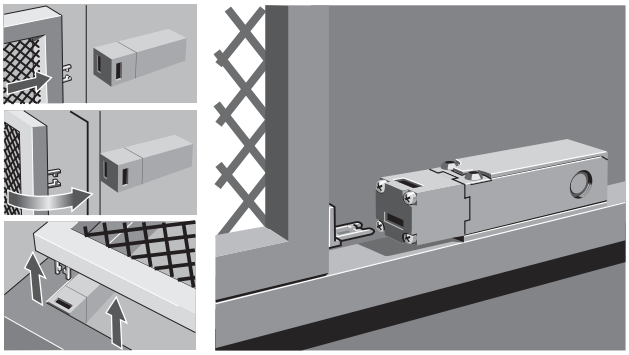


Figure 51 : Interrupteurs à broche sur protections coulissantes, sur charnière ou amovibles

Certaines des dernières normes de sécurité fonctionnelle mettent l'accent sur la nécessité d'intégrer une tolérance totale aux pannes dans les exigences des dispositifs utilisés pour les niveaux de risque élevés (p. ex. SIL 3 ou PLe). Cela parce que, en théorie, les interrupteurs à broche mécaniques ont des points uniques de défaillance (p. ex., l'actionneur à broche), même s'ils ont deux voies de commutation électrique. Ceci signifie que les interrupteurs sans contact peuvent être préférés dans ces conditions parce qu'ils n'ont généralement pas ces points de défaillance mécanique uniques.

Les interrupteurs à broche possèdent trois fonctions de base qui leur permet d'avoir une classification de sécurité : contournement, isolation galvanique et ouverture directe.

Contournement

La sécurité d'un interrupteur de verrouillage dépend de sa capacité à résister aux tentatives de "tricherie" ou de contournement du mécanisme. Un interrupteur de sécurité doit être conçu de façon à ne pas pouvoir être contourné par de simples outils faciles à se procurer (comme des tournevis, des pièces, du ruban ou des câbles).

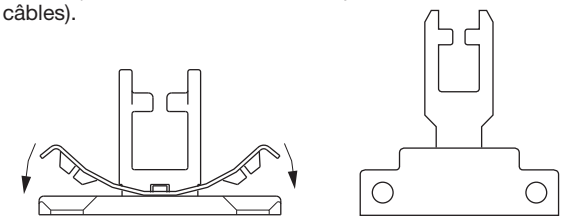


Figure 52 : Actionneurs à broche de formes spéciales pour empêcher le contournement

Pour cela, l'actionneur peut avoir une forme spéciale, comme illustré à la figure 52. Lorsqu'il est nécessaire d'effectuer la maintenance de la machine, il peut être nécessaire de contourner les interrupteurs. Dans ce cas, d'autres méthodes de protection doivent être fournies. L'accès aux actionneurs de rechange doit être supervisé par des procédures administratives. Certains actionneurs, comme celui de gauche sur la figure 52, possèdent un ressort pour les empêcher de pénétrer complètement et d'actionner l'interrupteur s'il n'est pas correctement fixé sur la protection.

Dans certaines situations, le personnel peut être tenté de contourner l'interrupteur d'une façon ou d'une autre. Les informations relatives à l'utilisation de la machine, recueillies lors de l'évaluation des risques, permettent de déterminer si cette éventualité est probable ou non. Plus il est probable que cela se produise, plus il doit être difficile de contourner l'interrupteur ou le système. Le niveau de risque estimé doit également être un facteur à ce stade. Il existe des interrupteurs avec des niveaux de sécurité divers, allant de la résistance au contournement impulsif, à l'impossibilité presque totale de contournement.

Il doit être noté à ce stade que si un niveau de sécurité élevé est requis, il est parfois plus pratique de l'obtenir par la façon dont le montage est réalisé.

Par exemple, si l'interrupteur est monté comme sur la figure 53 avec une glissière recouvrante, il n'est pas possible d'accéder à l'interrupteur lorsque la grille de protection est ouverte. La nature des mesures de prévention de la "tricherie" prises au moment de l'installation dépend du principe de fonctionnement de l'interrupteur.

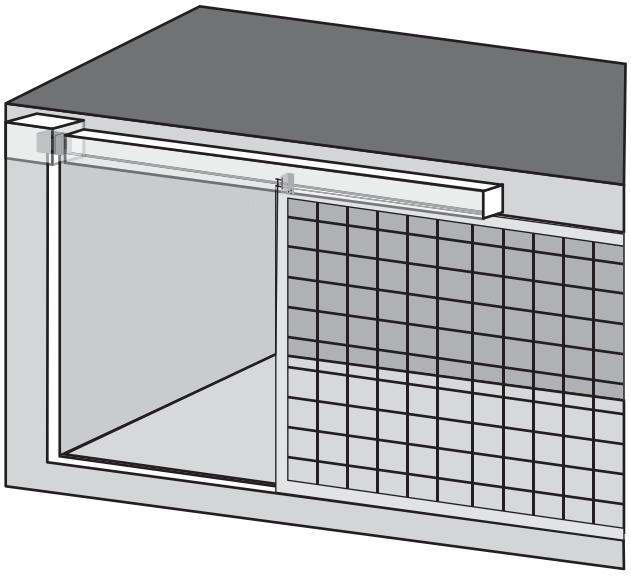


Figure 53 : Interrupteur et actionneur inaccessibles

Ouverture directe

La norme ISO 12100-2 explique que si un composant mécanique mobile déplace inévitablement un autre composant en même temps que lui, soit par contact direct, soit par des éléments rigides, ces composants sont dit être connectés en mode positif. La norme CEI 60947-5-1 utilise le terme Ouverture directe et le définit comme la séparation des contacts en tant que résultat direct d'un mouvement spécifique de l'actionneur par des membres non résilents (par exemple indépendant des ressorts). Cette norme fournit un ensemble de tests pouvant être utilisés pour vérifier l'action d'ouverture directe. Les produits qui sont conformes aux exigences de l'ouverture directe affichent sur leur boîtier le symbole indiqué à la figure 54.

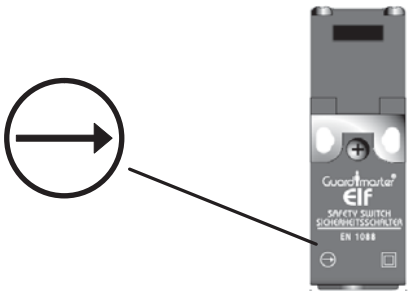


Figure 54 : Symbole de l'ouverture directe

La figure 55 montre un exemple de fonctionnement en mode positif permettant la déconnexion forcée des contacts. Les contacts sont considérés comme normalement fermés (N.F.) lorsque l'actionneur est inséré dans l'interrupteur (c.-à-d. protection fermée). Cela ferme un circuit électrique et permet au courant de circuler dans le circuit lorsque la machine est autorisée à fonctionner. L'approche à circuit fermé permet la détection de fil déconnecté, ce qui initie une fonction d'arrêt. Ces interrupteurs sont généralement conçus avec des contacts à double coupure. Lorsque la protection est ouverte, la broche est retirée de la tête de l'appareil et une came interne tourne. La came entraîne le piston qui force la lame à ouvrir les deux contacts, entraînant la rupture des contacts potentiellement soudés.

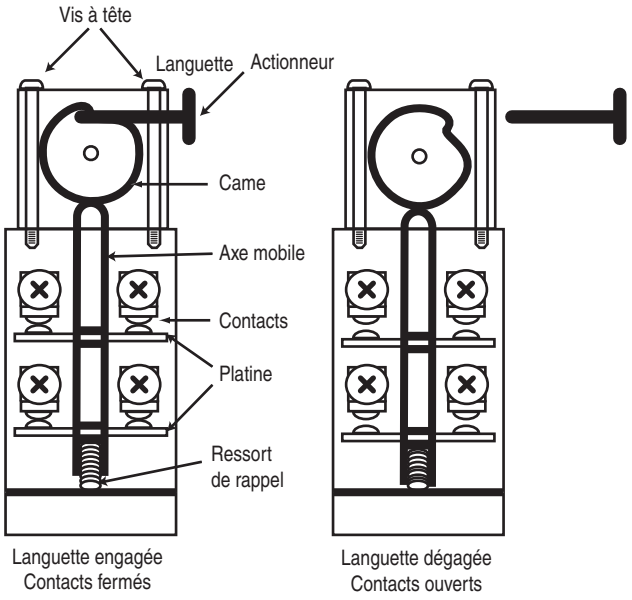


Figure 55 : Double coupure avec ouverture directe

La plupart des interrupteurs à broche possèdent égalemneet des contacts normalement ouverts (N.O.). Ces contacts sont généralement fermés par la force du ressort de rappel. Si le ressort casse, les contacts ne fonctionnent pas avec un degré de fiabilité suffisant. Ils sont donc généralement utilisés pour signaler au système de commande de la machine que la protection est ouverte.

Les contacts à ressort de rappel normalement ouverts peuvent être utilisés comme voie secondaire dans un système de sécurité. Cette approche fournit une diversité au système de sécurité afin d'aider à empêcher les causes courantes de défaillance. Le relais de surveillance ou l'automate de sécurité doit être conçu de façon à prendre en charge cette diversité de contacts N.O. + N.F.

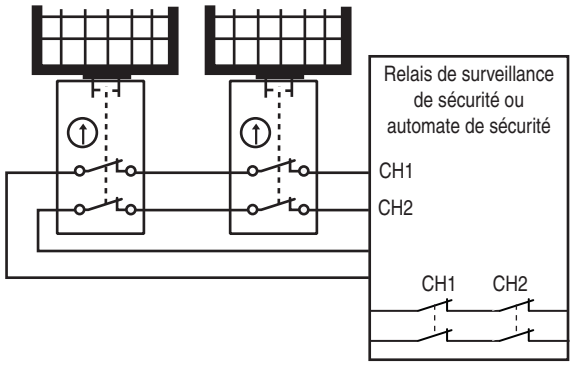


Figure 56 : Connexion en série de plusieurs interrutpeurs à 2 contacts N.F.

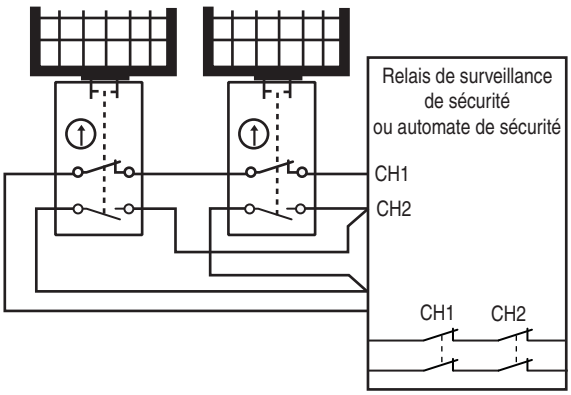


Figure 57 : Plusieurs interrupteurs avec contacts N.F. et N.O.

Un des avantages de l'utilisation de deux contacts normalement fermés avec les dispositifs de verrouillage est la réduction du câblage lorsque plusieurs barrières doivent être surveillées. La figure 56 montre comment plusieurs barrières peuvent être connectées en série. Cela peut être pratique pour un petit nombre de barrières, mais devient plus difficile à dépanner lorsque trop de barrières sont connectées en série.

Lorsque l'évaluation des risques préconise l'utilisation de différents contacts, les contacts N.F. sont connectés en série et les contacts N.O. sont connectés en parallèle. La figure 57 montre un schéma simplifié de cette approche dans lequel plusieurs dispositifs de verrouillage sont surveillés par un relais de surveillance. Les contacts N.O. sur le circuit de la voie 2 sont connectés en parallèle.

Duplication (également appelée Redondance)

Si des composants qui n'ont pas une sécurité intrinsèque sont utilisés dans la conception, et s'ils sont critiques pour la fonction de sécurité, un niveau de sécurité acceptable peut être obtenu en dupliquant ces composants ou systèmes. En cas de défaillance d'un composant, l'autres peut toujours exécuter la fonction. Il est généralement nécessaire de fournir une surveillance afin de détecter la première défaillance afin que, par exemple, un système à deux voies ne soit pas dégradé à une seule voie sans que personne n'en soit conscient. Il faut également faire attention à la question des défaillances dues à des causes courantes.

Une protection doit être fournie contre les pannes, qui entraînent la défaillance de tous les composants dupliqués (ou voies) en même temps. Les mesures adaptées peuvent consister à utiliser des technologies différentes pour chaque voie ou assurer un mode de défaillance orienté.

Isolation galvanique

La figure 58 montre des blocs de contacts avec deux jeux de contacts. Une barrière d'isolation galvanique est requise s'il existe une possibilité que les contacts se touchent en cas de contact soudé ou d'adhérence.

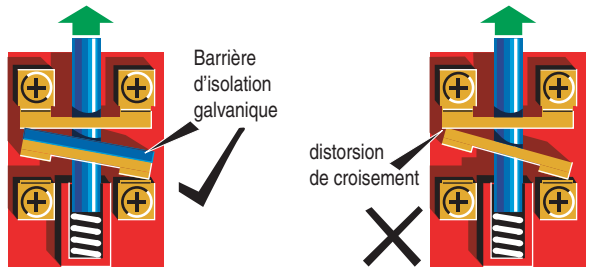


Figure 58 : Isolation galvanique des contacts

Arrêts mécaniques

Les interrupteurs de sécurité ne sont pas prévus pour résister à l'arrêt d'une barrière. Le concepteur de la machine doit prévoir un arrêt adapté tout en permettant une course suffisante pour que l'actionneur pénètre complètement dans l'interrupteur (figure 59).

Mesures de protection et équipement complémentaire

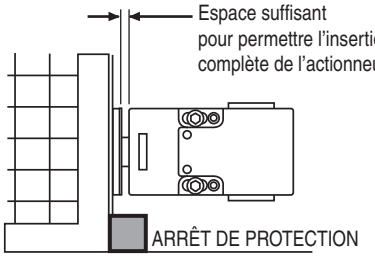


Figure 59 : Arrêts mécaniques

La broche montée sur de dispositif de protection doit rester raisonnablement bien alignée avec le trou d'entrée sur le corps de l'interrupteur. Avec le temps, les charnières peuvent s'user et les protections peuvent se plier ou se vriller. Cela a un effet négatif sur l'alignement de l'actionneur avec la tête. Le concepteur de la machine devrait envisager des interfaces avec un corps en métal et des actionneurs souples, comme sur la figure 60.

Figure 60 : Interface métallique avec actionneur souple

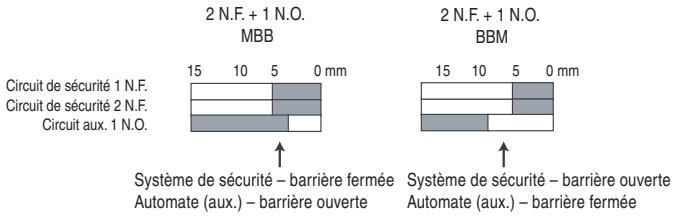


Figure 61 : Contacts MBB et BBM – Messages contradictoires

En raison de l'usure, des dégâts ou d'autres modifications du disposition de protection dans le temps, une pression peut s'exercer sur la barrière, forçant une légère ouverture. Si la barrière bouge jusqu'au point où la commutation se produit, le système de sécurité et le système de commande machine reçoivent des messages contradictoires, comme illustré à la figure 61.

Pour corriger cela, il faut verrouiller la barrière en position fermée ou utiliser des contacts à action brusque. Le choix de l'interrupteur à broche adapté implique la prise en compte de nombreux critères : corps en plastique ou en métal, nombre de contacts, fonctionnement des contacts, taille de la barrière de protection, alignement de la barrière, mouvement de la barrière, espace disponible et projections d'eau. Les interrupteurs à broche peuvent être difficiles à nettoyer correctement. C'est pourquoi les industries agroalimentaire et pharmaceutique préfèrent généralement des interrupteurs sans contact.

Dans certaines applications, le verrouillage de la barrière de protection en position fermée ou son ouverture retardée est nécessaire. Les dispositifs adaptés à ces impératifs sont appelés des gâches de sécurité à interverrouillage. Ils sont adaptés aux machines ayant des caractéristiques de décélération particulières, mais peuvent également fournir un niveau de protection supérieur pour la plupart des machines.

Pour la plupart des gâches de sécurité, l'action de déverrouillage est conditionnée par la réception d'un signal électrique, par exemple une tension électrique destinée à activer un électroaimant de déverrouillage. Ce principe de déclenchement conditionnel fait de la gâche de sécurité à électroaimant un dispositif très utile et polyvalent. Alors qu'avec la plupart des dispositifs la sécurité est obtenue par l'arrêt de la machine, les gâches de sécurité empêchent également l'accès à la machine et bloquent son redémarrage lorsque le verrouillage est désactivé. Ces dispositifs peuvent donc exécuter deux fonctions de sécurité distinctes mais connexes : prévention de l'accès et prévention du mouvemnet dangereux. Cela signifie que ces interrupteurs ont une importance fondamentale dans le domaine de la sécurité des machines. Le texte suivant décrit certaines des raisons typiques, liées aux applications, pour lesquelles les gâches de sécurité sont couramment utilisées :

Protection des machines et des personnes : Dans de nombreuses situations, les outils ou la pièce de travail peuvent subir des dégâts ou le processus peut subir une interruption importante si une machine est arrêtée soudainement au mauvais moment dans sa séquence de fonctionnement. Un exemple typique de cela est l'ouverture de la grille de protection interconnectée d'une machine-outil automatisée en milieu de cycle. Cette situation peut être éviter par l'utilisation d'une gâche de sécurité à électroaimant. S'il y a besoin d'accèder par la grille de protection, une demande de déverrouillage est envoyée à la commande machine qui attend un arrêt lors d'une séquence appropriée avant d'envoyer le signal de déverrouillage à la gâche de sécurité.

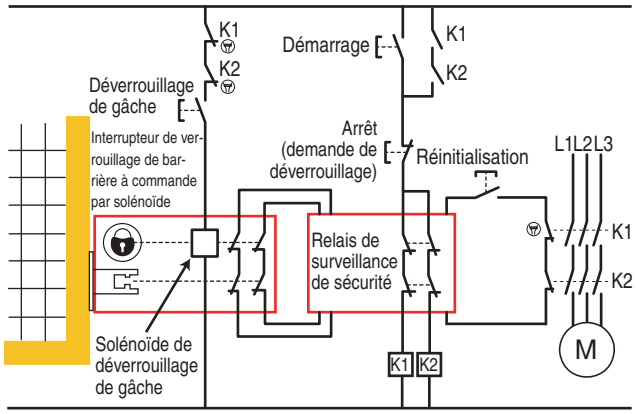


Figure 62 : Schéma simplifié d'une gâche de sécurité à électroaimant

La figure 62 montre un schéma très simplifié du principe. En pratique, les fonctions de démarrage, d'arrêt et de déverrouillage des interrupteurs illustrés sont généralement exécutées par des entrées et sorties de l'automate de la machine. L'automate accepte une entrée de requête de déverrouillage à n'importe quelle étape du cycle de la machine, mais n'active une commande de déverrouillage qu'à la fin du cycle. La commande de déverrouillage équivaut à appuyer sur les boutons-poussoirs d'arrêt et de déverrouillage.

Lorsque le verrou est déverrouillé est que la grille de protection est ouverte, les contacts de l'interrupteur s'ouvrent et provoquent l'isolement de l'alimentation de la source du danger.

Ce type d'approche peut être poussée plus loin par l'utilisation d'un interrutpeur à clé pour la requête de déverrouillage. De cette façon, il est possible de contrôler non seulement quand la protection peut être ouverte, mais également qui peut l'ouvrir.

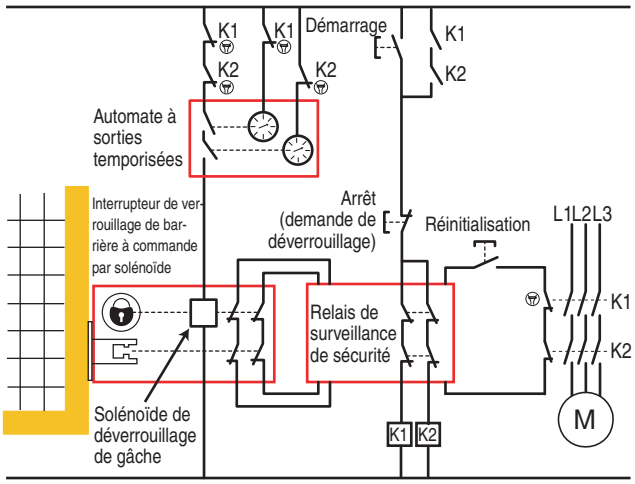


Figure 63 : Schéma de gâche de sécurité à électroaimant temporisée

Protection contre la décélération de la machine : Sur de nombreuses machines, la mise hors tension du moteur ou de l'actionneur n'entraîne pas forcément un arrêt fiable et immédiat du mouvement dangereux. Pour faire face à cette situation il est possible d'utiliser une gâche de sécurité à électroaimant dont le déverrouillage est conditionné par la mise en œuvre d'une forme de temporisation qui assure que tout mouvement dangereux est arrêté avant le déverrouillage.

Temporisation : La méthode la plus simple consiste à utiliser une fonction de temporisation configurée de façon à ce que l'interrupteur ne déverrouille pas la barrière de protection avant que le contacteur ne soit désactivé (OFF) et qu'un intervalle de temps prédéfini ne se soit écoulé. Ceci est illustré à la figure 63. La fonction de temporisation peut être fournit par un automate de sécurité ou par un contrôleur dédié. Il est important qu'il soit de sécurité parce qu'une défaillance qui provoque une temporisation plus courte que celle définie peut entraîner une exposition à des pièces mobiles dangereuses.

L'intervalle de temporisation doit être réglé au moins selon le temps d'arrêt de la machine le plus défavorable. Ce temps d'arrêt doit être prévisible, fiable et ne pas dépendre des méthodes de freinage qui peuvent se dégrader avec le temps.

Confirmation d'arrêt du mouvement : Il est également possible de conditionner le déverrouillage à une confirmation de l'arrêt du mouvemen. Les avantages de cette approche sont que même si la machine prend plus de temps que prévu pour s'arrêter, le verrou n'est jamais déverrouillé trop tôt. Cela est également plus efficace qu'une temporisation parce que le verrou est déverrouillé aussitôt que le mouvement est arrêté sans avoir à attendre le temps d'arrêt le plus défavorable. Une exemple de ceci est illustré à la figure 64.

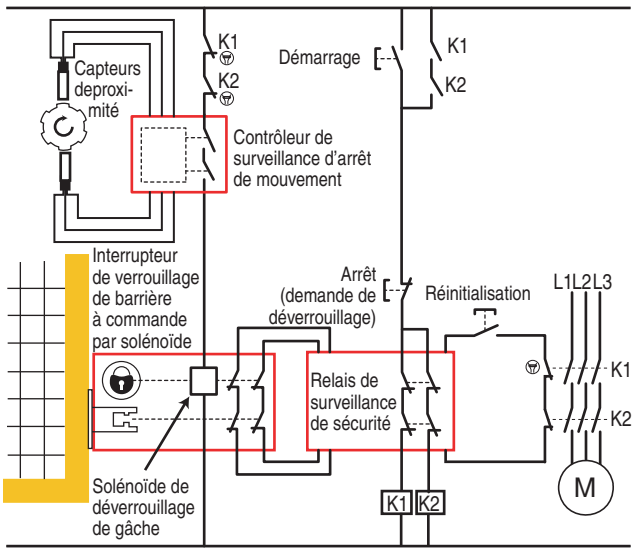


Figure 64 : Schéma simplifié d'une gâche de sécurité commandée par l'arrêt du mouvement

Cette fonction de surveillance de l'arrêt du mouvement doit être classée fonction de sécurité et s'obtient généralement par l'une des méthodes suivantes :

Détecteurs de proximité ou codeurs d'axes combinés avec un contrôleur dédié ou un automate de sécurité.

Détection de la force contre-élecromotrice (FCEM) à l'aide d'un bloc logique de sécurité dédié.

Les prochaines versions des variateurs de vitesse et des systèmes de commande d'axe fourniront également cette fonction classée en fonction de sécurité.

Sécurité à petite vitesse : Pour certains types de machines, il peut être nécessaire d'avoir accès à des pièces en mouvement pour effectuer certaines tâches, comme la maintenance, le réglage, l'alimentation ou l'armorçage. Ce type d'activité n'est envisagé que si une sécurité adéquate peut être apportée par d'autres mesures. Généralement, ces autres mesures se présentent sous la forme d'au moins l'une des solutions suivantes :

a) l'accès n'est autorisé qu'en présence d'une vitesse lente de sécurité ;

b) toute personne qui a accès aux pièces en mouvement doit avoir une commande personnelle locale permettant d'arrêter le mouvement ou d'empêcher son démarrage. La commande locale doit contourner tout autre signal de commande.

Ceci doit être considéré comme un minimum. Savoir si cela est acceptable ou non dépend de l'évaluation des risques et des normes et réglementations de sécurité pertinentes. Cependant, lorsqu'elle est acceptable, ce type de fonction de sécurité est souvent mis en œuvre par une gâche de sécurité à électroaimant combinée à une unité de surveillance de la vitesse lente et une poignée de sécurité à trois positions.

L'unité de surveillance de la vitesse lente de sécurité vérifie en permanence la vitesse des pièces en mouvement via ses détecteurs d'entrée et n'autorise l'envoi du signal de déverrouillage que lorsque la vitesse n'est pas supérieure à sa valeur de seuil définie. Après le déverrouillage, l'unité continue de surveiller la vitesse. Si son seuil prédéfini est dépassé lorsque l'accès est autorisé, l'alimentation du moteur est coupée immédiatement. De plus, la vitesse lente de sécurité ne peut être conservée que lorsque la poignée de sécurité est maintenue dans la position médiane (voir la figure 70). Il est évident que la gâche de sécurité, l'unité de surveillance de la vitesse lente de sécurité et la poignée de sécurité doivent être connectées à un forme de contrôleur logique de sécurité pour mettre en œuvre la fonction requise pour la sécurité et la production. Dans sa forme la plus simple, cela peut être la façon dont les unités sont câblées entre elles, généralement commutable via un sélecteur de mode manuel. Ce sélecteur est souvent à clé pour limiter le mode d'accès avec vitesse lente au personnel autorisé. Une meilleure efficacité et une plus grande souplesse de fonctionnement peuvent être obtenues en utilisant un dispositif configurable ou programmable pour la fonction de contrôleur logique. Cela peut être n'importe quoi, depuis un relais configurable modulaire jusqu'à un automate de sécurité.

Ce type de fonction de vitesse lente de sécurité est souvent requis sur les systèmes machines complexes intégrés où l'équipement est divisé en différentes zones, chacune avec un mode de fonctionnement différent et interdépendant. Dans ces types d'applications, un automate de sécurité ou un bloc logique de sécurité configurable dédié, comme le MSR57, constitue souvent une solution plus adaptée que des relais et des blocs logique de sécurité individuels.

La plupart des gâche de sécurité sont des adaptations d'interrupteurs à broche. Un électroaimant est ajouté à l'interrupteur. Cet électroaimant verrouille l'actionneur en place. Il existe deux types de verrouillage par électroaimant :

1. Déverrouillage par mise sous tension
2. Verrouillage par mise sous tension

Les dispositifs de déverrouillage par mise sous tension requièrent que l'électroaimant soit sous tension pour déverrouiller l'actionneur. Tant que l'électroaimant est sous tension, la barrière de protection peut être ouverte. Lorsque l'actionneur n'est plus alimenté, la barrière de protection se verrouille dès qu'elle est fermée.

En cas de perte d'alimentation, la barrière reste fermée et verrouillée. Si la gâche de sécurité est utilisée dans des applications avec accès du corps entier, une possibilité d'évacuation doit être fournie pour le cas où une personne se trouverait enfermée dans la zone du danger. Cela peut être rendu possible par l'utilisation d'un levier pivotant, d'un bouton-poussoir ou d'un moyen mécanique, comme sur la figure 65.

Figure 65 : moyens d'évacuation pour verrouillage par gâche de sécurité

Le verrouillage par mise sous tension requiert que l'électroaimant soit sous tension pour verrouiller la gâche. Une évaluation des risques doit évaluer les situations potentiellement dangereuses pouvant se produire en cas de perte d'alimentation et si la barrière de protection se trouve déverrouillée alors que la machine décélère.

Un critère important pour le choix de la gâche de sécurité est sa force de maintien. Quelle force est nécessaire pour maintenir la gâche fermée ? Lorsque la barrière est manipulée manuellement, la force de maintien peut-être minimale. Selon l'endroit où la gâche de sécurité est installée, le levier d'actionnement peut suggérer une force de maintien supérieure. Les portes électriques peuvent nécessiter une force de maintien supérieure.

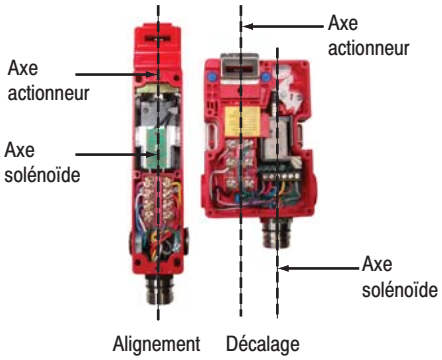


Figure 66 : électro-aimant en ligne et décalé

Un autre critère important pour le processus de sélection implique la relation entre électroaimant et actionneur. Deux relations existent : en ligne ou décalé, comme sur la figure 66. L'électroaimant est sur le même axe que les contacts de l'actionneur ou il est décalé par rapport à ces contacts. La disposition décalée fournit des contacts distincts qui indiquent l'état de l'électroaimant.

La disposition en ligne ne fournit pas de contacts distincts pour l'électroaimant. Cette disposition est un peu plus facile à mettre en œuvre. La disposition décalée fournit plus d'informations sur le fonctionnement de la gâche. Avec la disposition décalée, le concepteur de la machine doit s'assurer que l'état de l'électroaimant est surveillé par le système de sécurité. Le choix d'une disposition ou de l'autre est une question de préférence de l'utilisateur.

Une deuxième type de dispositif de sécurité est actionné manuellement et la barrière de protection peut être ouverte à tout moment. Une poignée ou un bouton qui déverrouille le dispositif de verrouillage ouvre également les contacts du circuit de commande.

Sur un dispositif comme l'interrupteur à pêne, une temporisation est imposée. Le pêne qui verrouille la barrière de protection actionne les contacts et pour le rétracter il faut tourner le bouton. Les premiers tours ouvrent les contacts, mais le pêne de verrouillage n'est pas totalement rétracté tant que le bouton n'a pas été tourné de nombreuses fois supplémentaires (cela prend jusqu'à 20 secondes). Ces dispositifs sont simples à mettre en œuvre et ils sont extrêmement robustes et fiables. L'interrupteur à pêne temporisé ne convient principalement qu'aux protections coulissantes.

Le temps d'arrêt de la source du danger doit être prévisible et le pêne ne doit pas pouvoir être rétracté avant que le danger ait été éliminé. Le pêne doit pouvoir être sorti en position fermée uniquement lorsque la grille de protection est totalement fermée. Cela signifie qu'il est nécessaire d'ajouter des butées pour limiter la course de la grille de protection, comme illustré à la figure 67.

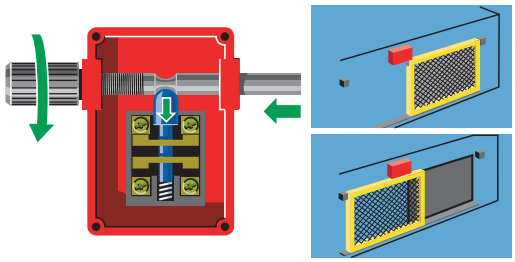


Figure 67 : interrupteur à pêne coulissant

Interrupteurs de sécurité sans contact

Certaines des dernières normes de sécurité fonctionnelle mettent l'accent sur la nécessité d'intégrer une tolérance totale aux pannes dans les exigences des dispositifs utilisés pour les niveaux de risque élevés (p. ex. SIL 3 ou PLe). Cela parce que, en théorie, les interrupteurs mécaniques ont des points uniques de défaillance (p. ex., l'actionneur à broche), même s'ils ont deux voies de commutation électrique. Cela signifie que les interrupteurs sans contact à deux voies peuvent être préférables dans ces cas parce qu'ils ne présentent généralement par les points uniques de défaillance mécanique.

Pour les interrupteurs sans contact, aucun contact physique (en situtation normale) ne se produit entre l'interrupteur et l'actionneur. Par conséquent, le fonctionnement en mode positif ne peut pas être utilisé comme moyen d'assurer l'action de coupure et il faut utiliser d'autres méthodes pour obtenir un fonctionnement équivalent.

Redondance

Comme décrit dans la section sur les interrupteurs à broche, un niveau élevé de sécurité peut être fourni par des dispositifs sans contact conçus avec duplication de composants (ou redondance). En cas de défaillance d'un composant, un autre est prêt à exécuter la fonction de sécurité et également une fonction de surveillance pour détecter cette première défaillance. Dans certains cas, cela peut être un avantage de concevoir des dispositifs avec des composants qui ont la même fonction mais des mécanismes de défaillance différents. Cela s'appelle la redondance différenciée. Un exemple typique est l'utilisation d'un contact normalement ouvert et d'un contact normalement fermé.

Mode de défaillance orientée

Avec des dispositifs simples, il est possible d'utiliser des composants avec un mode de défaillance orienté, comme expliqué dans la norme ISO 12100-2. Cela signifie utiliser des composants dont le mode de défaillance prédominant est connu à l'avance et toujours le même. Le dispositif est conçu de façon à ce que tout ce qui peut provoquer une défaillance entraîne également l'arrêt du dispositif.

Un exemple de dispositif qui utilise cette technique est un interrupteur de sécurité sans contact magnétique. Les contacts sont connectés avec un dispositif de protection contre les surintensités non réinitialisable interne. Toute situation de surintensité dans le circuit commuté provoque un circuit ouvert au niveau du dispositif de protection qui est prévu pour fonctionner à une intensité bien inférieure à celle qui mettrait en danger les contacts de sécurité.

En raison de l'utilisation de composants spéciaux, le défaut de sécurité critique susceptible de se produire serait une soudure des contacts à lames souples due à une intensité excessive sur l'interrupteur, comme illustré à la figure 68. Cela est évité grâce au dispositif de protection contre les surintensités non réinitialisable. Il existe une grande marge de sécurité entre le classement de ce dispositif et les contacts à lames souples. Parce qu'il n'est pas réinitialisable, l'interrupteur doit être protégé par un fusible externe d'une puissance adaptée. Les dispositifs de verrouillage Ferrogard Guardmaster d'Allen-Bradley utilisent cette technique.

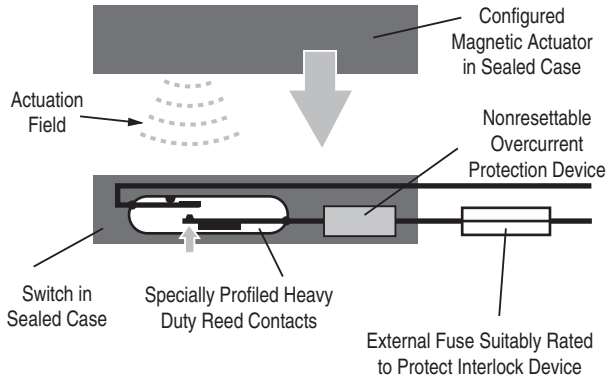


Figure 68 : interrupteur sans contact magnétique simple

Les dispositifs sans contact sont construits avec des boîtiers lisses et sont totalement étanches, ce qui en fait un choix idéal pour les applications agroalimentaires puisqu'ils n'ont pas de recoins où la saleté pourrait se loger et peuvent être lavés sous pression. Ils sont très faciles à mettre en œuvre et possèdent une tolérance de fonctionnement très élevée, il peuvent donc supporter une certaine usure ou distorsion du dispositif de protection et continuer à fonctionner correctement.

Un des points importants à prendre en considération pour l'utilisation des interrupteurs sans contact est leur plage de détection et leur tolérance au désalignement. Chaque gamme de produit a une courbe de fonctionnement qui indique la plage de détection et la tolérance au désalignement, comme illustré à la figure 69.

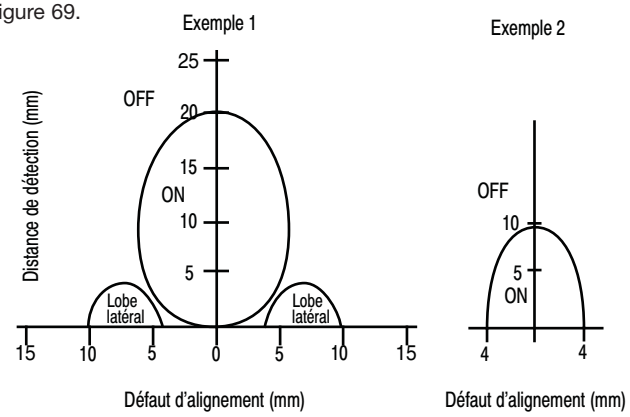


Figure 69 : courbe de fonctionnement sans contact

Un autre point important à prendre en considération pour l'utilisation des interrupteurs sans contact est la direction d'approche de l'actionneur, comme illustré à la figure 70. Les techniques de codage déterminent quelles approches sont acceptables.

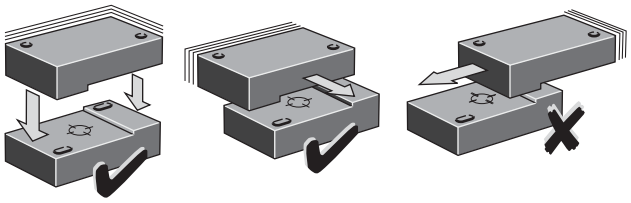
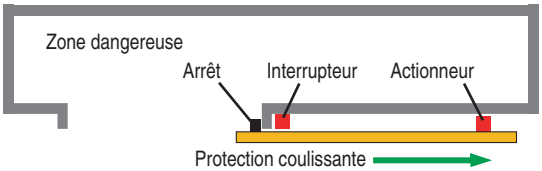


Figure 70 : l'approche de l'actionneur affecte le fonctionnement

Contournement – Interrupteurs sans contact

Il est important que l'interrupteur ne soit activé que par son actionneur. Cela signifie que les détecteurs de proximité ordinaires qui détectent les métaux ferreux ne conviennent pas. L'interrupteur doit fonctionner avec un actionneur "actif".

Lorsque la protection contre le contournement par un simple outil (un tournevis, des pinces, un câble, une pièce ou un aimant) est jugée nécessaire lors de l'évaluation des risques, les types d'actionnement sans codage doivent être installés de façon à empêcher l'accès lorsque la barrière est ouverte. Une exemple de ceci est illustré à la figure 71. Ils doivent également être installés là où ils ne sont pas soumis à des interférences parasites provoquées par des champs magnétiques/électriques.



Protection ouverte – machine arrêtée – protection recouvrant l'interrupteur

Figure 71 : la protection coulissante protège l'accès au détecteur

Mesures de protection et équipement complémentaire

Une sécurité élevée contre le contournement peut être obtenue en utilisant un actionneur et un détecteur codés. Pour les dispositifs à activation et codage magnétiques, l'actionneur intègre plusieurs aimants agencés pour créer plusieurs champs magnétiques spécifiques. Le détecteur possède plusieurs interrupteurs à lames souples spécialement agencés pour fonctionner uniquement avec les champs magnétiques spécifiques de l'actionneur. Il n'est généralement pas possible de réaliser un codage spécifique et unique avec les techniques de codage magnétique ; c'est à dire un codage où un actionneur est spécialement « apparié » à un détecteur particulier.

Les interrupteurs à lames souples utilisés avec les interrupteurs à codage magnétique sont souvent petits. Pour éviter le risque de contacts soudés, certains interrupteurs utilisent un contact normalement ouvert et un contact normalement fermé comme sorties. Ceci est basé sur le principe qu'il n'est pas possible de souder un contact ouvert. Le dispositif logique ou le bloc logique de sécurité doit être compatible avec le circuit N.F. + N.O. et doit également fournir une protection contre les surintensités. Les dispositifs de verrouillage Sipha Guardmaster d'Allen-Bradley utilisent cette technique du codage magnétique.

Interrupteurs de sécurité RFID sans contact

Les interrupteurs de sécurité sans contact avec technologie RFID (identification par radiofréquence) peuvent fournir un niveau de sécurité très élevé contre le contournement par de « simples » outils. Cette technologie peut également être utilisée pour fournir un codage unique aux dispositifs pour les applications dans lesquelles la sécurité est essentielle.

L'utilisation de la technologie RFID a de nombreux autres avantages. Elle convient à une utilisation avec les archtitectures de circuits à haute intégrité, comme la catégorie 4 ou SIL 3.

Elle peut être intégrée aux dispositifs ayant un boîtier étanche avec une protection IP69K en plastique ou en acier inoxydable.

Lorsque la technologie RFID est utilisée pour le codage, et la technologie inductive pour la détection, il est possible d'obtenir une portée de détection étendue et une tolérance importante au désalignement, généralement 15 à 25 mm. Cela signifie que ces dispositifs peuvent fournir des services stables et fiables, ainsi que des niveaux élevés d'intégrité et de sécurité pour une grande diversité d'applications industrielles.

Les dispositifs de verrouillage SensaGuard Guardmaster d'Allen-Bradley utilisent la technologie RFID.

Le dispositif est monté sur l'axe de charnière de la grille de protection, comme illustré sur la figure 72. L'ouverture de la grille de protection est transmise aux contacts du circuit de commande via un mécanisme à déclenchement positif.

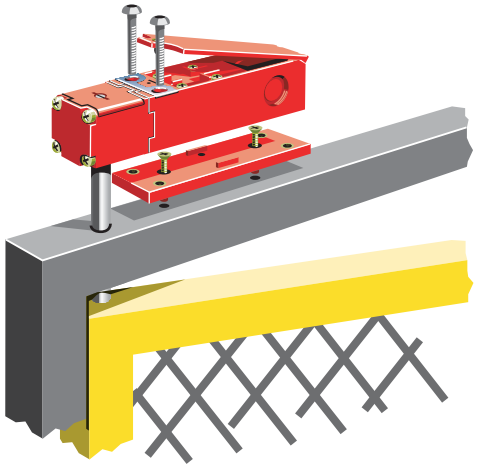


Figure 72 : installation de l'interrupteur à came

Lorsqu'ils sont correctement installés, ces interrupteurs sont parfaits pour la plupart des grilles de protection à charnière lorsqu'il est possible d'accéder à l'axe de la charnière. Ils peuvent isoler le circuit de commande dès qu'il y a un mouvement de 3° de la grille de protection et ils sont virtuellement impossibles à contourner sans démonter la grille.

Il faut tout de même prendre des précautions puisqu'une ouverture de 3° peut engendrer un espace singificatif sur une grille très large. Il faut également s'assurer qu'une grille de protection lourde ne crée pas de contraintes excessives sur l'axe de l'interrupteur.

Le déclenchement par came se présente généralement sous la forme d'une interrupteur de fin de course (de position) à déclenchement positif et d'une came linéaire ou rotative (comme illustré à la figure 73). Il est généralement utilisé sur les grilles de protection coulissantes. Lorsque la protection est ouverte, la came force le piston vers le bas pour ouvrir les contacts du circuit de commande. La simplicité du système permet à l'interrupteur d'être à la fois petit et fiable.

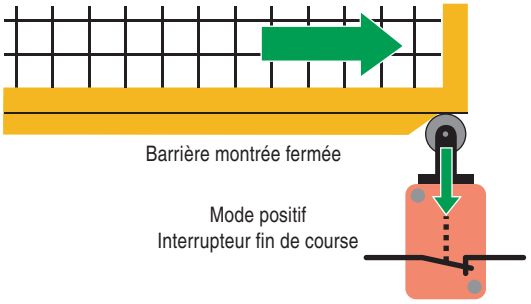


Figure 73 : interrupteur de fin de course à déclenchement positif

Les interrupteurs de fin de course (détecteurs de position) ne doivent pas être utilisés sur des grilles de protection basculantes ou sur charnière.

Il est extrêmement important que le piston de l'interrupteur ne puisse sortir que lorsque la grille de protection est complètement fermée. Cela signifie qu'il peut être nécessaire d'installer des butées supplémentaires pour limiter le mouvement de la grille dans les deux directions.

Il est nécessaire de fabriquer une came avec un profil adapté qui fonctionne selon des tolérances définies. La came montée sur la protection ne doit jamais se trouver séparée de l'interrupteur, autrement les contacts de l'interrupteur se ferment. Un tel système est sujet aux défaillances dues à l'usure, particulièrement avec des cames dont le profil n'est pas parfaitement adapté ou en présence de matériaux abrasifs.

Il est souvent recommandé d'utiliser deux interrupteurs, comme illustré à la figure 74. L'un fonctionne en mode positif (action directe pour ouvrir le contact) et l'autre fonctionne en mode négatif (rappel par ressort).

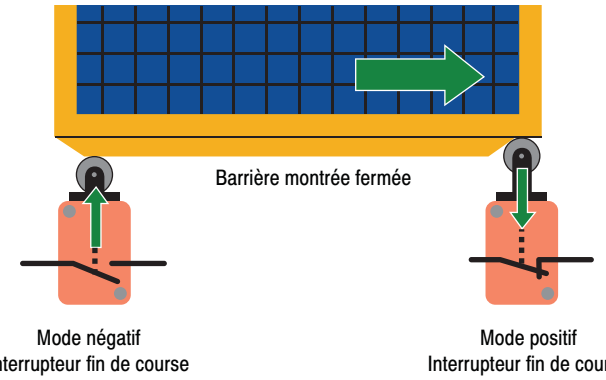


Figure 74 : interrupteurs de fin de course complémentaires redondants

Les dispositifs à clé captive peuvent être utilisés pour le verrouillage de la commande ou de l'alimentation. Avec le verrouillage de la commande, un interrupteur envoie une commande d'arrêt à un dispositif intermédiaire, qui arrête un autre dispositif afin de déconnecter l'énergie de l'actionneur. Avec le verrouillage de l'alimentation, la commande d'arrêt interrompt directement l'alimentation des actionneurs de la machine.

La méthode la plus pratique pour le verrouillage de l'alimentation est un système à clé captive (voir la figure 75). L'interupteur d'isolement de l'alimentation est actionné par une clé qui est maintenue captive en position lorsque l'interrupteur est en position activée (ON). Lorsque la clé est tournée, les contacts de l'interrupteur d'isolement sont verrouillés en position ouverte (isolant l'alimentation) et la clé peut être retirée.

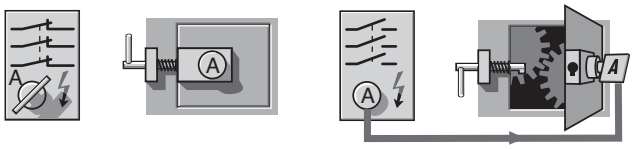


Figure 75 : verrouillage de l'alimentation avec système à clé captive

La grille de protection est verrouillée en position fermée et la seule façon de la déverrouiller et d'utiliser la clé de l'isolateur. Lorsqu'elle est tournée pour déverrouiller le dispositif de verrouillage de la grille, la clé est maintenue captive en position et ne peut pas être retirée tant que la grille n'est pas fermée et verrouillée de nouveau.

Il est donc impossible d'ouvrir la grille de protection sans d'abord isoler l'alimentation et il est églament impossible de mettre sous tension sans fermer et verrouiller la grille.

Ce type de système est très fiable et a l'avantage de ne par nécessiter de câblage électrique avec la grille de protection. L'inconvénient principal est que comme il nécessite de transférer la clé à chaque fois, il ne convient pas s'il faut accéder fréquemment à la grille de protection.

Lorsque l'accès de tout le corps est nécessaire, l'utilisation d'une clé personnelle est recommandée. Comme le montre la figure 76, la clé « B » est la clé personnelle. L'opérateur emmène la clé « B » avec lui dans la zone dangereuse. Les systèmes à clé captive sont disponibles avec deux, trois ou quatre clés pour les points d'accès multiples. L'utilisation d'une clé personnelle permet de s'assurer que l'opérateur ne peut pas être bloqué dans la zone protégée. La clé peut également être amenée dans la cellule et insérée dans un autre interrupteur pour activer des fonctions comme les modes d'apprentissage du robot et de marche par à-coup de la machine.

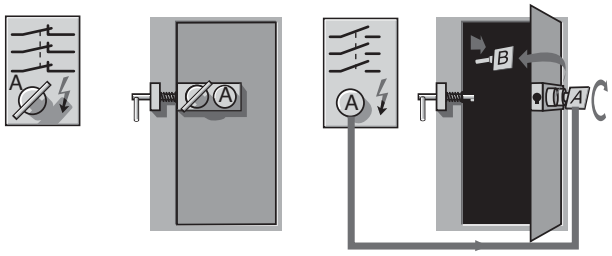


Figure 76 : accès du corps entier – L'opérateur prend la clé "B"

Dans un autre exemple illustré à la figure 77, la clé "A" est tournée et retirée de l'isolateur d'alimentation. L'alimentation est alors désactivée (OFF). Pour passer les grilles de protection, la clé "A" est insérée et tournée dans le dispositif d'échange de clé. Les deux clés "B" sont alors libérées et peuvent être utilisées sur les dispositifs de verrouillage. La clé "A" est maintenue captive, ce qui empêche d'activer l'alimentation. Deux clés "C" sont libérées des dispositifs de verrouillage de la grille de protection et pourront être utilisées dans l'étape suivante ou comme clés personnelles.

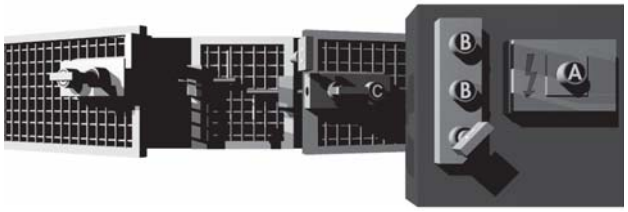


Figure 77 : plusieurs portes sont accessibles

La figures 78 présente un autre exemple de verrouillage à clé captive qui utilise des dispositifs de verrouillage à une ou deux clés captives et des clés avec différents codages, ainsi qu'un dispositif d'échange de clé. Des systèmes complexes peuvent être créés. En plus de s'assurer que l'alimentation est isolée avant de permettre l'accès, il est possible d'utiliser le système pour mettre en vigueur une séquence d'actions prédéfinie.

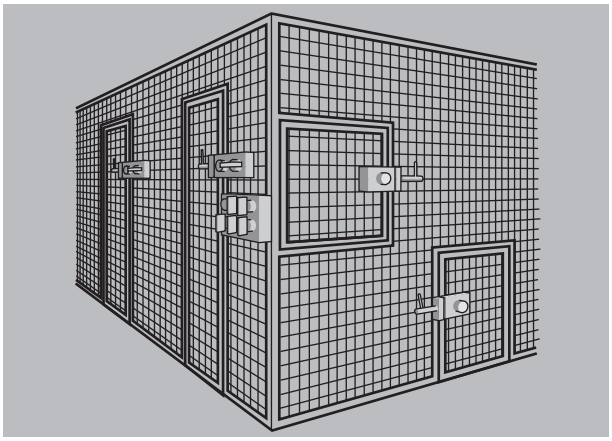


Figure 78 : séquence prédéfinie d'événements

Etant donné que la sécurité de ce type de système dépend de son bon fonctionnement mécanique, il est essentiel que les principes et les matériaux utilisés soient adaptées à leurs contraitntes d'utilisation.

Si un interrupteur d'isolement fait partie du système, il doit fonctionner en mode positif et il doit être conforme aux parties concernées de la norme CEI 60947.

L'intégrité et la sécurité du système reposent sur le fait que dans certaines conditions les clés sont captives, deux critères de base doivent donc être respectés :

1. LE DISPOSITIF DE VERROUILLAGE NE PEUT ÊTRE ACTIONNÉ QUE PAR LA CLÉ DÉDIÉE.

Cela signifie qu'il ne doit pas être possible de "tromper" le dispositif de verrouillage en utilisant des tournevis, etc., ou de neutraliser le mécanisme en le maltraitant d'une façon ou d'une autre. Lorsqu'il y a plusieurs dispositifs de verrouillage sur le même site, cela implique également que le codage des clés doit permettre d'empêcher toute activation non autorisée.

2. IL N'EST PAS POSSIBLE D'OBTENIR LA CLÉ D'UNE AUTRE FAÇON QUE CELLE PRÉVUE.

Cela signifie par exemple que lorsque la clé est captive, toute force exercée sur cette clé provoque sa rupture et non celle du dispositif de verrouillage.

Dispositifs d'interface opérateur

Fonction d'arrêt

Aux Etats-Unis, au Canada, en Europe et au niveau international, il existe une harmonisation des normes qui concerne les descriptions des catégories d'arrêt pour les machines ou les systèmes de fabrication.

REMARQUE : ces catégories sont différentes des catégories de la norme EN 954-1 (ISO 13849-1). Voir les normes NFPA79 et CEI/EN60204-1 pour plus d'informations. Les arrêts sont classés en trois catégories :

- Categorie 0 : arrêt par coupure immédiate de l'alimentation des actionneurs de la machine. Ceci est considéré comme un arrêt non contrôlé. Lorsque l'alimentation est coupée, le freinage qui a recours à une alimentation ne fonctionne pas. Les moteurs sont en roue libre et s'arrêtes progressivement sur un laps de temps étendu. Dans d'autres cas, des matériaux peuvent être lâchés par la machine, qui a besoin d'être alimentée pour tenir les matériaux. L'arrêt mécanique, qui n'a pas besoin d'alimentation, peut égalemnet être utilisé avec un arrêt de catégorie 0. L'arrêt de catégorie 0 est prioritaire sur les arrêts de catégories 1 ou 2.
- Catégorie 1 : arrêt contrôlé avec alimentation des actionneurs de la machine durant l'opération. L'alimentation des actionneurs est ensuite coupée une fois l'arrêt réalisé.Cette catégorie d'arrêt permet d'alimenter un système de freinage pour arrêter rapidement le mouvement dangereux, puis de couper l'alimentaton des actionneurs.
- Catégorie 2 : arrêt contrôlé de la machine avec alimentation des actionneurs restant active. Un arrêt normal en cours de production est considéré comme un arrêt de catégorie 2.

Ces catégories d'arrêt doivent être appliquées à chaque fonction d'arrêt, ceci lorsque la fonction d'arrêt est l'action exécutée par les composants de sécurité du système de commande en réponse à une entrée ; il faut utiliser la catégorie 0 ou 1. Les fonctions d'arrêt sont prioritaires sur les fonctions de démarrage correspondantes. Le choix d'une catégorie d'arrêt pour chaque fonction d'arrêt de sécurité doit être déterminé par une évaluation des risques.

Fonction d'arrêt d'urgence

La fonction d'arrêt d'urgence doit fonctionner en tant qu'arrêt de catégorie 0 ou 1, selon ce qui a été déterminé par l'évaluation des risques. Elle doit être initiée par une seule action humaine. Lorsqu'elle est exécutée, elle doit être prioritaire sur toutes les autres fonctions et les modes de fonctionnement de la machine. L'objectif est de couper l'alimentation aussi rapidement que possible sans créer de nouveaux dangers.

Jusqu'à récemment, il fallait utiliser des composants électro-mécaniques câblés pour les circuits d'arrêt d'urgence. Des modifications récentes des normes, comme les normes CEI 60204-1 et NFPA 79, permettent à des automates de sécurité et autres types de dispositifs électroniques conformes aux exigences des normes comme la norme CEI 61508 d'être utilisés dans le circuit d'arrêt d'urgence.

Dispositifs d'arrêt d'urgence

Lorsqu'une machine présente un risque pour l'opérateur, il doit être possible d'atteindre rapidement un dispositif d'arrêt d'urgence. Ce dispositif doit être opérationnel en permanence et facilement accessible. Les panneaux de commande doivent comporter au moins un dispositif d'arrêt d'urgence. Des dispositifs d'arrêt d'urgence supplémentaires peuvent être utilisés dans d'autres emplacements si nécessaire. Ces dispositifs existent sous différentes formes. Les interrupteurs à bouton-poussoir et les interrupteurs à câble font partie des dispositifs d'arrêt d'urgence les plus répandus. Lorsque le dispositif d'arrêt d'urgence est actionné, il doit rester enclenché et il ne doit pas être possible de générer la commande d'arrêt sans l'enclencher. Le réarmement du dispositif d'arrêt d'urgence ne doit pas créer de situation dangereuse. Une action distincte et délibérée doit être nécessaire pour redémarrer la machine.

Pour de plus amples informations sur les dispositifs d'arrêt d'urgence, consultez les normes ISO/EN13850, CEI 60947-5-5, NFPA79 et CEI 60204-1, 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 des dispositifs de protection principaux parce qu'ils n'empêchent pas d'accéder à la zone dangereuse et ne détectent pas l'accès à cette zone.

L'arrêt d'urgence est généralemnet fourni sous la forme d'un bouton-poussoir « coup de poing » rouge sur un fond jaune sur lequel l'opérateur appuie en cas d'urgence (voir la figure 79). Ils doivent être placés à des endroits stratégiques et en quantité suffisante autour de la machine afin de s'assurer qu'il y en a toujours un accessible aux endroits dangereux.

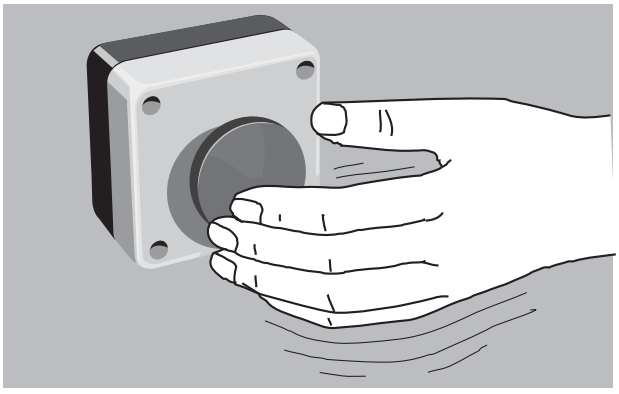


Figure 79 : bouton-poussoir d'arrêt d'urgence – Bouton « coup de poing » rouge sur fond jaune

Les boutons-poussoirs d'arrêt d'urgence doivent être facilement accessibles et utilisables dans tous les modes de fonctionnement de la machine. Lorsqu'un bouton-poussoir est utilisé comme dispositif d'arrêt d'urgence, il doit être bombé (coup de poing) et rouge avec fond jaune. Lorsque le bouton est enfoncé, les contacts doivent changer d'état et le bouton doit en même temps être verrouillé en position enfoncée.

Une des dernières technologies appliquée aux boutons-poussoirs est l'autocontrôle. Un contact supplémentaire est ajouté à l'arrière du bouton-poussoir pour surveiller si les composants à l'arrière du panneau sont toujours présents. Ceci s'appelle un élément de contact autocontrôlé. Il est constitué d'un contact à ressort qui se ferme lorsque l'élément de contact est enclenché sur le panneau. La figure 80 montre le contact autocontrôlé raccordé en série avec un des contacts de sécurité à ouverture directe.

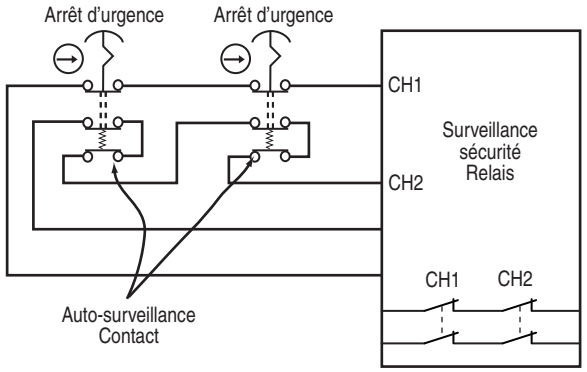


Figure 80 : contacts autocontrôlés sur arrêt d'urgence

Interrupteurs à câble

Pour des mécanismes comme les convoyeurs, il est souvent plus pratique et efficace d'utiliser un interrupteur à câble comme dispositif d'arrêt d'urgence le long de la zone dangereuse (comme illustré à la figure 81). Ces dispositifs utilisent un câble en acier raccordé à des interrupteurs à verrouillage par traction, de sorte que lorsque l'opérateur tire sur le câble dans une direction quelconque et en n'importe quel point du câble, cela déclenche l'interrupteur qui interrompt l'alimentation de la machine.

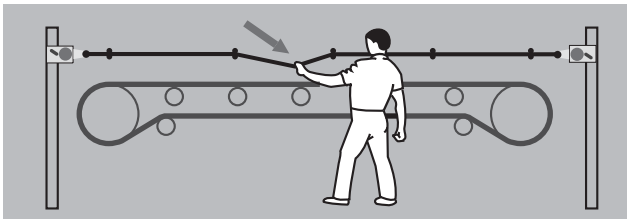


Figure 81 : interrupteurs à câble

Les interrupteurs à câble doivent détecter aussi bien la traction du câble que sa détente. La détection de câble détendu permet de s'assurer que le câble n'est pas coupé et qu'il est prêt à être utilisé.

La longueur du câble a un effet sur son efficacité. Pour les distances courtes, l'interrupteur de sécurité est monté à une extrémité et un ressort de traction est monté à l'autre extrémité. Pour les distances plus longues, des interrupteurs de sécurité doivent être montés aux deux extrémités du câble afin de s'assurer que lorsque l'opérateur tire une fois sur le câble, cela envoie une commande d'arrêt.

La force de traction devant être exercée ne doit pas dépasser 200 N (45 lb) ou une distance de 400 mm (15,75 in.) à une position centrale entre deux fixations du câble.

Commandes bimanuelles

La commande bimanuelle (nécessitant d'utiliser les deux mains) est un moyen courant pour empêcher l'accès lorsque la machine présente un danger. Deux commandes doivent être actionnées simultanément (dans un délai de 0,5 s entre l'activation de l'une et de l'autre) pour démarrer la machine. Cela permet de s'assurer que les deux mains de l'opérateur sont occupées dans une position sécurisée (c.-à-d. sur les commandes) et qu'elles ne peuvent donc pas se trouver dans la zone dangereuse. Les commandes doivent être actionnées en permanence lors du fonctionnement dangereux. Le fonctionnement de la machine doit s'arrêter si l'une des commandes est relâchée ; si l'une des commandes est relâchée, l'autre doit également être relâchée avant que la machine ne puisse redémarrer.

Un système de commande bimanuelle dépend fortement de l'intégrité de ses commandes et du système de surveillance pour la détection des défauts, il est donc important que cet aspect soit pris en compte dans la conception et présente les caractéristiques adéquates. Le fonctionnement du système bimanuel est organisé par Types dans la norme ISO 13851 (EN 574), comme illustré ; 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 4.1 montre la relation entre les types et les catégories de performance de la sécurité.

	Types				
			III		
Exigences	I	II	A	B	C
Actionnement 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

Tableau 3 : types et catégories de commande bimanuelle

L'écartement physique doit permettre d'éviter l'activation inappropriée (p. ex., par la main et le coude). Ceci peut être obtenu grâce à la distance ou des protections, comme illustré à la figure 82.

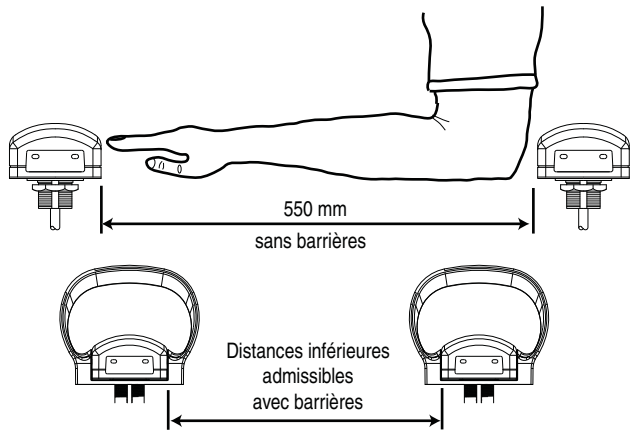


Figure 82 : séparation des commandes bimanuelles

La machine ne doit passer d'un cycle à un autre sans que les deux boutons aient été relâchés puis enfoncés. Ceci permet d'éliminer le risque que les deux boutons soient bloqués, ce qui laisserait la machine fonctionner en permanence. Le relâchement d'un des boutons doit entraîner l'arrêt de la machine.

L'utilisation d'une commande bimanuelle doit être étudiée avec attention parce qu'elle n'élimine généralement pas tous les risques. Cette commande ne protège que la personne qui l'utilise. Les autres personnes n'étant pas protégées, l'opérateur doit pouvoir surveiller tous les accès à la zone dangereuse.

La norme ISO 13851 (EN574) fournit des recommandations supplémentaires sur la commande bimanuelle.

Poignées de sécurité

Les poignées de sécurité sont des commandes qui permettent à un opérateur de pénétrer dans une zone dangereuse lorsque la source du danger fonctionne uniquement s'il tient en main la poignée en position enclenchée. Les poignées de sécurité utilisent des interrupteurs à deux ou trois positions. Les types à deux positions sont désactivés lorsque l'actionneur n'est pas manœuvré et sont activés lorsque l'actionneur est manœuvré. Les poignées à trois positions sont désactivées lorsque l'actionneur n'est pas actionné (position 1), activées lorsqu'il est tenu dans la position médiane (position 2) et désactivées lorsque l'actionneur est enfoncé au-delà de la position médiane (position 3). De plus, lorsque l'actionneur repasse de la position 3 à la position 1, le circuit de sortie ne doit pas se fermer lors du passage par la position 2. Ce concept est illustré à la figure 83.

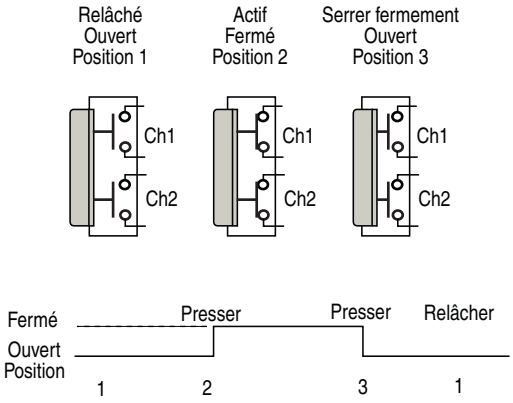


Figure 83 : fonctionnement de la poignée de sécurité à trois positions

Les poignées de sécurité doivent être utilisées conjointement avec d'autres fonctions de sécurité. Un exemple typique consiste à placer le mouvement dans un mode lent contrôlé. Une fois en mode lent, un opérateur peut entrer dans la zone dangereuse en tenant la poignée de sécurité.

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

Dispositifs logiques

Les dispositifs logiques jouent le rôle central dans la partie sécurité du système de commande. Les dispositifs logiques exécutent les fonctions de vérification et de surveillance du système de sécurité et autorisent la machine à démarrer ou lui envoient des commandes d'arrêt.

Il existe une gamme complète de dispositifs logiques qui sont utilisés pour créer une architecture de sécurité adaptée à la complexité et aux fonctions requises par la machine. Les petits relais de surveillance câblés sont les plus économiques pour les petites machines pour lesquelles un dispositif logique dédié est requis pour exécuter la fonction de sécurité. Des relais de surveillance modulaires et configurables sont préférés lorsqu'un grand nombre de dispositifs de protection différents et un contrôle de zone minimal sont requis. Dans le cas des machines complexes de taille moyenne à grande, des systèmes programmables avec E/S distribuées sont plus adaptés.

Relais de surveillance

Les relais de surveillance (Monitoring safety relay - MSR) jouent un rôle dlé dans de nombreux systèmes de sécurité. Ces modules sont généralement constitués de plusieurs relais à guidage réciproque avec des circuits supplémentaires pour assurer le bon fonctionnement de la fonction de sécurité.

Les relais à guidage réciproque sont des relais spécialisés « en cube ». Les relais à guidage réciproque doivent être conformes aux exigences de la norme EN50025. Leur objectif principal est d'empêcher les contacts normalement fermés et normalement ouverts d'être fermés en même temps. Les conceptions les plus récentes remplacent les sorties électromécaniques par des sorties à semi-conducteurs de sécurité.

Les relais de surveillance exécutent de nombreuses vérifications sur le système de sécurité. A la mise sous tension, ils effectuent des auto-vérifications de leurs composants internes. Lorsque les dispositifs d'entrée sont activés, le MSR compare les résultats des entrées redondantes. Si le résultat est acceptable, le MSR vérifie les actionneurs externes. Si le résultat est OK, le MSR attend un signal de réinitialisation pour activer les sorties.

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

Types d'entrées

Les dispositifs de protection ont différentes façon d'indiquer que quelque chose s'est produit :

- Verrouillages à contact et arrêts d'urgence
  Contacts mécaniques, à une voie avec un contact normalement fermé ou à double voie, avec les deux contacts normalement fermés. Le MSR doit être capable d'accepter une ou deux voies et de fournir une détection transversale des défauts pour la version à deux voies.
- Verrouillages sans contacts et arrêts d'urgence
  Contacts mécaniques, double voie, un contact normalement ouvert et un normalement fermé. Le MSR doit être capable de gérer différentes entrées.
- Dispositifs de commutation à sorties statiques
  Barrières immatérielles, scrutateurs laser, les sorties statiques sans contacts ont deux sorties PNP et exécutent leur propre détection de défaut transversal. Le MSR doit être capable d'ignorer la méthode de détection transversale des défauts des dispositifs.
- Tapis
  Les tapis crées un court-circuit entre deux voies. Le MSR doit être capable de résister aux courts-circuits répétés.
- Bourrelets
  Certains bourrelets sont conçus comme des tapis à 4 fils. Certains sont des dispositifs à 2 fils qui créent un changement de résistance. Le MSR doit être capable de détecter un court-circuit ou le changement de la résistance.
- Tension
  Mesure la force contre-électromotrice d'un moteur pendant la décélération. Le MSR doit être capable de tolérer des tensions élevées et de détecter des basses tensions lorsque le moteur décélère.
- Arrêt du mouvement
  Le MSR doit détecter les flux d'impulsions venant de divers détecteurs redondants.
- Commande bimanuelle
  Le MSR doit détecter différentes entrées normalement ouvertes et normalement fermées, il doit également fournir une temporisation de 0,5 s et une logique séquentielle.

Impédance d'entrée

L'impédance d'entrée des relais de surveillance détermine combien de dispositifs d'entrée peuvent être raccordés au relais et à quelle distance ils peuvent être montés. Par exemple, un relais de sécurité peut avoir une impédance d'entrée maximale autorisée de 500 ohms (W). Lorsque l'impédance d'entrée est supérieure à 500W, les sorties ne sont pas activées. L'utilisateur doit faire attention à ce que l'impédance d'entrée reste sous les valeurs maximales des spécifications. La longueur, la taille et le type des câbles a une influence sur l'impédance d'entrée. Le tableau 4 montre la résistance typique d'un fil de cuivre recuit à 25 °C.

Section ISO en mm^2	Calibre AWG	W pour 1000 m	W pour 1000 pieds
0,5	20	33,30	10,15
0,75	18	20,95	6,385
1,5	16	13,18	4,016
2,5	14	8,28	2,525
4	12	5,21	1,588

Tableau 4 : Valeurs de résistance du câble

Nombre de dispositifs d'entrée

Le processus d'évaluation des risques doit être utilisé pour déterminer combien de dispositifs d'entrée doivent être raccordés à un relais de surveillance et à quelle fréquence ces dispositifs doivent être vérifiés. Pour s'assurer que les dispositifs d'arrêt d'urgence et de verrouillage de barrière de protection sont opérationnels, leur fonctionnement doit être vérifié à intervalle régulier ; intervalle déterminé par l'évaluation des risques. Par exemple, un MSR à double voie d'entrée raccordé à une barrière de protection verrouillée devant être ouverte à chaque cycle de la machine (p. ex., plusieurs fois par jour) n'a pas besoin d'être vérifié. Ceci parce que lors de l'ouverture de la barrière, le MSR vérifie son propre fonctionnement, ses entrées et ses sorties (selon la configuration) pour détecter le moindre défaut. Plus la protection est ouverte souvent, plus l'intégrité du processus de vérification est élevée.

Un autre exemple pourrait être les arrêts d'urgence. Etant donné qu'ils sont généralement utilisés uniquement en cas d'urgence, ils est probable qu'ils soient rarement utilisés. Il faut donc établir un programme d'activation régulière de ces arrêts d'urgence pour vérifier leur efficacité. Cette activation régulière du système de sécurité est appelée Test de validité, et le laps de temps entre les tests de validité est appelé Intervalle entre tests de validité. Un troisième exemple peut être les portes d'accès pour le réglage de la machine, qui, comme les arrêts d'urgence, peuvent être rarement utilisées. Là encore, un programme doit être créé afin d'activer la fonction de vérification à intervalle régulier.

L'évaluation des risques permet de déterminer si les dispositifs doivent être vérifiés et à quelle fréquence. Plus le risque est élevé, plus l'intégrité du processus de vérification doit être élevée. Et moins la vérification "automatique" est fréquente, plus la vérification "manuelle" imposée doit être fréquente.

Détection de défaut transversal d'entrée

Dans les systèmes à double voie, les défauts de court-circuit entre les voies des dispositifs d'entrée, également appelés défauts transversaux, doivent être détectés par le système de sécurité. Cette opération est exécutée par le dispositif de détection ou le relais de surveillance.

Les relais de surveillance à microprocesseur, comme les barrières immatérielles, les scrutateurs laser et les détecteurs sans contact évolués, détectent ces courts-circuits de différentes manières. Une façon courante de détecter les défauts transversaux est l'utilisation de différents tests par impulsion, illustré à la figure 84. Les signaux de sortie sont envoyés par impulsions très rapides. 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, ce qui est détecté par le dispositif.

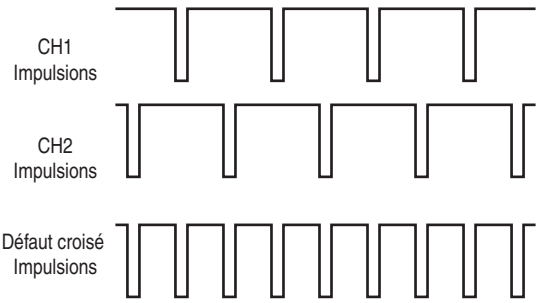


Figure 84 : test par impulsion pour détecter les défauts transversaux

Les relais de surveillance électro-mécaniques utilisent une technique de diversité différente : une entrée à enclenchement et une entrée à déclenchement. Ceci est illustré à la figure 85. 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.

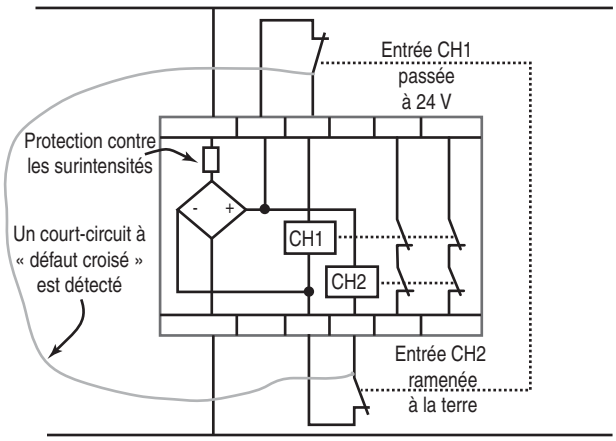


Figure 85 : les entrées complémentaires détectent les défauts transversaux

Sorties

Les MSR ont un nombre variable de sorties. Les types de sortie aide à déterminer quel MSR doit être utilisé selon l'application.

La plupart des MSR ont au moins 2 sorties de sécurité immédiatement opérationnelles. Les sorties de sécurité du MSR sont caractérisées comme normalement ouvertes. Elles sont classées comme sorties de sécurité en raison de la redondance et des vérifications internes.

Un deuxième type de sorties sont les sorties temporisées. Ces sorties temporisées sont généralemnet utilisées dans les arrêts de catégorie 1, où la machine requiert du temps pour exécuter la fonction d'arrêt avant d'autoriser l'accès à la zone dangereuse. La figure 86 montre les symboles utilisés pour les contacts immédiats et temporisés.

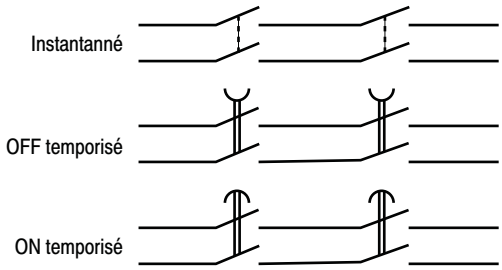


Figure 86 : symboles des types de contact

Les MSR ont également des sorties auxiliaires. Celles-ci sont généralement considérées comme normalement fermées. La figure 87 montre trois agencements de contacts normalement fermés. Le circuit de gauche permet d'utiliser les contacts normalement fermés uniquement comme circuits auxiliaires ; parce qu'un seul défaut sur CH1 ou CH2 ferme le circuit. L'agencement du milieu permet une utilisation comme circuit auxiliaire, tel qu'illustré, ou comme circuit de sécurité lorsque la connexion est en série. Le circuit de droite montre les contacts normalement fermés dans un agencement redondant, pour qu'ils puissent être utilisés dans les circuits de sécurité.

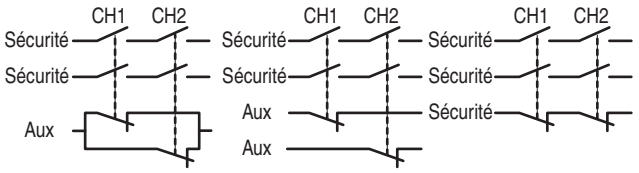


Figure 87 : utilisation des contacts N.F.

Caractéristiques de sortie

Les caractéristiques de sortie décrivent la capacité du dispositif de protection à commuter les charges. Généralement, les caractéristiques pour les dispositifs industriels sont décrits comme résistives ou électromagnétiques. Une charge résistive peut être par exemple un élément chauffant. Les charges électromagnétiques sont généralement des relais, des contacteurs ou des électro-aimants, sur lesquels la charge a une caractéristique inductive importante. L'annexe A de la norme CEI 60947-5-1, illustrée dans le tableau 5, décrit les caractéristiques des charges.

Lettre d'identification : l'identificant est une lettre suivie d'un nombre, par exemple A300.

La lettre fait référence au courant thermique interne conventionnel et au fait qu'il soit direct ou alternatif. Par exemple, A représente un courant alternatif de 10 ampères. Le nombre indique la tension d'isolement nominale. Par exemple, 300 représente 300 V.

Mesures de protection et équipement complémentaire

Identifiant	Utilisation	Courant thermique interne	Courant assigné nominal le à la tension assignée nominale Ue						VA	
			120 V	240 V	380 V	480 V	500 V	600 V	Fermeture	Ouverture
A150	AC-15	10	6	—	—	—	—	—	7200	720
A300	AC-15	10	6	3	—	—	—	—	7200	720
A600	AC-15	10	6	3	1,9	1,5	1,4	1,2	7200	720
B150	AC-15	5	3	—	—	—	—	—	3600	360
B300	AC-15	5	3	1,5	—	—	—	—	3600	360
B600	AC-15	5	3	1,5	0,95	0,92	0,75	0,6	3600	360
C150	AC-15	2,5	1,5	—	—	—	—	—	1800	180
C300	AC-15	2,5	1,5	0,75	—				1800	180
C600	AC-15	2,5	1,5	0,75	0,47	0,375	0,35	0,3	1800	180
D150	AC-14	1,0	0,6	—	—	—	—	—	432	72
D300	AC-14	1,0	0,6	0,3	—	—	—	—	432	72
E150	AC-14	0,5	0,3	—	—	—	—	—	216	36
Courant continu			125 V	250 V		400 V	500 V	600 V		
N150	DC-13	10	2,2	—		—	—	—	275	275
N300	DC-13	10	2,2	1,1		—	—	—	275	275
N600	DC-13	10	2,2	1,1		0,63	0,55	0,4	275	275
P150	DC-13	5	1,1	—		—	—	—	138	138
P300	DC-13	5	1,1	0,55		—	—	—	138	138
P600	DC-13	5	1,1	0,55		0,31	0,27	0,2	138	138
Q150	DC-13	2,5	0,55	—		—	—	—	69	69
Q300	DC-13	2,5	0,55	0,27		—	—	—	69	69
Q600	DC-13	2,5	0,55	0,27		0,15	0,13	0,1	69	69
R150	DC-13	1,0	0,22	—		—	—	—	28	28
R300	DC-13	1,0	0,22	0,1		—	—	—	28	28

Tableau 5 : Valeurs nominales des contacts pour la coupure de charge inductive

Utilisation : l'utilisation décrit les types de charges que le dispositif est prévu de commuter. Les utilisations relatives à la norme CEI 60947-5 sont indiquées dans le tableau 6.

Utilisation	Description de la charge
AC-12	Commande de charges résistives et de charges à semi-conducteurs avec isolation par opto-coupleurs
AC-13	Commande de charges à semi-conducteurs avec isolation par transformateur
AC-14	Commande de petites charges électromagnétiques (inférieures à 72 VA)
AC-15	Charges électromagnétiques supérieures à 72 VA
DC-12	Commande de charges résistives et de charges à semi-conducteurs avec isolation par opto-coupleurs
DC-13	Commande d'électro-aimants
DC-14	Commande de charges électromagnétiques avec résistances d'économie dans le circuit

Tableau 6 : Catégories d'utilisation

Courant thermique, Ith : Le courant thermique interne conventionnel est la valeur du courant utilisé pour les tests de montée en température de l'équipement lorsqu'il est installé dans un boîtier défini.

Tension Ue et courant Ie de fonctionnement nominaux : Le courant et la tension de fonctionnement nominaux définissent les capacités de fermeture et d'ouverture des éléments de coupure en conditions normales de fonctionnement. Les produits Guardmaster d'Allen-Bradley ont une tension de fonctionnement nominale de 125 V c.a., 250 V c.a. et 24 V c.c. Contactez l'usine pour des tensions d'utilisation autres que celles-ci.

VA : La valeur nominale VA (tension x ampère) indique la puissance nominale des éléments de coupure lors de la fermeture et de l'ouverture du circuit.

Exemple 1 : une puissance nominale A150, AC-15 indique que les contacts peuvent fermer un circuit de 7200 VA. Sous 120 V c.a., les contacts peuvent fermer un circuit avec un courant d'appel de 60 A. Etant donné que AC-15 est une charge électromagnétique, les 60 A ne sont que pour une courte durée ; le courant d'appel de la charge électromagnétique. L'ouverture du circuit n'est que de 720 VA parce que le courant en régime permanent de la charge électromagnétique est de 6 A, qui est le courant de fonctionnement nominal.

Exemple 2 : une puissance nominale N150, DC-13 indique que les contacts peuvent fermer un circuit de 275 VA. Sous 125 V c.a., les contacts peuvent fermer un circuit de 2,2 A. Les charges électromagnétiques c.c. n'ont pas de courant d'appel comme les charges électromagnétiques c.a. L'ouverture du circuit est également de 275 VA parce que le courant en régime permanent de la charge électromagnétique est de 2,2, qui est le courant de fonctionnement nominal.

Redémarrage machine

Si, par exemple, une grille interconnectée est ouverte lorsque la machine fonctionne, l'interrupteur de sécurité arrête cette machine. Dans la plupart des cas il est impératif que la machine ne redémarre pas immédiatement après la fermeture de la grille. Pour cela, il est courant d'utiliser un système de démarrage avec contacteur à verrouillage, comme illustrè à la figure 88. Une grille de protection interconnectée est utilisée comme exemple ici, mais les exigences concernent d'autres dispositifs de protection et d'arrêt d'urgence.

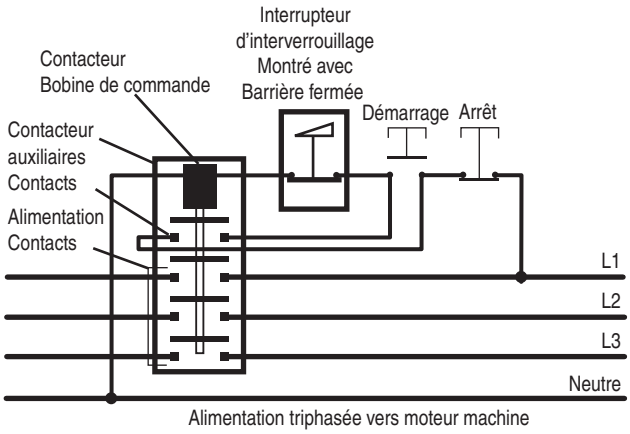


Figure 88 : circuit simple de verrouillage marche/arrêt d'une machine

Appuyer et relâcher le bouton de démarrage active la bobine de commande du contacteur qui ferme les contacts d'alimentation. Tant que l'alimentation circule dans les contacts d'alimentation, la bobine de commande reste activée (verrouillée électriquement) via les contacts auxiliaires du contacteur qui sont couplés mécaniquement aux contacts d'alimentation. Toute interruption de l'alimentation principale ou de l'alimentation de commande entraîne la désactivation de la bobine et l'ouverture des contacts d'alimentation principaux et auxiliaires. Le dispositif de verrouillage de la grille est câblé avec le circuit de commande du contacteur. Cela signifie que le redémarrage ne peut se faire que par la fermeture de la grille, puis activation ("ON") du bouton de démarrage normal qui réinitialise le contacteur et démarre la machine.

Les exigences pour une situation de verrouillage normale sont clarifiées dans la norme ISO 12100-1, paragraphe 3.22.4 (extrait).

Lorsque la grille de protection est fermée, les parties dangereuses de la machine protégées par la grille peuvent fonctionner, mais la fermeture de la grille ne suffit pas à limiter leur fonctionnement.

De nombreuses machines ont déjà des contacteurs simples ou doubles qui fonctionnent comme décrit ci-dessus (ou ont un système qui donne le même résultat). Lorsqu'un dispositif de verrouillage est installé sur une machine, il est nécessaire de déterminer si l'agencement de la commande d'alimentation est conforme aux exigences et de prendre des mesures supplémentaires si nécessaire.

Fonctions de réarmement

Les relais de surveillance Guardmaster d'Allen-Bradley possèdent un réarmement manuel surveillé ou un réarmement automatique/manuel.

Réarmement manuel surveillé

Un réarmement manuel surveillé requiert un changement d'état du circuit de réarmement après la fermeture de la grille de protection, ou la réinitialisation de l'arrêt d'urgence. La figure 89 montre une configuration typique d'un interrupteur de réarmement connecté au circuit de surveillance de sortie d'un relais de sécurité avec fonction de réarmement manuel surveillé. Les contacts auxiliaires normalement fermés à couplage mécanique des contacteurs de commutation de l'alimentation sont raccordés en série avec un bouton-poussoir à impulsion. Lorsque la grille a été ouverte, puis refermée, le relais de sécurité n'autorise pas le redémarrage de la machine tant qu'il n'y a pas de changement d'état sur le bouton de réarmement. Ceci est conforme aux objectifs mis en avant par les exigences relatives au réarmement manuel complémentaire décrites dans la norme EN ISO 13849-1. ; c.-à-d., la fonction de réarmement assure que les deux contacteurs sont désactivés (OFF) et que les deux circuits de verrouillage (et donc les grilles de protection) sont fermés et également (puisqu'un changement d'état est requis) que l'actionneur de réarmement n'a pas été contourné ou bloqué. Si ces vérifications réussissent, la machine peut être redémarrée à partir des commandes normales. La norme EN ISO 13849-1 cite le changement d'état comme le passage de l'état sous tension à l'état hors tension, mais le même principe de protection peut être obtenu par l'effet inverse.

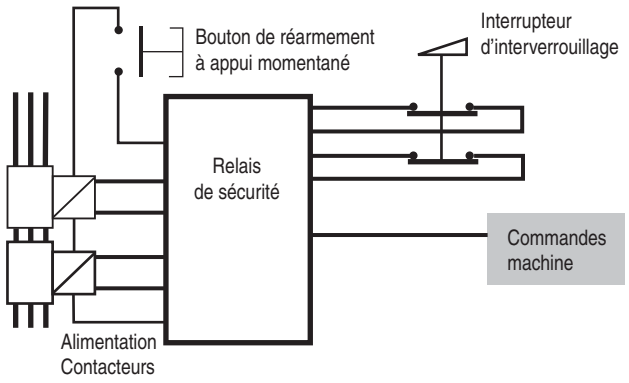


Figure 89 : réarmement manuel surveillé

L'interrupteur de réarmement doit être installé dans un endroit qui permet d'avoir une bonne visibilité du danger pour que l'opérateur puisse vérifier que la zone est dégagée avant le démarrage.

Réarmenent auto/manuel

Certains relais de sécurité ont un réarmement automatique/manuel. Le mode de réarmement manuel n'est pas surveillé et le réarmement se produit lorsque le bouton est enfoncé. Un réarmement en court-circuit ou bloqué en position enfoncée n'est pas détecté. Cette approche ne permet pas toujours d'atteindre le niveau d'exigence requis pour le réarmement manuel supplémentaire par la norme EN ISO 13849-1, sauf si des moyens complémentaires sont utilisés.

Une alternative consiste à contourner la ligne de réarmement, ce qui permet un réarmement automatique. L'utilisateur doit alors fournir un autre mécanisme pour empêcher le démarrage de la machine lorsque la grille est fermée.

L'interrupteur de réarmement doit être installé dans un endroit qui permet d'avoir une bonne visibilité du danger pour que l'opérateur puisse vérifier que la zone est dégagée avant le démarrage.

Réarmenent auto/manuel

Certains relais de sécurité ont un réarmement automatique/manuel. Le mode de réarmement manuel n'est pas surveillé et le réarmement se produit lorsque le bouton est enfoncé. Un réarmement en court-circuit ou bloqué en position enfioncée n'est pas détecté. Cette approche ne permet pas toujours d'atteindre le niveau d'exigence requis pour le réarmement manuel supplémentaire par la norme EN ISO 13849-1, sauf si des moyens complémentaires sont utilisés.

Une alternative consiste à contourner la ligne de réarmement, ce qui permet un réarmement automatique. L'utilisateur doit alors fournir un autre mécanisme pour empêcher le démarrage de la machine lorsque la grille est fermée.

Un dispositif d'auto-réarmement n'a pas besoin d'une commutation manuelle, mais après la désactivation, il effectue toujours une vérification de l'intégrité du système avant de réarmer le système. Un système à auto-réarmement ne doit pas être confondu avec un dispositif sans dispositif de réarmement. Dans ce dernier, le système de sécurité est activé immédiatement après la désactivation, mais il n'y a pas de vérification de l'intégrité du système.

Protection de contrôle

Une protection de contrôle arrête une machine lorsque la protection est ouverte et la redémarre directement lorsque la protection est fermée. L'utilisation de protections de contrôle n'est autorisé que sous certaines conditions très strictes parce que tout démarrage imprévu ou défaillance d'arrêt serait extrêmement dangereux. Le système de verrouillage doit présenter la fiabilité la plus élevée possible (il est souvent conseillé d'utiliser une gâche de sécurité). L'utilisation de protections de contrôle peut être utilisée UNIQUEMENT sur les machines où il n'est PAS POSSIBLE qu'un opérateur ou une partie seulement du corps de l'opérateur se trouve ou pénètre dans la zone dangereuse lorsque la barrière est fermée ;la protection de contrôle doit être le seul moyen d'accès à la zone dangereuse ;

Commande logique programmable de sécurité

Le besoin d'applications de sécurité flexibles et évolutives a conduit au développement d'automates/contrôleurs de sécurité. Les automates de sécurité programmables fournissent aux utilisateurs le même niveau de flexibilité de commande pour application de sécurité que celle à laquelle ils sont habitués avec les automates programmables standard. Cependant, il existe des différences importantes entre les automates standard et de sécurité. Les automates de sécurité, illustrès à la figure 90, existent sur différentes plates-formes pour s'adapter à l'évolutivité et aux impératifs fonctionnels et d'intégration des systèmes de sécurité complexes.

Figure 90 : plates-formes automate de sécurité

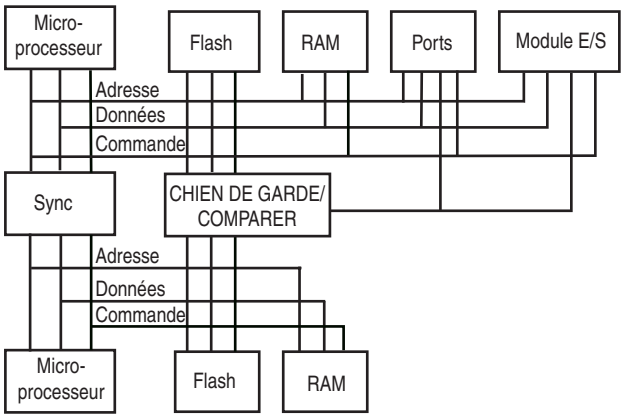


Figure 91 : architecture 1oo2D

Plusieurs microprocesseurs sont utilisés pour gérer les E/S, la mémoire et les communications sécurisées. Les circuits chien de garde effectuent une analyse de diagnostic. Ce type de construction est connu sous l'appellation 1oo2D, parce que n'importe lequel des deux microprocesseurs peut assurer la fonction de sécurité, et des diagnostics complets sont effectués afin de s'assurer que les deux microprocesseurs fonctionnent de façon synchrone.

Chaque circuit d'entrée est également testé en interne de nombreuses fois chaque seconde pour vérifier son bon fonctionnement. La figure 92 présente un schéma fonctionnel d'une entrée. Il se peut que vous n'activiez l'arrêt d'urgence qu'une fois par mois ; mais lorsque vous le faites, le circuit a été testé en permanence de sorte que l'arrêt d'urgence est détecté correctement dans l'automate de sécurité.

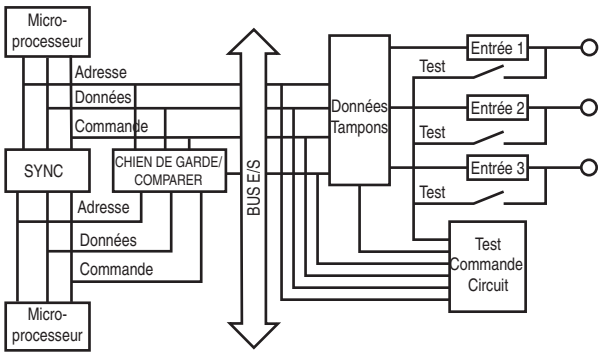


Figure 92 : schéma fonctionnel d'un module d'entrée de sécurité

Les sorties d'un automate de sécurité sont électromécaniques ou à semi-conducteurs classées de sécurité. La figure 93 montre plusieurs interrupteurs dans chaque circuit de sortie d'un automate de sécurité. Comme les circuits d'entrée, les circuits de sortie sont testés plusieurs fois par seconde pour vérifier qu'ils sont capables de désactiver la sortie. Si l'un des trois est défaillant, la sortie est désactivée par les deux autres et le défaut est signalé par le circuit de surveillance interne.

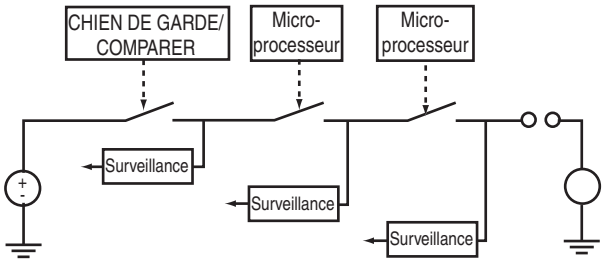


Figure 93 : schéma fonctionnel du module de sortie de sécurité

Lorsque des dispositifs de sécurité sont utilisés avec des contacts mécaniques (arrêts de sécurité, interrupteurs de barrière, etc), l'utilisateur peut utiliser des signaux de test par impulsion pour détecter les défauts transversaux. Pour ne pas user les sorties de sécurité coûteuses, de nombreux automates de sécurité fournissent des sorties à impulsion spécifiques pouvant être raccordées à des dispositifs à contact mécanique. Un exemple de câblage est illustré à la figure 94. Dans cet exemple, les sorties O1, O2, O3 et O4 ont des fréquences d'implusions différentes. L'automate de sécurité s'attend à voir ces différentes fréquences d'impulsions reflétées dans les entrées. Si des fréquences d'impulsions identiques sont détectées, un défaut transversal s'est produit et des mesures appropriées sont prises dans l'automate de sécurité.

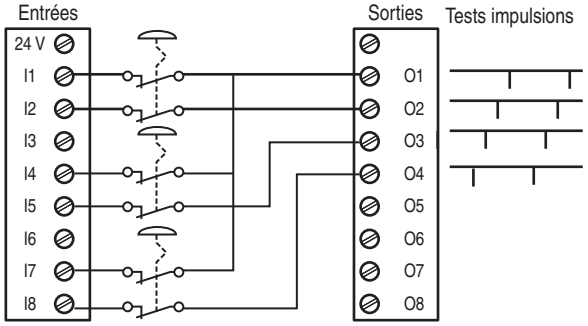


Figure 94 : test par impulsion des entrées mécaniques à 2 contacts N.F.

Logiciel

La programmation des automates de sécurité est très semblable à celle des automates standard. Tous les diagnostics supplémentaires et la vérification des erreurs mentionnées plus haut sont exécutés par le système d'exploitation, le programmeur ne s'en aperçoit même pas. La plupart des automates de sécurité ont des instructions spéciales utilisées pour écrire le programme du système de sécurité, et ces instructions ont tendance à imiter la fonction équivalente du relais de sécurité. Par exemple, l'instruction d'arrêt d'urgence de la figure 95 fonctionne de façon très semblable à un MSR127. Bien que la logique derrière chacune de ces instructions soit complexe, les programmes de sécurité semblent relativement simples parce que le programmeur se contente de relier ces blocs ensemble. Ces instructions, ainsi que d'autres instructions logiques, mathématiques, de manipulation de données, etc., sont certifiées par un tierce partie afin de s'assurer que leur fonctionnement est en adéquation avec les normes en vigueur.

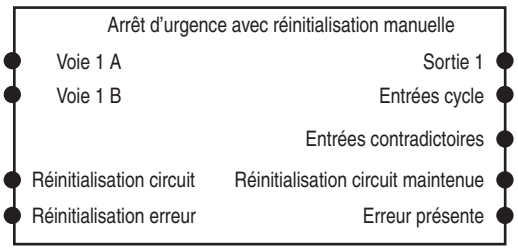


Figure 95 : bloc fonctionnel d'arrêt d'urgence

Les blocs fonctionnels constituent la méthode prédominante pour la programmation des fonctions de sécurité. En plus des blocs fonctionnels et de la logique à relais, les automates de sécurité fournissent également des instructions de sécurité certifiées. Les instructions de sécurité certifiées permettent un comportement adapté à l'application. Cet exemple montre une instruction d'arrêt d'urgence. Pour obtenir la même fonction en logique à relais demanderait environ 16 lignes. Puisque le comportement du programme est intégré à l'instruction d'arrêt d'urgence, le programme intégré n'a pas besoin d'être testé.

Des blocs fonctionnels certifiés sont disponibles pour dialoguer avec pratiquement tous les dispositifs de sécurité. Une exception à cette liste est le bourrelet de sécurité qui utilise la technologie résistive. Voici une liste d'instructions certifiées disponibles dans le GuardPLC.

1. Entrée complémentaire (1 N.O. + 1 N.F.) avec réarmement auto
2. Entrée complémentaire (1 N.O. + 1 N.F.) avec réarmement manuel
3. Arrêt d'urgence avec réarmement automatique
4. Arrêt d'urgence avec réarmement manuel
5. Entrée redondante (2 N.F.) avec réarmement automatique
6. Entrée redondante (2 N.F.) avec réarmement manuel
7. Sortie redondante avec retour positif
8. Sortie redondante avec retour négatif
9. Boîte pendante de validation avec réarmement automatique
10. Boîte pendante de validation avec réarmement manuel
11. Station bimanuelle avec broche active
12. Station bimanuelle sans broche active
13. Barrière immatérielle avec réarmement automatique
14. Barrière immatérielle avec réarmement manuel
15. Sélecteur de mode à cinq positions
16. Sortie unique de test par impulsion
17. Sortie de test par impulsion redondante

Les automates de sécurité génèrent une « signature » qui permet de suivre les changements apportés. Cette signature est généralement un combinaison du programme, de la configuration des entrées/sorties et un horodatage. Lorsque le programme est finalisé et validé, l'utilisateur doit enregistrer cette signature dans les résultats de la validation pour référence. Si le programme a besoin d'être modifié, une nouvelle validation est nécessaire et une nouvelle signature doit être enregistrée. Le programme peut également être verrouillé par un mot de passe afin d'empêcher les modifications non autorisées.

Le câblage des systèmes logiques programmables est plus simple que celui des relais de surveillance de sécurité. A l'inverse des relais de surveillance qui doivent être câblés sur des bornes spécifiques, les dispositifs d'entrée sont raccordés à n'importe quelle borne d'entrée et les dispositifs de sortie sont raccordés à n'importe quelle borne de sortie. Les bornes sont ensuite affectées par le logiciel.

Automates à sécurité intégrée

Les solutions de commande de sécurité fournissent désormais une intégration complète avec une architecture de commande unique là où les fonctions de commande de sécurité et standard résident et travaillent ensemble. La capacité d'intégrer la commande de mouvement, de variateur, de process, de traitement par lots, de séquentiel à haute vitesse et la sécurité SIL 3 dans un même automate présente des avantages significatifs. L'intégration des commandes de sécurité et standard permet d'utiliser des technologies et des outils communs, ce qui réduit les coûts de conception, d'installation, de mise en service et de maintenance. La capacité d'utiliser des équipements de commande communs, des E/S de sécurité distribuées ou des dispositifs de sécurité sur des réseaux de sécurité et des dispositifs IHM communs, permet de réduire les coûts d'acquisition et de maintenance, ainsi que le temps consacré au développement. Toutes ces caractéristiques améliorent la productivité, accélèrent le dépannage et réduisent les coûts de formation grâce à la standardisation.

La figure 96 montre un exemple de l'intégration de la commande et de la sécurité. Les fonctions de commande standard (pas de sécurité) résident dans la tâche principale. Les fonctions de sécurité résident dans la tâche de sécurité.

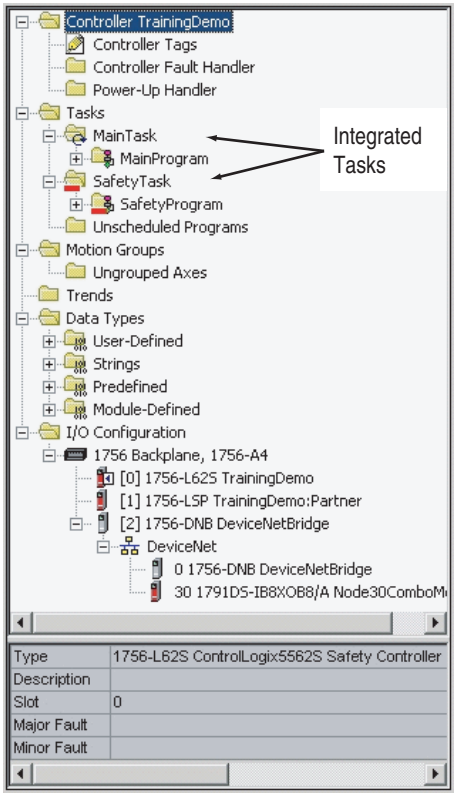


Figure 96 : tâches de sécurité et standard intégrées

Toutes les fonctions standard et de sécurité sont isolées les unes des autres. La figure 97 montre un schéma fonctionnel des interactions autorisées entre les parties standard et de sécurité de l'application. Par exemple, les points de sécurité peuvent être directement lus par le programme standard. Les points de sécurité peuvent être échangés entre les automates GuardLogix sur EtherNet, ControlNet ou DeviceNet. Les données de point de sécurité peuvent être directement lus par les dispositifs externes, les interfaces homme-machine (IHM), les ordinateurs personnels (PC) ou d'autres automates.

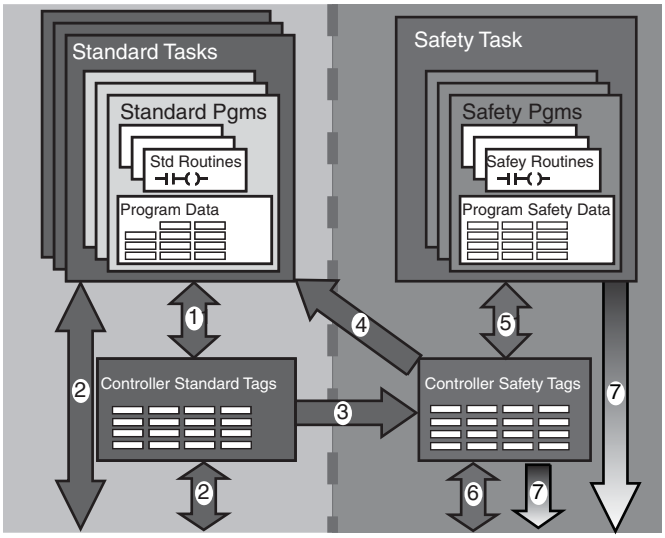


Figure 97 : interaction des tâches de sécurité et standard

1. Les points et le programme standard se comportent de la même façon que ControlLogix.
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) les données de point standard dans les points de sécurité pour les utiliser dans la tâche de sécurité. Cela permet aux utilisateurs de lire les informations d'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 directement lus par le programme standard.
5. Les points de sécurité peuvent être lus ou écrits par le programme de sécurité.
6. Les points de sécurité peuvent être échangés entre 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 : lorsque ces données sont 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 permis aux fabricants d'améliorer la flexibilité et les diagnostics, d'allonger les distances, de réduire les coûts d'installation et de câblage, de faciliter la maintenance et plus généralement d'améliorer la productivité de leurs activités de production. Les mêmes motivations conduisent à la mise en œuvre de réseaux de sécurité industriels. Ces réseaux de sécurité permettent aux fabricants de distribuer les E/S de sécurité et les dipositifs de sécurité autour de leurs machines à l'aide d'un seul câble réseau, ce qui réduit les coûts d'installation tout en améliorant les diagnostics et permet d'avoir des systèmes de sécurité de plus en plus complexes. Ils permettent également des communications sécurisées entre les automates/contrôleurs de sécurité ; les utilisateurs peuvent ainsi répartir leur commande de sécurité entre plusieurs systèmes intelligents.

Les réseaux de sécurité n'empêchent pas les erreurs de communication. Ils ont une plus grande capacité à détecter les erreurs de transmission et permettent aux dispositifs de sécurité de prendre les mesures appropriées. Les erreurs de communication détectées incluent : insertion de message, perte de message, corruption de message, délai de message, répétition de message et séquence de message incorrecte.

Pour la plupart des applications, lorsqu'une erreur est détectée le dispositif se met dans un état désactivé connu, 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 si besoin.

Les premiers réseaux de sécurité étaient liés à un support ou à un schéma d'accès particulier, les facricants devaient donc utiliser des câbles spécifiques, des cartes d'interface réseau, des routeurs, des passerelles, etc. qui sont également devenus des composants de la fonction de sécurité. Ces réseaux étaient limités parce qu'ils ne prenaient en charge que la communication entre les dispositifs de sécurité. Cela signifiait que les fabricants devaient utiliser plusieurs réseaux dans leur stratégie de commande de machine (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 détachées.

Les réseaux de sécurité modernes permettent à un seul câble réseau de communiquer avec les 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 les 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 les dispositifs standard peuvent tous résider sur le même réseau. Les utilisateurs peuvent également faire des passerelles entre des réseaux contenant des dispositifs de sécurité, ce qui permet de subdiviser les dispositifs de sécurité pour affiner les temps de réponse de la sécurité, ou pour simplement faciliter la répartition des dispositifs de sécurité. Etant donné que seuls les dispositifs finaux (automate/contrôleur de sécurité, module d'E/S de sécurité, composant de sécurité) ont la responsabilité du protocole de sécurité, des câbles, cartes d'interface réseau, passerelles et routeurs standard sont utilisés, ce qui évite d'avoir recours à des équipements réseau spéciaux et élimine ces dispositifs de la fonction de sécurité.

La figure 98 montre un exemple simplifié de système d'E/S distribuées. L'opérateur ouvre la barrière.L'interrupteur de sécurité, raccordé au bloc d'E/S de sécurité local, envoie ses données de sécurité vers l'automate de sécurité par le réseau DeviceNet. L'automate de sécurité renvoie un signal au bloc d'E/S de sécurité pour qu'il désactive l'équipement se trouvant à l'intérieur de la zone protégée par la barrière et envoie une sortie standard à une colonne lumineuse pour signaler l'ouverture de la porte. L'IHM et l'automate standard surveillent les données de sécurité à afficher et les mesures de contrôle supplémentaires, comme un arrêt du cycle de l'équipement adjacent.

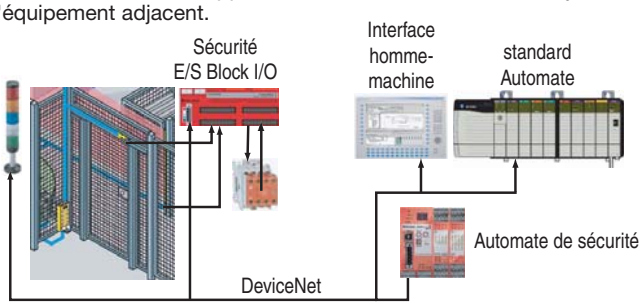


Figure 98 : exemple d'un réseau de sécurité réparti simple

Pour les systèmes de production de taille plus importante, où les informations de sécurité et la commande doivent être partagées, il est possible d'utiliser Ethernet/IP. La figure 99 (page suivante) donne un exemple de communication entre deux automates de sécurité avec DeviceNet utilisé pour la distribution locale des E/S dans un sous-système plus petit.

Dispositifs de sortie

Contacteurs auxiliaires de sécurité et contacteurs de sécurité

Les contacteurs auxiliaires et les contacteurs sont utilisés pour couper l'alimentation de l'actionneur. Des caractéristiques spéciales sont ajoutées aux contacteurs auxiliaires et aux contacteurs pour leur fournir la fonction de sécurité.

Les contacts à couplage mécanique normalement fermés sont utilisés pour renvoyer l'état des contacteurs auxiliaires et des contacteurs au dispositif logique. L'utilisation de contacts à couplage mécanique permet d'assurer la fonction de sécurité. Pour se conformer aux exigences des contacts à couplage mécanique, les contacts normalement fermés et normalement ouverts ne peuvent pas être fermés en même temps. La norme CEI 60947-5-1 définit les exigences pour les contacts à couplage mécanique. Si les contacts normalement ouverts deviennent soudés, les contacts normalement fermés restent ouverts d'au moins 0,5 mm. Réciproquement, si les contacts normalement fermés deviennent soudés, les contacts normalement ouverts restent ouverts. Si le produit est conforme aux exigences, le symbole indiqué à la figure 100 se trouve sur le produit.

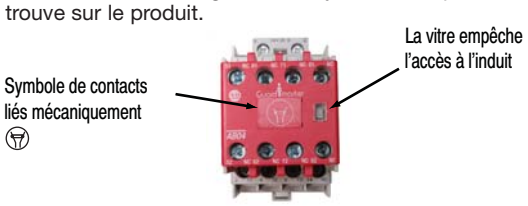


Figure 100 : symbole de contact à couplage mécanique

Les systèmes de sécurité ne doivent être démarrés qu'à certains endroits. Les contacteurs auxiliaires et les contacteurs standards permettent d'enfoncer l'armature 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 contacteurs auxiliaires de sécurité, le contact normalement fermé est géré par la lame principale. Les contacteurs de sécurité utilisent un bloc supplémentaire pour les contacts à couplage mécanique. Si le bloc de contacts devait tomber de la base, les contacts à couplage mécanique restent fermés. Les contacts à couplage mécanique sont fixés de façon permanente sur le contacteur auxiliaire de sécurité ou sur le contacteur de sécurité.

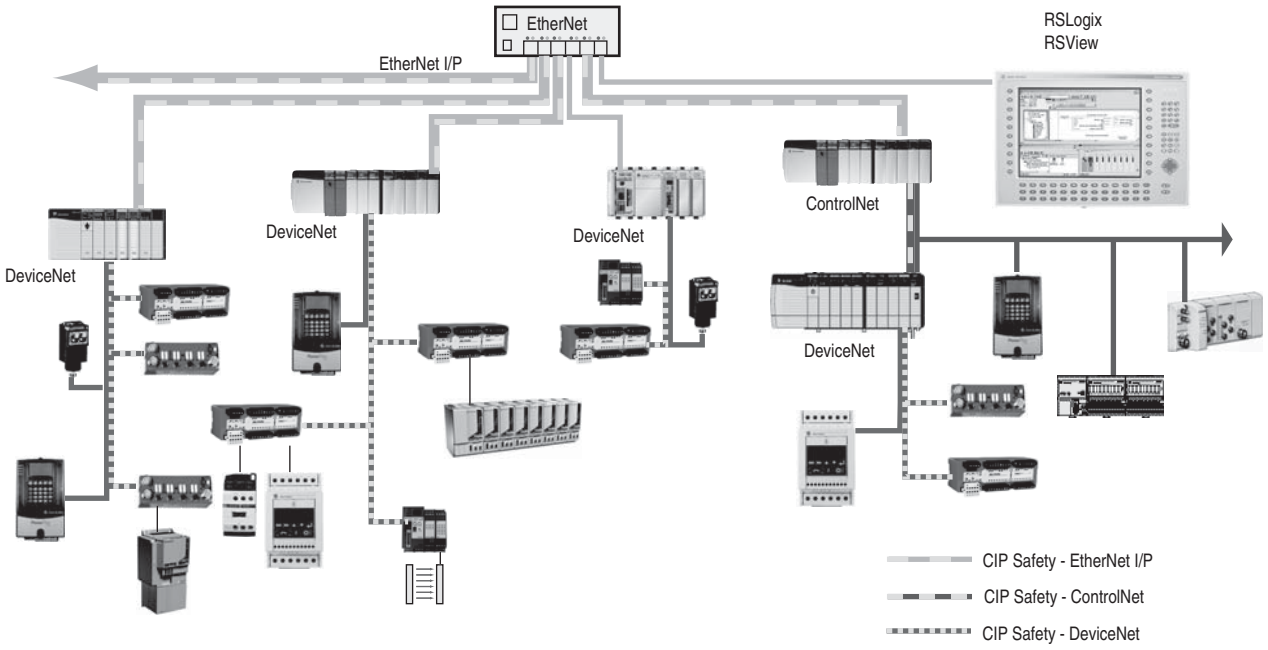


Figure 99 : exemple d'un réseau de sécurité réparti complexe

Sur les contacteurs de plus grande taille, un bloc de contacts supplémentaire n'est pas suffisant pour refléter de façon exacte l'état de la lame plus large. Les contracts miroirs, illustrés à la figure 101, situés de chaque côté du contacteur sont utilisés.

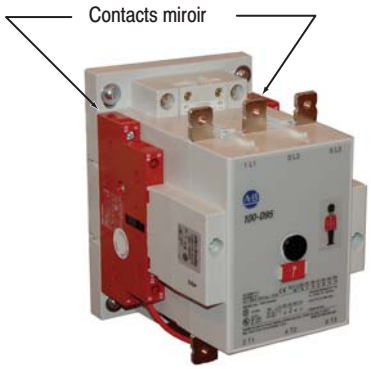


Figure 101 : contacts miroirs normalement fermés

Le temps de désexcitation des contacteurs auxiliaries ou des contacteurs jouent un rôle dans le calcul de la distance de sécurité. Un suppresseur de tension est souvent relié à la bobine pour améliorer la durée de vie des contacts qui commandent la bobine. Pour les bobines d'alimentation c.a., le temps de désexcitation n'est pas affecté. Pour les bobines d'alimentation c.c., le temps de désexcitation est allongé. L'augementation dépend du type de suppression choisi.

Les contacteurs auxiliaires et les contacteurs sont prévus pour interrompre des charges élevées entre 0,5 A et plus de 100 A. Le système de sécurité fonctionne avec des courants faibles. Le signal de retour génèré par le dispositif logique du système de sécurité peut être de quelques milliampères jusqu'à des dizaines de milliampères, généralement sous 24 V c.c. Les contacteurs auxiliaries de sécurité et les contacteurs de sécurité utilisent des contacts jumelés plaqués or pour interrompre de façon fiable ce courant faible.

Protection contre les surcharges

La protecton contre les surcharges des moteurs est requise 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 celle de l'opérateur. Les technologies disponibles actuellement peuvent détecter des condtions de défaut comme les surcharges, la perte de phase, un défaut de terre, un rotor bloqué, une sous-charge, un courant asymétrique et une surchauffe. Détecter et communiquer des conditions anormales avant le déclenchement permet d'améliorer le temps de production effectif et de protéger les opérateurs et le personnel de maintenance contre les situations dangereuses imprévues.

La figure 102 montre un exemple de dispositifs de protection contre les surcharges. Lorsque des contacteurs doubles sont utilisés pour assurer l'interruption d'un moteur dans une solution de catégorie 3, 4 ou commande fiable, un seul dispositif de protection contre les surcharges est nécessaire pour chaque moteur.

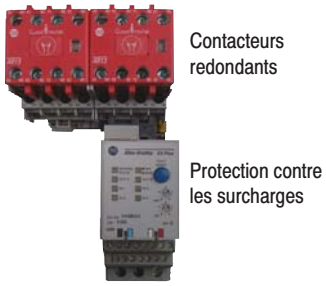


Figure 102 : protection contre les surcharges de contacteur

Variateurs et servovariateurs

Les variateurs et servovariateurs de sécurité peuvent être utilisés pour empêcher qu'une énergie de rotation ne soit transmise afin d'assurer un arrêt sécurisé ainsi qu'un arrêt d'urgence.

Les variateurs c.a. obtienne le classement de sécurité avec des voies redondantes pour couper l'alimentation du circuit de commande de gâchette. Une voie est le signal de validation, un signal matériel qui élimine le signal d'entrée du circuit de commande de gâchette. La deuxième voie est un relais à guidage réciproque qui élimine l'alimentation du circuit de commande de gâchette. Le relais à guidage réciproque renvoie également un signal d'état au système logique. Un schéma fonctionnel de la mise en œuvre de la fonction d'arrêt sécurisé dans le variateur PowerFlex est illustré à la figure 103.

Cette approche redondante permet au variateur de sécurité d'être utilisé dans les circuits d'arrêt d'urgence sans avoir recours à un contacteur.

Mesures de protection et équipement complémentaire

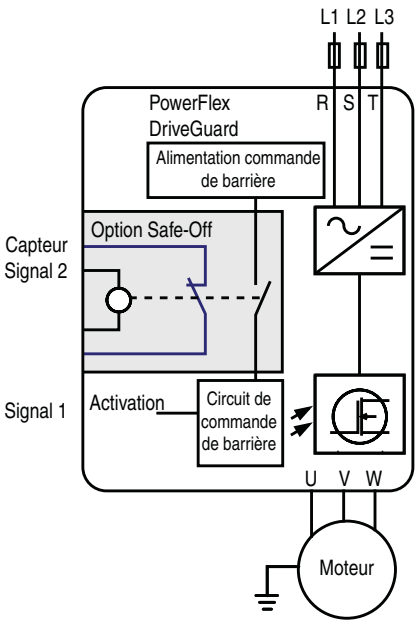


Figure 103 : signaux de sécurité du variateur

Le servovariateur obtient un résultat d'une façon similaire à celle des variateurs c.a. La figure 104 montre que les signaux de la sécurité redondante sont utilisés pour la fonction de sécurité. Un signal interrompt la commande vers le circuit de commande de gâchette. Un deuxième signal interrompt l'alimentation du circuit de commande de gâchette. Deux relais à guidage réciproque sont utilisés pour retirer les signaux et fournir un retour également au dispositif logique de sécurité.

Systèmes de raccordement

Les systèmes de raccordement apporte une plus value en réduisant les coûts d'installation et de maintenance des systèmes de sécurité. Les conceptions doivent prendre en compte les considérations de voie unique, voie double, voie double avec indication et types multiples de dispositifs.

Lorsqu'une connexion en série de dispositifs de verrouillage à double voie est nécessaire, un boîtier de distribution peut simplifier l'installation. La figure 105 montre un exemple simple d'une série de dispositifs de verrouillage raccordés à un port. Grâce à une proteciton IP67, ces types de boîtiers peuvent être montés sur la machine dans des installations décentralisées.

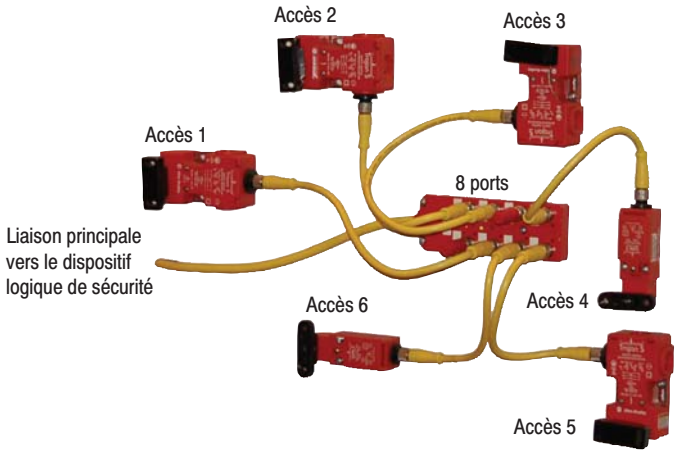


Figure 105 : boîtier de distribution de sécurité

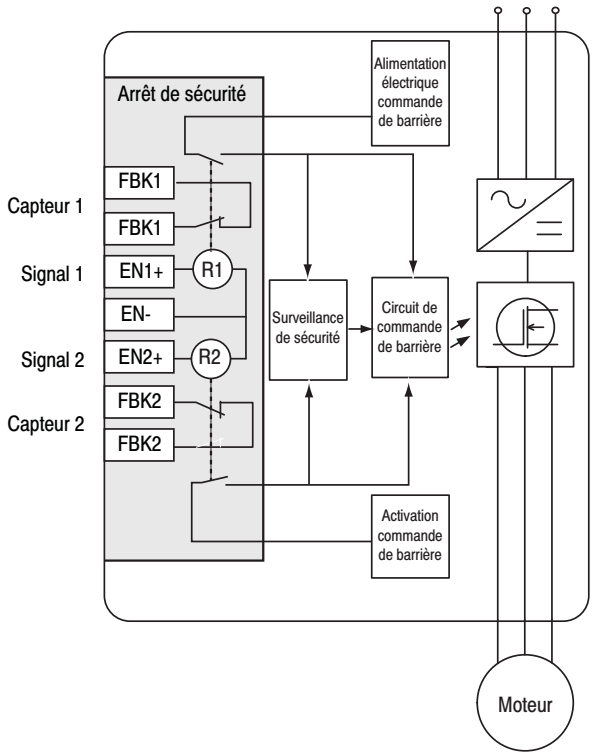


Figure 104 : signaux de sécurité du variateur Kinetix

Lorsque différents dispositifs sont nécessaires, un boîtier d'E/S ArmorBlock Guard I/O peut être utilisé. La figure 106 montre un boîtier à huit ports et un boîtier à quatre ports avec une protection IP67, qui peuvent être montés directement sur la machine sans coffret. Les entrées peuvent être configurées par le logiciel afin de pouvoir accueillir différents types de dispositifs.

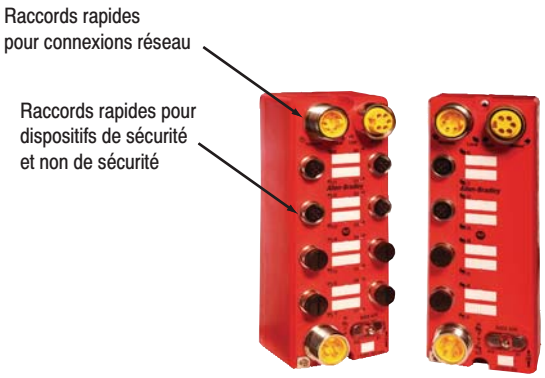


Figure 106 : ArmorBlock Guard I/O

Calcul des distances de sécurité

Les sources de danger doivent présenter un état de sécurité avant que l'opérateur ne puisse atteindre le danger. Pour le calcul des distances de sécurité, il existe deux groupes de normes qui se sont répendus. 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 nécessaire pour traiter la commande d'arrêt et de la distance que l'opérateur peut parcourir dans la zone de détection avant d'être détecter. La formule utilisée partout dans le monde a la même forme et les mêmes exigences. Les différences sont les symboles utilisés pour représenter les variables et les unités de mesure.

Les formules sont :

ISO EN :S =K x T+ C

US CAN : Ds =K x(Ts + Tc + Tr + Tbm) + Dpf

Où :

Ds et S représentent la distance de sécurité minimale entre la zone dangereuse et le point de détection le plus proche.

Directions d'approche

Lors du calcul de la distance de sécurité lorsqu'une barrière immatérielle ou un scrutateur de zone est utilisé, l'approche vers le dispositif de détection doit être prise en compte. Trois types d'approches sont à considérer :

Normale : approche perpendiculaire au plan de détection

Horizontale : approche parallèle au plan de détection

Selon un angle : approche de la zone de détection selon un angle.

Constante de vitesse

K est une constante de vitesse. La valeur de la constante de vitesse dépend des mouvements de l'opérateur (c.-à-d., vitesses des mains, vitesses de marche et longueur des pas). Ce paramètre est basé sur les données de recherche qui montrent qu'il est raisonnable de supposer une vitesse des mains de 1600 mm/s (63 in./s) avec le corps stationnaire. La situation réelle de l'application doit être prise en compte. De façon générale, la vitesse d'approche varie de 1600 mm/s (63 in./s) à 2500 mm/s (100 in./s). La constante de vitesse adéquate doit être déterminée par l'évaluation des risques.

Temps d'arrêt

T est le temps d'arrêt du système. Le temps total, en secondes, commence au moment de l'envoi du signal d'arrêt, jusqu'à l'arrêt du danger. Cette durée peut être divisée selon ses différentes parties (Ts, Tc, Tr et Tbm) pour faciliter l'analyse. Ts est le temps le plus long pour l'arrêt de la machine/de l'équipement. Tc est le temps le plus long pour l'arrêt du système de commande. Tr est le temps de réponse du dispositif de protection, et de son interface. Tbm est le temps d'arrêt supplémentaire autorisé par le dispositif de surveillance du freinage avant qu'il ne détecte une détérioration du temps d'arrêt au-delà des limites prédéfinies par l'utilisateur. Tbm est utilisé avec les presses mécaniques à tours incomplets. Ts + Tc + Tr sont généralement mesurés par un dispositif de mesure du temps d'arrêt si leurs valeurs sont inconnues.

Facteur de profondeur de pénétration

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

Dpf = 3,4 x (sensibilité d'objet – 6,875 mm), mais pas moins de zéro.

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

C = 8 x (sensibilité d'objet – 14 mm), mais pas moins de 0

La figure 107 montre une comparaison de deux facteurs. Ces deux formules ont un point d'intersection à 19,3 mm. Pour une sensibilité aux objets inférieure à 19 mm, l'approche de la norme US CAN est plus restrictive puisque la barrière immatérielle ou le scrutateur de zone doivent être plus éloignés du danger. Pour une sensibilité aux objets supérieure à 19,3 mm, la norme ISO EN est plus restrictive. Les fabricants de machines qui veulent fabriquer une machine utilisable dans le monde entier doivent s'appuyer sur les cas les plus défavorables des deux équations.

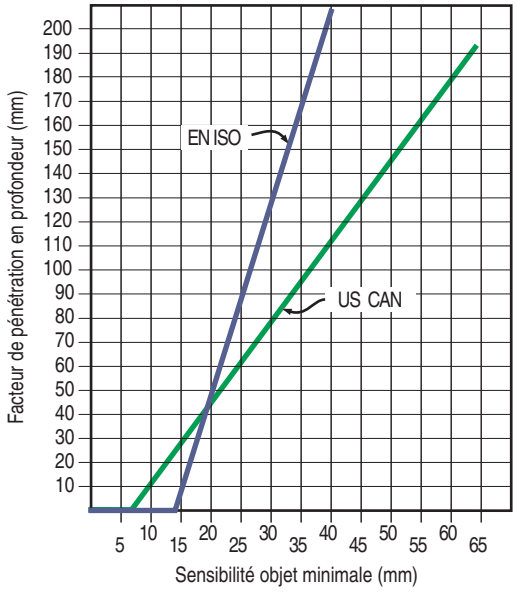


Figure 107 : profondeur de pénétration / sensibilité

Applicatins avec franchissement

Lorsque des sensibilités à des objets plus gros sont utilisées, les normes US CAN et ISO EN diffèrent légèrement pour le facteur de profondeur de pénétration et la sensibilité. La figure 108 résume les différences. La valeur de la norme ISO EN est de 850 mm, alors que la valeur de la norme US CAN est de 900 mm. Les normes diffèrent également dans le domaine de la sensibilité aux objets. La norme ISO EN permet 40 à 70 mm, alors que la norme US CAN permet jusqu'à 600 mm.

Calcul des distances de sécurité

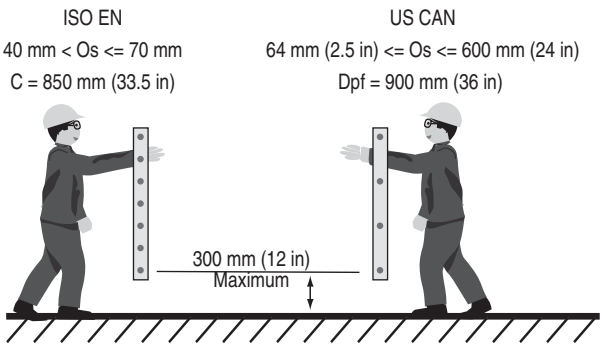


Figure 108 : facteurs de profondeur de pénétration pour applications avec franchissement

Applications avec franchissement par le haut

Les deux normes considèrent que la hauteur minimale du faisceau le plus bas doit être de 300 mm, mais elles diffèrent sur la hauteur minimale du faisceau le plus haut. La norme ISO EN indique 900 mm, alors que la norme US CAN indique 1200 mm. La figure 109 résume les différences.

La valeur du faisceau le plus haut semble être le point de divergence. Si l'on considère qu'il s'agit d'une application avec franchissement, la hauteur du faisceau le plus haut doit être bien plus élevée afin de prendre en compte un opérateur se tenant debout. Si l'opérateur peut passer par dessus le plan de détection, le critère de franchissement par le haut s'applique.

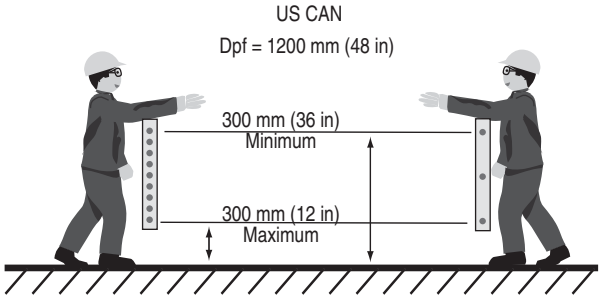


Figure 109 : facteurs de profondeur de pénétration pour applications avec franchissement par le haut

Un ou plusieurs faisceaux

Les systèmes à un ou plusieurs faisceaux distincts sont définis dans les normes ISO EN. Le tableau 5.1 montre les hauteurs « pratiques » pour plusieurs faisceaux au-dessus du sol. La profondeur de pénétration est de 850 mm dans la plupart des cas et de 1200 mm pour une utilisation avec un seul faisceau. En comparaison, la norme US CAN prend cela en considération par le biais de ses exigences relatives au franchissement. Le franchissement par le haut, par dessous ou par le côté des systèmes à un ou à plusieurs faisceaux doit toujours être prise en considération.

Nbre de faisceaux	Hauteur au-dessus du sol [mm (in.)]	C [mm (in.)]
1	750 (29,5)	1200 (47,2)
2	400 (15,7), 900 (35,4)	850 (33,4)
3	300 (11,8), 700 (27,5), 1100 (43,3)	850 (33,4)
4	300 (11,8), 600 (23,6), 900 (35,4), 1200 (47,2)	850 (33,4)

Tableau 7 : hauteurs et facteur de profondeur de pénétration pour un ou plusieurs faisceaux

Calculs des distances

Pour une approche normale des barrières immatérielles, le calcul des distances de sécurité des normes ISO EN et U.S. CAN sont proches, mais il existe des différences. Pour une approche normale des barrières immatérielles verticales pour lesquelles la sensibilité est au maximum de 40 m, la norme ISO EN requiert deux étapes. Premièrement, il faut calculer S et utiliser une vitesse constantde de 2000.

S = 2000 x T + 8 x (d -1 4)

La distance minimale de S peut être de 100 mm.

Une deuxième étape peut être utilisée lorsque la distance est supérieure à 500 mm. Puis, la valeur de K peut être réduite 1600. Lorsque K=1600 est utilisé, la valeur minimale de S est de 500 mm.

La norme U.S. CAN utilise une approche à une étape :

Ds = 1600 x T * Dpf

Cela conduit à des différences supérieures à 5 % entre les normes, lorsque le temps de réponse est inférieur à 560 ms. La figure 110 montre la distance de sécurité minimale en fonction du temps d'arrêt total pour des sensibilités de 14 et 30 mm. Une combinaison des deux approches doit être examinée afin d'obtenir le scénairo du cas le plus défavorable pour les machines destinées au marché mondial.

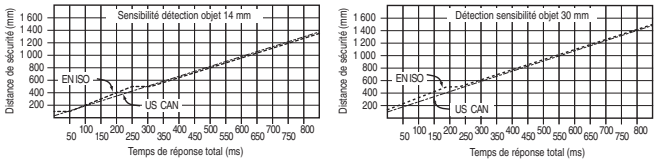


Figure 110 : comparaisons des distances de sécurité

Approches selon un angle

La plupart des barrières immatérielles et des scrutateurs sont installés verticalement (approche normale) ou horizontalement (approche parallèle). Ces montages ne sont pas considérés comme ayant un angle s'ils sont dans une plage de ±5° de l'utilisation prévue. Lorsque l'angle excède ±5°, les risques potentiels (p. ex., distance plus courte) liés aux approches prévisibles doivent être pris en considération. En général, les angles supérieurs à 30° par rapport au plan de référence (le sol par exemple) doivent être considérés comme normaux et les angles inférieurs à 30 sont considérés comme parallèles. Ceci est illustré à la figure 111.

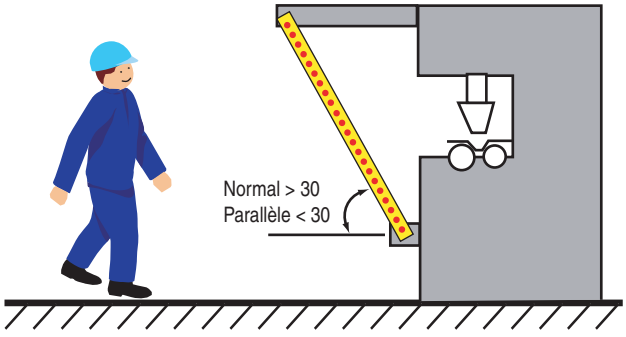


Figure 111 : approche du champ de détection selon un angle

Tapis de sécurité

Avec les tapis de sécurité, la distance de sécurité doit prendre en compte la vitesse et la longueur du pas des opérateurs. Cela en partant du principe que l'opérateur marche et que les tapis de sécurité sont montés au sol. Le premier pas de l'opérateur sur le tapis est un facteur de profondeur de pénétration de 1200 mm ou 48 in. Un exemple d'agencement est illustré à la figure 112.

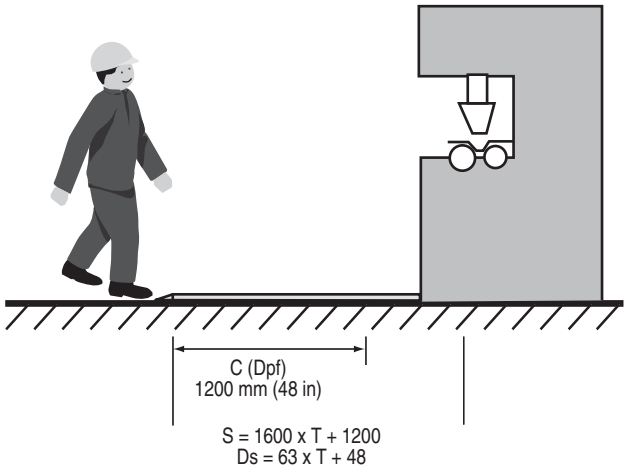


Figure 112 : tapis de sécurité monté au sol

Si l'opérateur doit monter sur une plate-forme, le facteur de profondeur de pénétration peut être réduit d'un facteur de 40 % de la hauteur de la marche (voir la figure 113).

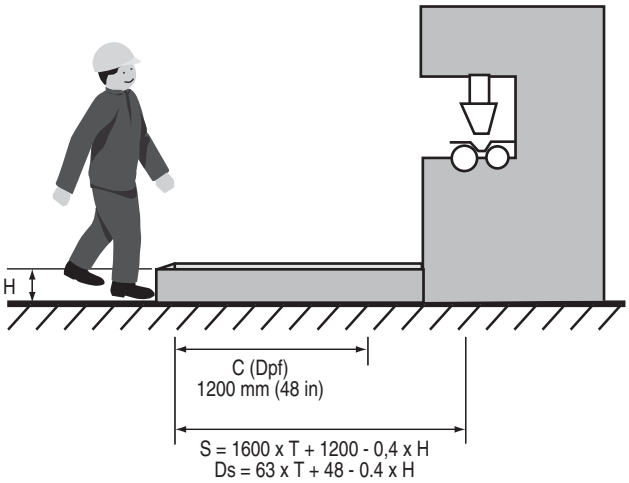


Figure 113 : tapis de sécurité monté sur une plate-forme

Exemples

Exemple : un opérateur utilise une approche normale vers une barrière immatérielle d'une sensibilité de 14 mm, qui est raccordée à un relais de surveillance lui-même raccordé à un contacteur c.c. avec un atténuateur à diode. Le temps de réponse du système de sécurité, Tr, est de 20 + 15 + 95 = 130 ms. Le temps d'arrêt de la machine, Ts+Tc, est de 170 ms. Aucune supervision de freinage n'est utilisée. La valeur Dpf est de 25,4 mm (1 in.), et la valeur C est zéro. Le calcul est le suivant :

Dpf = 3,4 (14 - 6,875) = 24,2 mm (1 in.) C = 8 (14-14) = 0
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 = 19,9 po (505 mm)

S = K x T + C
S = 1600 x (0,3) + 0
S = 480 mm (18,9 in.)

Par conséquent, la distance de sécurité minimale à laquelle la barrière immatérielle de sécurité doit être montée par rapport au danger est de 508 mm (20 in.) pour qu'une machine puisse être utilisée partout dans le monde.

Prévention de démarrage inattendu

La prévention des démarrages inattendus est abordée dans de nombreuses normes. Par exemple, dans ISO 14118, EN 1037, ISO 12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 et AS 4024.1603. Ces normes ont une base commune : la méthode principale pour la prévention des démarrages inattendus est de couper l'alimentation du système et de verrouiller le système en état désactivé. L'objectif est de permettre aux personnes de pénétrer en toute sécurité dans les zones dangereuses d'une machine.

Condamnation/signalisation

Les nouvelles machines doivent être construitent avec des dispositifs d'isolement d'énergie verrouillables. Ces dispositifs concernent tous les types d'énergie, notamment électrique, hydraulique, pneumatique, pesanteur et lasers. La condamnation fait référence au verrouillage d'un dispositif d'isolement de l'énergie. Le verrouillage ne doit être retiré que par son propriétaire ou par un superviseur dans des conditions contrôlées. Lorsque plusieurs personnes doivent travailler sur la machine, chaque personne doit installer son propre verrouillage sur les dispositifs d'isolement de l'énergie. Chaque verrouillage doivent permettre d'identifier son propriétaire.

Aux Etats-Unis, la signalisation est une alternative à la condamnation pour les machines plus anciennes sur lesquelles aucun dispositif de verrouillage n'a été installé. Dans ce cas, la machine est arrêtée et une étiquette est apposée pour prévenir tout le personnel de ne pas démarrer la machine tant que le propriétaire de l'étiquette travaille sur la machine. Depuis 1990, les machines modifiées doivent être mises à niveau pour inclure un dispositif d'isolement d'énergie verrouillable.

Un dispositif d'isolement de l'énergie est un dispositif mécanique qui empêche physiquement la transmission ou la libération d'énergie. Ces dispositifs peuvent se présenter sous la forme de disjoncteurs, de sectionneurs, d'interrupteur manuel, d'une combinaison de fiche/douille ou d'une vanne manuelle. Les dispositifs d'isolement électrique doivent interrompre tous les conducteurs d'alimentation non mis à la terre et aucun pôle ne doit fonctionner indépendamment.

L'objectif de la condamnationet/signalisation est d'empêcher le démarrage inattendu de la machine. Le démarrage inattendu peut avoir diverses causes : une défaillance du système de commande ; une action inappropriée sur une commande de démarrage, un détecteur, un contacteur ou une vanne ; une restauration de l'alimentation après une interruption ; ou autres influences internes ou externes. Lorsque le processus de condamnation/signalisation est terminé, la dissipation de l'énergie doit être vérifiée.

Systèmes d'isolement de sécurité

Les systèmes d'isolement de sécurité exécutent un arrêt automatique sans perte de données de la machine et fournissent également une méthode facile pour la condamnation de l'alimentation de la machine. Cette approche fonctionne bien pour les machines et les systèmes de fabrication de grande taille, particulièrement lorsque plusieurs sources d'énergie sont situées à un niveau intermédiaire ou à distance.

La figure 114 présente un schéma de système. Des stations verrouillables sont décentralisées, dans des endroits faciles d'accès de la machine. Lorsque c'est nécessaire, un opérateur utilise la station décentralisée pour arrêter la machine et la verrouiller en état désactivé. Le boîtier de commande déconnecte l'alimentation électrique et pneumatique, et renvoie un signal à l'opérateur pour indiquer que l'énergie a été déconnectée.

Prévention de démarrage inattendu

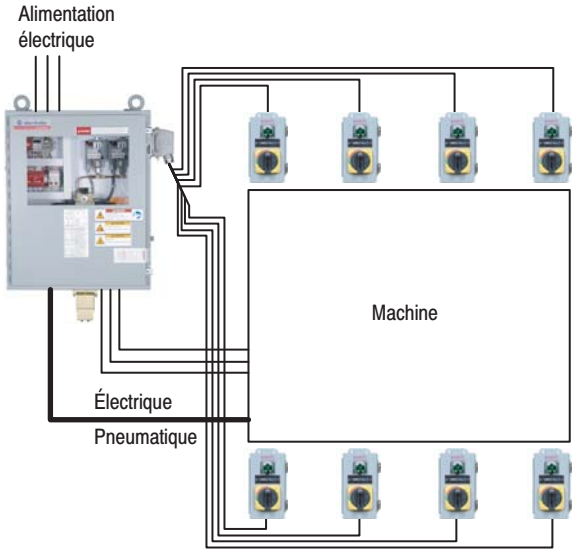


Figure 114 : schéma du système d'isolement de sécurité

La figure 115 montre que le système d'isolement de sécurité coupe non seulement l'alimentation de la machine, mais qu'il met à la terre le côté charge. L'opérateur reçoit un signal surveillé, visible au niveau de la station décentralisée qui indique que la machine est dans un état de sécurité et que l'énergie est dissipée.

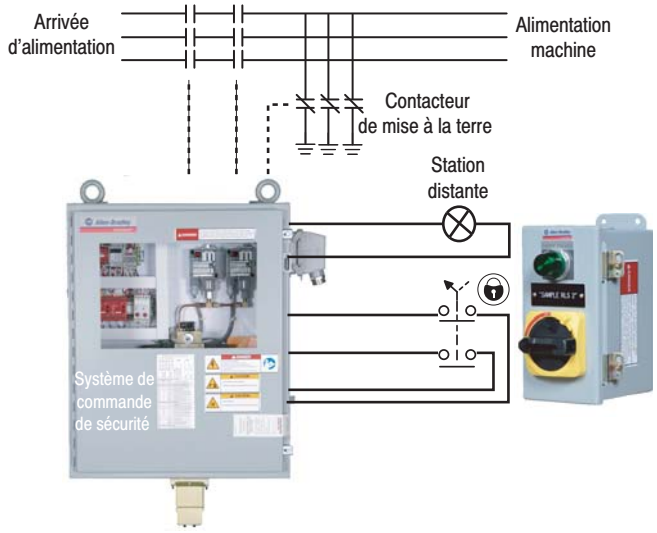


Figure 115 : le côté machine est mis à la terre avec un signal envoyé à l'opérateur

Déconnexion de charge

Pour l'isolement local des dispositifs électriques, des interrupteurs peuvent être placés juste avant le dispositif qui a besoin d'être isolé et condamné. Les interrupteurs de charge Série 194E constituent un exemple de produit capable d'isolement et de condamnation. La figure 116 présente un exemple de l'interrupteur Série 194E.

Figure 116 : interrupteur de charge avec capacité d'isolement et de condamnation

Systèmes de verrouillage à clé captive

Les systèmes de verrouillage à clé captive constituent une autre méthode pour mettre en place un système de condamnation. De nombreux systèmes à clé captive commencent par un dispositif d'isolement d'énergie. Lorsque l'interrupteur est ouvert par la clé « principale », l'énergie électrique de la machine est interrompue simultanément sur tous les conducteurs d'alimentation non mis à la terre. La clé principale peut être retirée et emmenée dans un endroit où l'accès à la machine est nécessaire. La figure 117 présente un exemple du système de base, un interrupteur d'isolement et un dispositif de verrouillage d'accès. Divers composants peuvent être ajoutés pour prendre en charge des agencements de condamnation plus complexes.

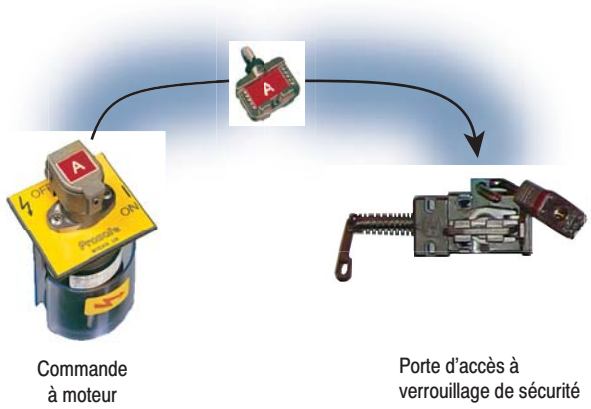


Figure 117 : dispositifs d'isolement verrouillables à clé captive

Alternatives à la condamnation

La condamnation et la signalisation doivent être utilisées pendant l'entretien et la maintenance des machines. Les interventions réalisées sur la machine en cours de fonctionnement normal sont couvertes par les dispositifs de protection. La différence entre les activités d'entretien/maintenance et de production n'est pas toujours claire.

Certains réglages et tâches d'entretien mineurs, qui sont effectués pendant les activités normales de production, ne nécessitent pas obligatoirement la condamnation de la machine. Par exemple, le chargement/déchargement des matériaux, les changements et réglages d'outils mineurs, la lubrification et l'élimination des déchets. Ces tâches doivent être routinières, répétitives et être inhérentes à l'utilisation de l'équipement de production ; de plus, 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 les dispositifs de verrouillage, les barrières immatérielles et les tapis de sécurité. Lorsqu'ils sont utilisés avec des dispostifis logiques et de sortie de sécurité appropriés, les opérateurs peuvent accéder en toute sécurité aux zones dangereuses de la machine au cours des tâches de production normale et d'entretien mineur.

Présentation des systèmes de commande de sécurité

Qu'est-ce qu'un système de commande de sécurité (SRCS) ? C'est la partie du système de commande d'une machine qui empêche la survenue d'une situation dangereuse. Il peut s'agir d'un système dédié et distinct ou il peut être intégré au système de commande normal de la machine.

Sa complexité varie d'un système simple, comme un interrupteur de sécurité pour grille de protection et un interrupteur d'arrêt d'urgence raccordés en série à la bobine de commande du contacteur d'alimentation, à un système combiné comprenant des dispositifs simples et complexes qui communiquent de façon logicielle et matérielle.

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

Fonction de sécurité

La fonction de sécurité est implémentée par les composants de sécurité du système de commande de la machine afin d'obtenir ou de maintenir une commande sécurisée de l'équipement par rapport à un danger spécifique. Une défaillance de la fonction de sécurité peut entraîner une augmentation immédiate des risques liés à l'utilisation de l'équipement, c'est-à-dire de la situation de danger.

Une machine doit présenter au moins un « danger », autrement ce n'est pas une machine. Une « situation de danger » se présente lorsqu'une personne est exposée à un risque. Une situation de danger n'implique pas que la personne soit blessée. La personne exposée peut être capable de reconnaître le danger et éviter les blessures. Cette personne peut ne pas être capable de reconnaître le danger, ou le danger peut être la conséquence d'un démarrage imprévu. La tâche principale du concepteur du système de sécurité est d'éviter les situations de danger et d'empêcher les démarrage imprévus.

La fonction de sécurité peut souvent être décrite par les exigences de plusieurs composants. Par exemple, la fonction de sécurité initiée par une grille de protection interconnectée a trois parties :

1. la source du danger protégée par la grille de protection ne peut pas fonctionner tant que la grille n'est pas fermée ;
2. l'ouverture de la grille arrête la source du danger si elle est en fonctionnement au moment de l'ouverture ; et
3. la fermeture de la grille ne redémarre pas la source du danger protégée par la grille.

Lorsque la fonction de sécurité est définie pour une application spécifique, le mot « danger » doit être remplacé par le danger spécifique. Le danger ne doit pas être confondu avec les conséquences de ce danger. L'écrasement, les coupures et les brûlures sont les conséquences d'un danger. Exemples de danger : moteur, piston, couteau, torche, pompe, laser, robot, effecteur, électro-aimant, vanne, autre type d'actionneur, ou un danger mécanique impliquant la pesanteur.

Lorsque l'on traite des systèmes de sécurité, l'expression « au moment où ou avant que la fonction de sécurité ne soit sollicitée » est utilisée. Qu'est-ce qu'une sollicitation de la fonction de sécurité ? Exemples de sollicitation de la fonction de sécurité : ouvrir une grille de protection interconnectée, interrompre une barrière immatérielle, monter sur un tapis de sécurité ou appuyer sur un arrêt d'urgence. L'opérateur sollicite l'arrêt du danger ou qu'il reste désactivé s'il était déjà arrêté.

Les composants de sécurité du système de commande de la machine exécute la fonction de sécurité. Cette fonction de sécurité n'est pas exécutée par un seul dispositif ; uniquement par la grille de protection par exemple. Le dispositif de verrouillage de la grille de protection envoie une commande à un dispositif logique, qui à son tour désactive un actionneur. La fonction de sécurité commence par la commande et se termine par sa mise en œuvre.

Le système de sécurité doit être conçu avec un niveau d'intégrité correspondant aux risques présentés par la machine. Les risques élevés requièrent des niveaux d'intégrité élevés afin d'assurer le bon fonctionnement de la fonction de sécurité. Les systèmes de sécurité de la machine peuvent être classés par les niveaux de performance correspondants à leur capacité à exécuter la fonction de sécurité ou, en d'autres termes, le niveau d'intégrité de leur sécurité fonctionnelle.

Présentation de la sécurité fonctionnelle des systèmes de commande

IMPORTANT Les normes et les exigences abordées dans cette section sont relativement nouvelles. Le travail des groupes rédactionnels se poursuit sur certains aspects, particulièrement en ce qui concerne la clarification et la combinaison de certaines de ces normes. Il est donc possible que des modifications soient apportées concernant certaines informations données dans ces pages. Pour obtenir les dernières informations, consultez le site Internet de Rockwell Automation sur les systèmes et composants de sécurité : http://www.ab.com/safety, et le site Internet de Rockwell Automation sur les solutions de sécurité : http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx.

En quoi consiste la sécurité fonctionnelle ?

La sécurité fonctionnelle est la partie du système de sécurité général qui dépend du fonctionnement correct des processus ou équipements en réponse à ses entrées. La norme CEI TR 61508-0 fournit les exemples suivants pour aider à clarifier la signification de la sécurité fonctionnelle. « Par exemple, un thermostat installé sur 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 l'installation d'une isolation spécialisée pour résister aux températures élevées n'est pas un exemple de sécurité fonctionnelle (bien qu'il s'agisse d'un exemple de sécurité qui peut protéger contre le même danger) ». Comme autre exemple, comparons un dispositif de protection matérielle à un dispositif de protection à verrouillage. Le dispositif de protection matérielle n'est pas considéré comme une « sécurité fonctionnelle », bien qu'il puisse protéger contre l'accès à la même zone dangereuse qu'une grille interconnectée. A l'inverse, la grille de protection à verrouillage est considérée comme un dispositif de sécurité fonctionnelle. En effet, lorsque la grille est ouverte, le mécanisme de verrouillage communique avec le système afin de prévenir toute situation à risque.De la même façon l'équipement de protection individuel (PPE) est utilisé comme mesure de protection pour améliorer la sécurité des personnes. Le PPE n'est pas considéré comme une sécurité fonctionnelle.

Le terme sécurité fonctionnelle a été introduit par la norme CEI 61508:1998. Depuis, ce terme a parfois été associé uniquement avec les systèmes de sécurité programmables. Mais il s'agit d'une erreur. La sécurité fonctionnelle couvre un large éventail de dispositifs utilisés pour créer des systèmes de sécurité. Les dispositifs comme les barrières immatérielles, les relais de sécurité, les automate 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. Voila ce qu'est la sécurité fonctionnelle.Par conséquent, la sécurité fonctionnelle d'un système de commande électrique est très pertinente pour le contrôle des dangers présentés par les pièces mobiles d'une machine.

Deux types d'exigences sont requis pour la sécurité fonctionnelle :

- La fonction de sécurité
- L'intégrité de la sécurité

L'évaluation des risques joue un rôle clé dans l'élaboration des exigences relatives à la sécurité fonctionnelle. L'analyse des tâches et des dangers conduit aux exigences fonctionnelles pour la sécurité (c.-à-d., la fonction de sécurité). La quantification des risques conduit aux exigences relatives à l'intégrité de la sécurité (c.-à-d., l'intégrité de la sécurité ou le niveau de performance).

Quatre des plus importantes normes machines relatives à la sécurité fonctionnelle des systèmes de commande sont :

1. CEI/EN 61508 « Sécurité fonctionnelle des systèmes de commande électrique, électronique et électronique programmable

   Cette norme définit les exigences et les dispositions relatives à la conception de systèmes et sous-systèmes électroniques et programmables complexes. Il s'agit d'une norme générale qui peut être utilisée dans tous les secteurs industriels.

2. CEI/EN 62061 "Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électrique, électronique et électronique programmable relatifs à la sécurité"

   Cette norme est l'implémentation spécifique aux machines de la norme CEI/EN 61508. Les règles qu'elle préconise en matière de conception sont applicables à tous les systèmes de commande électrique relatifs à la sécurité des machines, quel qu'en soit le type, ainsi qu'à tous les sous-systèmes ou dispositifs non complexes. Elle requiert la conformité des sous-systèmes complexes ou programmables à la norme CEI/EN 61508.

3. EN ISO 13849-1 "Sécurité des machines – Composants de sécurité des systèmes de commande"

   Cette norme est destinée à fournir une transition directe pour les catégories de l'ancienne norme EN 954-1.

4. CEI 61511 "Sécurité fonctionnelle – Systèmes équipés pour la sécurité et destinés à l'industrie des procédés"

   Cette norme est l'implémentation spécifique au secteur des procédés de la norme CEI/EN 61508.

Les normes de sécurité foncitonnelle représentent une étape significative pour aller au-delà des exigences existantes sur la fiabilité de la commande et le système de catégories de la norme ISO 13849-1:1999 (EN 954-1:1996) précédente.

Remarque : peu de temps avant la publication de ce texte, le CEN (Comité européen de normalisation) a annoncé que la date finale pour la présomption de conformité à la norme EN 954-1 serait étendue jusque fin 2011 afin de faciliter la transition vers des normes plus récentes. Ceci remplace la date originale qui était fixée au 29 décembre 2009.

Pour les informations les plus récentes sur l'utilisation et l'état de la norme EN 954-1, visitez : *http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx*. En attendant, il est recommandé d'utiliser l'extension de la période de transition pour passer aux nouvelles normes (EN ISO 13849-1 ou CEI/EN 62061) en temps utile.

Les catégories ne disparaîtront pas totalement ; elles apparaissent également dans la norme actuelle EN ISO 13849-1 qui utilise le concept de sécurité fonctionnelle et a introduit une nouvelle terminologie et de nouvelles exigences. Elle présente des ajouts et des différences significatifs par rapport à l'ancienne norme EN 954-1 (ISO 13849-1:1999). Dans cette section nous nous référerons à la version actuelle EN ISO 13849-1. (EN ISO 13849-1:2008 a le même texte que la norme ISO 13849-1:2006).

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

Les normes CEI/EN 62061 et ISO/EN 13849-1 concernent toutes deux les systèmes de commande électrique relatifs à la sécurité. Il est prévu qu'elles soient combinées en une seule norme utilisant une terminologie commune. Toutes deux permettent d'obtenir les mêmes résultats, mais font appel à des méthodes différentes. Leur objectif est de permettre aux utilisateurs de choisir celle qui est la plus adaptée à leur situation. Un utilisateur peut choisir d'utiliser l'une ou l'autre norme ; elles sont de plus harmonisés sous la Directive Machines européenne.

Les deux normes donnent des résultats comparables en termes de niveau de performance et d'intégrité de la sécurité. Les méthodologies sont en effet adaptées aux utilisateurs auxquels elles sont destinées.

La méthodologie de la norme CEI/EN 62061 permet l'utilisation de fonctions de sécurité complexes qui peuvent être implémentées par des architectures système non conventionnelles. La méthodologie de la norme EN ISO 13849-1 fournit une chemin plus direct et moins compliqué pour les fonctions de sécurité conventionnelles implémentées par les architectures système conventionnelles.

Une distinction importante entre ces deux normes est l'applicabilité de diverses technologies. La norme CEI/EN 62061 est limitée aux systèmes électriques. Tandis que la norme ISO/EN 13849-1 est applicable aux systèmes pneumatiques, hydrauliques, mécaniques et électriques.

La figure 118 fournit une schéma fonctionnel simplifié pour aider le concepteur du système de sécurité à choisir laquelle de ces deux normes utiliser.

Rapport technique conjoint sur les normes CEI/EN 62061 et EN ISO 13849-1

Un rapport conjoint a été préparé par la CEI et l'ISO afin d'aider les utilisateurs des deux normes.

Il explique la relation entre les deux normes et explique comment établir l'équivalence entre le niveau de performance PL (Performance level) de la norme EN ISO 13849-1 et le niveau d'intégrité de la sécurité SIL (Safety Integrity Level) de la norme CEI.EN 62061, aussi bien au niveau système qu'au niveau sous-système.

Afin de montrer que les deux normes donnent des résultats équivalents, le rapport donne un exemple de système de sécurité calculé selon les méthodologies des deux normes.

Ce rapport clarifie également plusieurs questions qui font l'object de différentes interpértations. L'une des questions les plus significatives est peut-être l'aspect des exclusions de défauts.

En général, lorsqu'un niveau de performance PLe est requis pour qu'une fonction de sécurité soit mise en œuvre par un système de commande de sécurité, il n'est pas normal de s'appuyer uniquement sur les exclusions de défaut afin d'atteindre ce niveau de performance. Cela dépend de la technologie utilisée et de l'environnement d'utilisation prévu. Il est donc essentiel que le concepteur prenne des précautions supplémentaires pour l'utilisation des exclusions de défaut à mesure que les exigences PL augmentent.

En général, l'utilisation des exclusions de défaut ne peut s'appliquer aux aspects mécaniques des interrupteurs de fin de course électromécaniques et des interrupteurs manuels (p. ex., un dispositif d'arrêt d'urgence) afin d'atteindre un niveau PLe dans la conception du système de commande de sécurité. Les exclusions de défaut pouvant être appliquées à des conditions de défaut mécanique spécifiques (p. ex., usure/corrosion, rupture) sont décrites dans le tableau A.4 de la norme ISO 13849-2.

Par exemple, un système de verrouillage de porte qui doit atteindre un niveau de performance PLe doit incorporer une tolérance aux défauts minimale de 1 (p. ex., deux interrupteuirs de fin de course mécaniques conventionnels) afin d'atteindre ce niveau de performance puisqu'il n'est normalement pas justifiable d'exclure les défauts, comme par exemple des actionneurs d'interrupteur défaillants. Cependant, il peut être acceptable d'exclure des défauts, comme un court-circuit du câblage dans un panneau de commande conçu en conformité avec les normes appropriées.

SIL et CEI/EN 62061

CEI/EN 62061 décrit à la fois le niveau de risque qui doit être réduit et la capacité d'un système de commande à réduire ce risque en termes de niveau d'intégrité SIL (Safety Integrity Level). Trois niveaux SIL sont utilisés dans le secteur des machines, SIL 1 est le plus faible et SIL 3 est le plus élevé.

Etant donné que l'abréviation SIL est utilisé de la même façon dans d'autres secteurs industriels, comme la pétrochimie, la génération de puissance et les chemins de fer, la norme CEI/EN 62061 est très utile lorsque les machines sont utilisées dans ces secteurs.

Des risques plus importants peuvent survenir dans d'autres secteurs, comme dans l'industrie des procédés ; par conséquent, la norme CEI 61508 et la normeCEI 61511 spécifique au secteur des procédés incluent un niveau SIL 4.

Un classement SIL concerne une fonction de sécurité. Les sous-systèmes qui composent le système qui met en œuvre la fonction de sécurité doivent avoir un niveau SIL adapté. Cela est parfois appelé la limite de déclaration SIL (SIL Claim Limit - SIL CL).

Une étude complète de la norme CEI/EN 62061 est nécessaire avant qu'elle ne puisse être correctement appliquée. Certaines des exigences de la norme pouvant faire l'objet d'une application générale sont présentées plus loin.

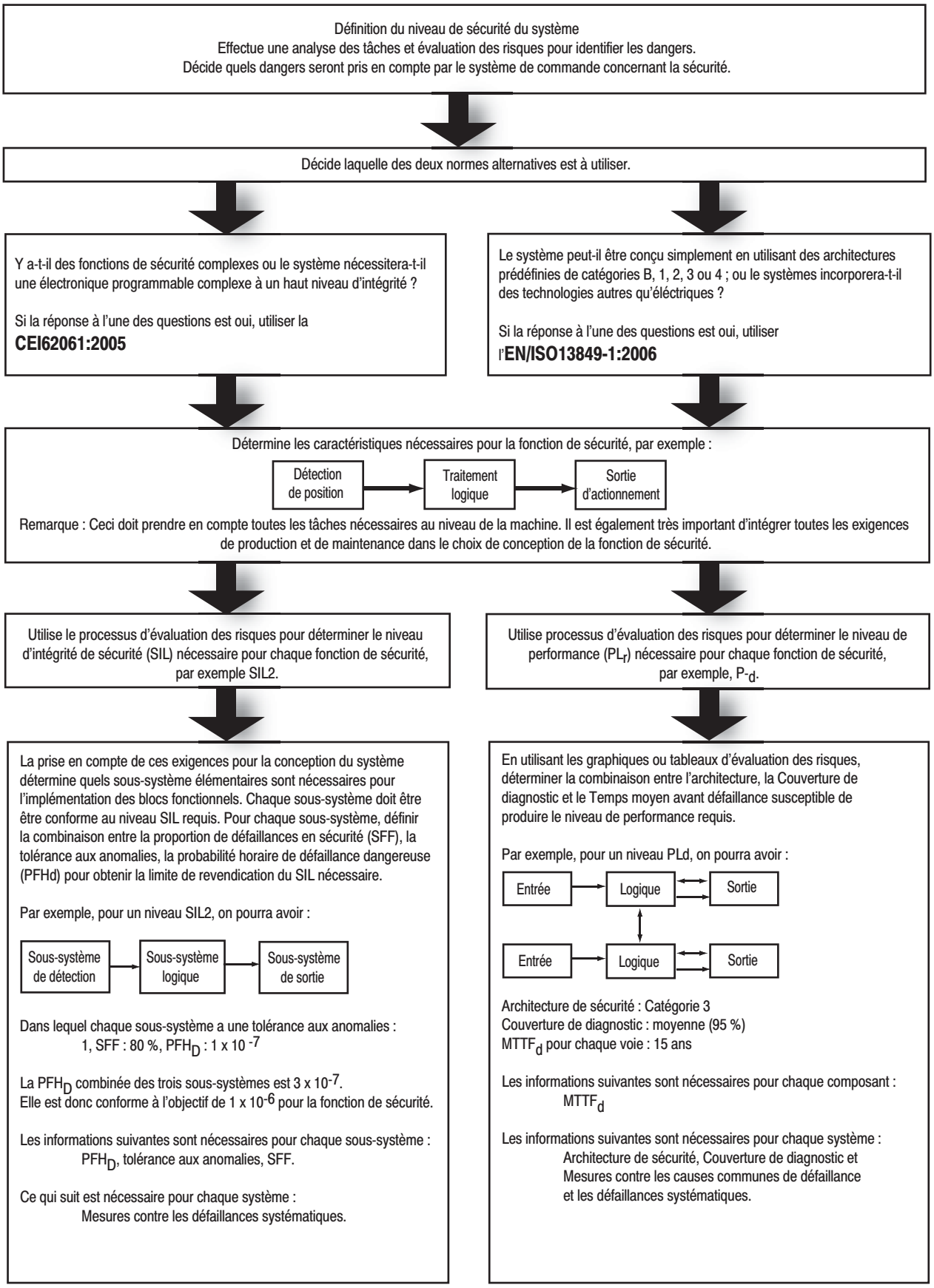


Figure 118 : schéma de conception du système

Conception de système ISO/EN 13849 et SISTEMA

PL et EN ISO 13849-1

EN ISO 13849-1 n'utilise pas l'abréviation SIL, mais PL (Performance Level) pour niveau de performance. PL peut être relié à SIL sur de nombreux aspects. Il existe cinq niveaux de performance, PLa est le plus faible et PLe est le plus élevé.

Comparaison entre PL et SIL

Le tableau 8 montre la relation entre PL et SIL en terme de probabilité de défaillance dangereuse lorsque ces niveaux de performance sont appliqués à des structures de circuit typiques.

PL (Performance Level)	PFH_D (probabilité de défaillance dangereuse par heure)	SIL
a	$\geq 10^{-5}$ à $<10^{-4}$	Aucun
b	$\geq 3 \times 10^{-6}$ à $<10^{-5}$	1
c	$\geq 10^{-6}$ à $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ à $<10^{-6}$	2
e	$\geq 10^{-8}$ à $<10^{-7}$	3

Tableau 8 : Correspondance approximative entre PL et SIL

IMPORTANT Le tableau 8 est donné à titre de recommandation et NE DOIT PAS être utilisé pour la conversion. Toutes les exigences des normes doivent être prises en compte.

Conception de système EN ISO 13849 et SISTEMA

Une étude complète de la norme EN ISO 13849-1 est nécessaire avant qu'elle ne puisse être correctement appliquée. Ce qui suit est une présentation rapide :

Cette norme définit des exigences pour la conception et l'intégration des composants de sécurité des systèmes de commande, notamment certains aspects logiciels. La norme concerne le système de sécurité mais peut égalemnet être appliquée aux composants du système.

Outil de calcul du niveau PL du logiciel SISTEMA

SISTEMA est un logiciel destiné à la mise en œuvre de la norme EN ISO 13849-1. Son utilisation simplifie très largement la mise en œuvre de la norme.

SISTEMA signifie "Safety Integrity Software Tool for the Evaluation of Machine Applications" (logiciel d'intégrité de la sécurité pour l'évaluation des applications machines). Il a été développé par BGIA en Allemagne et est libre de droits. Il requiert d'entrer différents types de données de sécurité fonctionnelle, comme décrit plus loin dans cette section.

Les données peuvent être entrées manuellement ou automatiquement par le biais de la bibliothèque de données SISTEMA d'un fabricant (SISTEMA Data Library).

La bibliothèque de données SISTEMA de Rockwell Automation est disponible en téléchargement, avec un lien vers le site de téléchargement de SISTEMA, sur : http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx.

Présentation de la norme EN ISO 13849-1

Cette norme a un domaine d'application très large puisqu'elle concerne toutes les technologies, notamment électricité, hydraulique, pneumatique et mécanique. Bien que la norme ISO 13849-1 concerne les systèmes complexes, elle renvoit également le lecteur vers les normes CEI 62061 et CEI 61508 pour les sytèmes logicielles intégrés complexes.

Voyons quelles sont les différences de base entre l'ancienne norme EN 954-1 et la nouvelle norme EN ISO 13849-1. L'ancienne norme définissait les Catégories [B, 1, 2, 3 ou 4]. La nouvelle norme définit les Niveaux de performance [PL a, b, c, d ou e]. Le concept des catégories est conservé mais il existe des exigences supplémentaires à satisfaire avant qu'un niveau PL puisse être atteint par un système.

Les exigences peuvent être listées sous une forme simple de la façon suivante :

- L'architecture du système. Cela couvre essentiellement ce à quoi nous nous sommes habitués en tant que Catégories
- Des données de fiabilité sont requises pour les composants du système
- Le taux de couverture des tests de diagnostic (Diagnostic Coverage - DC) du système est requis. Cela représente le niveau de surveillance des défauts dans le système
- Protection contre les défaillances de cause commune
- Protection contre les défauts systématiques
- Le cas échéant, les exigences logicielles particulières

Nous étudierons ces facteurs de plus près plus tard ; mais avant cela, il est utile d'étudier l'intention et le principe de base de la norme dans son ensemble. Il est clair à ce stade qu'il y a d'autres choses à apprendre, mais les détails auront plus de sens lorsque nous aurons compris quel est son objectif et sa raison d'être.

Premièrement, pourquoi avons-nous besoin d'une nouvelle norme ? Il est évident que la technologie utilisée dans les systèmes de sécurité des machines a progressé et changé considérablement au cours des dix dernières années. Jusqu'à récemment, les systèmes de sécurité dépendaient d'équipements "simples" présentant des modes de défaillance prévisibles. Ces dernières années, nous avons vu l'émergence de dispositifs électroniques et programmables plus complexes dans les systèmes de sécurité. Cela nous a été bénéfique en termes de coût, de flexibilité et de compatibilité, mais cela signifie également que les normes existantes ne sont plus adaptées. Pour savoir si un système de sécurité est suffisant, nous devons en savoir plus sur ce système. C'est pourquoi la nouvelle norme demande plus d'informations. A mesure que les systèmes de sécurité commencent à utiliser une approche de type "boîte noire", nous dépendons plus de leur conformité aux normes. Ces normes doivent donc être capables d'interroger correctement la technologie. Pour cela, elles doivent communiquer avec les facteurs de base en matière de fiabilité, de détection des défauts et d'intégrité architecturale et du système. C'est l'objectif de la norme EN ISO 13849-1.

Pour tracer un chemin logique au travers de la norme, deux types d'utilisateurs fondamentalement différents doivent être pris en compte : le concepteur des sous-systèmes de sécurité et le concepteur des systèmes de sécurité. En général le concepteur du sous-système (généralemnet un fabricant de composants de sécurité) est soumis à un niveau de complexité supérieur. Il doit fournir les données requises pour que le concepteur du système puisse s'assurer que le sous-système a une intégrité suffisante pour le système. En général, cela nécessite des tests, une analyse et des calculs. Les résultats sont exprimés sous la forme de données requises par la norme.

Le concepteur du système (généralement un concepteur ou un intégrateur de machines) utilise les données du sous-système pour effectuer des calculs relativement simples afin de déterminer le niveau de performance (PL) global du système.

PLr est utilisé pour indiquer quel niveau de performance est requis par la fonction de sécurité. Pour déterminer le PLr, la norme fournit un graphique des risques dans lequel sont indiqués les facteurs de gravité des blessures, de fréquence d'exposition et de possibilité d'évitement pour l'application.

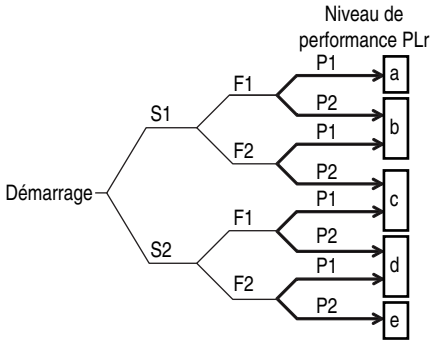


Figure 119 : graphe des risques - annexe A de la norme EN ISO 13849-1

Le résultat est le niveau PLr. Les utilisateurs de l'ancienne norme EN 954-1 reconnaîtront cette approche, mais il faut noter que la ligne S1 est désormais divisée. Notez que cela peut signifier une nouvelle prise en compte de l'intégrité des mesures de sécurité requises aux niveaux les moins élevés de risque.

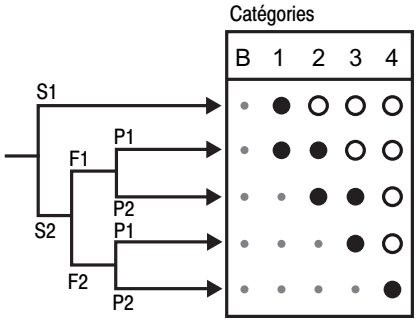


Figure 120 : graphe des risques - annexe B de la norme EN 945-1

Il reste une partie très importante à aborder. Nous savons désormais par la norme à quel niveau le système doit être et également comment déterminer son niveau actuel, mais nous ne savons pas ce qu'il doit faire. Nous devons définir ce que doit être la fonction de sécurité. Il est clair que la fonction de sécurité doit être adaptée à la tâche. Comment s'assurer qu'elle l'est ? Comment la norme nous y aide-t-elle ?

Il est important de réaliser que la fonction requise ne peut être déterminée que par la prise en compte des caractéristiques présentes dans l'application réelle. Cela peut être considéré comme l'étape de conception de la sécurité. Elle ne peut pas être totalement couverte par la norme puisque la norme ne connaît pas toutes les caractéristiques d'une application spécifique. Ceci concerne souvent également le constructeur de machines qui produit la machine, mais qui ne connaît pas forcément les conditions exactes dans lesquelles elle sera utilisée.

La norme fournit une aide en listant un grand nombre d'utilisation courantes des fonctions de sécurité (p. ex., fonction d'arrêt sécurisé initié par un dispositif de protection, fonction d'inhibition, fonction de démarrage/redémarrage) et en indiquant certaines des exigences généralement connexes à ces fonctions. L'utilisation d'autres normes, comme la norme EN ISO 12100 : Principes de base pour la conception, et la norme EN ISO 14121 : Evaluation des risques, est fortement recommandées à ce stade. Il existe également un grand nombre de normes spécialement adaptées à certaines machines qui fournissent des solutions pour des machines particulières. Dans les normes européenne (EN), se sont des normes de type C, dont certaines ont des équivalents exacts dans les normes ISO.

Nous voyons désormais que l'étape de conception de la sécurité dépend du type de machine et également des caractéristiques de l'application et de l'environnement dans lequel elle est utilisée. Le constructeur de machines doit anticiper ces facteurs pour être capable de concevoir la sécurité. Les conditions d'utilisation prévues doivent être indiquées dans le manuel utilisateur. L'utilisateur de la machine doit vérifier que ces conditions correspondent aux conditions d'utilisation réelles.

Nous avons désormais une description de la fonction de sécurité. Grâce à l'annexe A de la norme, nous connaissons également le niveau de performance requis [PLr] pour les composants de sécurité du système de commande (SRP/CS) qui seront utilisés pour mettre en œuvre cette fonction. Nous devons maintenant concevoir le système et nous assurer qu'il est conforme au niveau PLr.

Un des facteurs important pour décider quelle norme utiliser [EN ISO 13849-1 ou EN/CEI 62061] est la complexité de la fonction de sécurité. Dans la plupart des cas, pour ce qui est des machines, la fonction de sécurité est relativement simple et la norme EN ISO 13849-1 est l'option la plus adaptée. Les données de fiabilité, le taux de couverture des tests de diagnostic (DC), l'architecture système (catégorie), la défaillance de cause commune et, le cas échéant, les exigences logicielles sont utilisés pour évaluer le niveau de performance PL.

Ceci est une description simplifiée destinée uniquement à donner un aperçu. Il est important de comprendre que toutes les dispositions de la norme doivent être mises en application. Cependant, une aide est disponible. Le logiciel SISTEMA est là pour aider dans les domaines de la documentation et des calculs. Il produit égalemnet un document technique.

Au moment de la plublication de ce document, SISTEMA est disponible en allemand et en anglais. D'autres langues seront disponibles plus tard. BGIA, le développeur de SISTEMA, est un institut de recherche et développement très respecté basé en Allemagne. Il est particulièrement engagé à résoudre des problèmes scientifiques et techniques relatifs à la sécurité dans le domaine de l'assurance obligatoire des accidents et de la prévention en Allemagne. Il collabore avec les organismes qui s'occupent de la santé et la sécurité au travail dans plus de 20 pays. Les experts de BGIA, avec leurs collègues de BG, ont largement participé à la rédaction des normes EN ISO 13849-1 et CEI/EN 62061.

La « bibliothèque » des données de composants de sécurité de Rockwell Automation pour SISTEMA est disponible sur : *http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx*.

Quelle que soit la façon dont le calcul du niveau de performance PL est effectué, il est important de partir de bonnes bases. Nous devons aborder notre système de la même façon que la norme, alors commençons par cela.

Structure du système

Tout système peut être divisé selon les composants à la base de ce système ou en "sous-systèmes." Chaque sous-système a sa propre fonction discrète. La plupart des systèmes peuvent être divisés selon trois fonctions de base ; entrée, résolution logique et déclenchement (certains systèmes simples n'ont pas de résolution logique). Les groupes de composants qui implémentent ces fonctions sont les sous-systèmes.

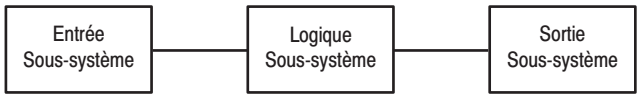


Figure 121

Un exemple de système électrique simple à une voie est donné à la figure 122. Il n'est constiué que de sous-systèmes d'entrée et de sortie.

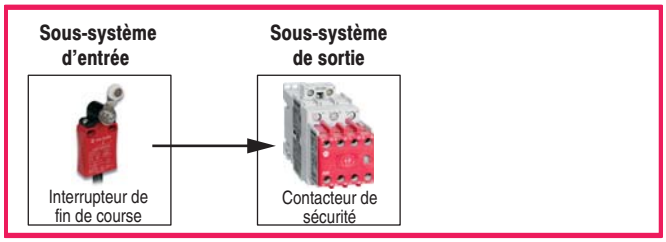


Figure 122 : interrupteur de sécurité et contacteur

A la figure 123, le système est un peu plus complexe parce qu'une certain quantité de logique est également requise. L'automate de sécurité lui-même a une tolérance interne aux défauts (p. ex., double voie), mais le système global est toujours limité à une voie à cause de l'unique interrupteur de fin de course et de l'unique contacteur.

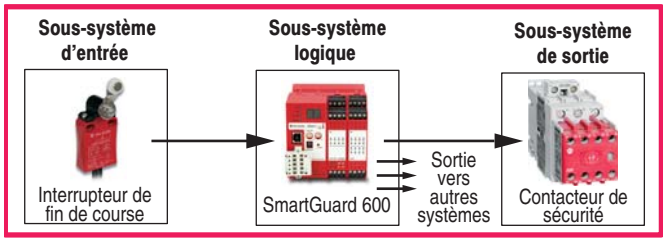


Figure 123 : interrupteur de sécurité, automate de sécurité et contacteur de sécurité

Si nous prenons l'architecture de base de la figure 123, il y a également d'autres points à prendre en considération. D'abord, combien de "voies" le système a-t-il ? Un système à une voie est défaillant si l'un de ses sous-systèmes est défaillant. Un système à deux voies (également appelé redondant) doit présenter deux défaillances, une sur chaque voie, avant que le système soit défaillant. Etant donné qu'il possède deux voies, il peut tolérer une défaillance et continuer à fonctionner. La figure 124 montre un système à deux voies.

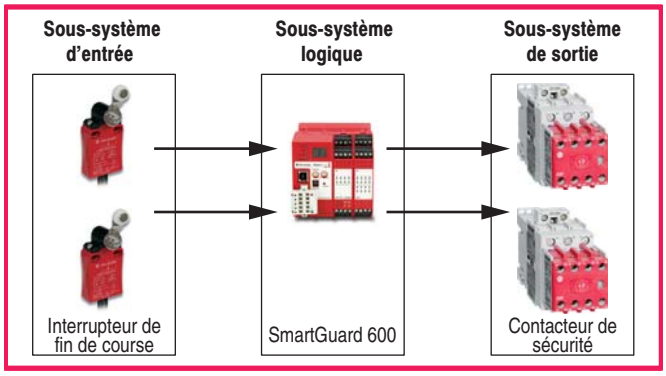


Figure 124 : deux voies avec interrupteur de sécurité, automate de sécurité et contacteur de sécurité

Le système de la figure 124 a clairement moins de chance de tomber en panne que celui de la figure 123, mais il est possible de le rendre encore plus fiable (pour ce qui est de sa fonction de sécurité) si nous incluons des mesures de diagnostic pour la détection des défauts. Evidemment, après avoir détecté le défaut, nous devons également réagir et mettre le système dans un état de sécurité. La figure 125 montre l'ajout de mesures de diagnostic obtenues grâce à des techniques de surveillance.

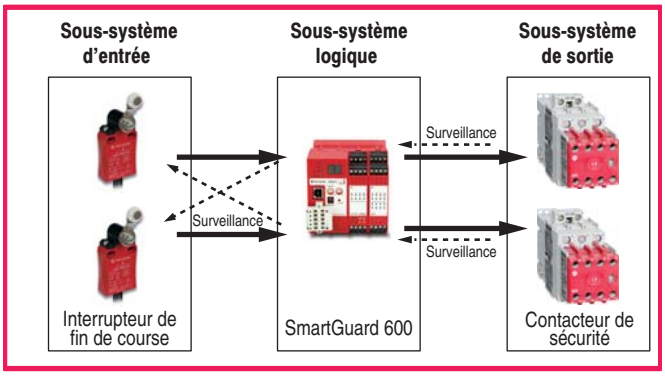


Figure 125 : système à double voie avec interrupteur de sécurité, automate de sécurité et contacteurs de sécurité – Diagnostics indiqués par les flèches en pointillé

Le système comprend généralement (mais pas toujours) deux voies dans tous ses sous-systèmes, comme illustré à la figure 125. Nous constatons que dans ce cas chaque sous-système possède deux "sous-voies." La norme les décrit comme des "blocs." Un sous-système à deux voies possède deux blocs et un sous-système à une voie possède un bloc. Il est possible que certains systèmes comprennent une combinaison de blocs à deux voies et à une voie.

Si nous voulons examiner le système plus en profondeur, nous devons étudier les composants de ces blocs. Le logiciel SISTEMA utilise le terme "éléments" pour ces composants. La figure 126 montre notre système avec la terminologie utilisée par SISTEMA.

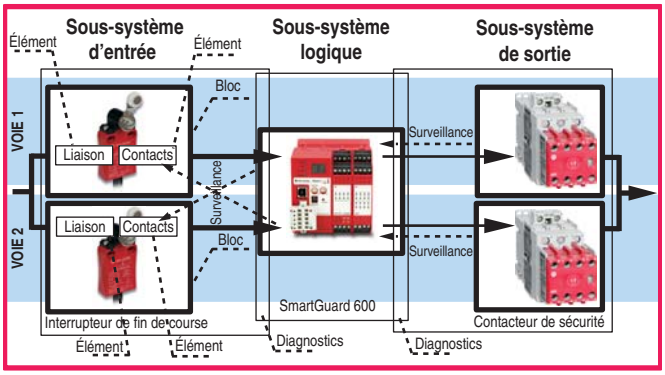


Figure 126 : système à deux voies illustré décomposé en sous-systèmes, blocs et éléments

Le sous-système des interrupteurs de fin de course est illustré décomposé selon ses éléments. Le sous-système du contacteur de sortie est décomposé selon ses blocs et le sous-système logique n'est pas décomposé. La fonction de surveillance des interrupteurs de fin de course et des contacteurs est exécutée dans l'automate. Les boîtes représentant les sous-systèmes de l'interrupteur de fin de course et du contacteur présentent un petit chevauchement avec la boîte du sous-système logique.

Ce principe de décomposition du système peut être reconnu dans la méthodologie définie dans la norme EN ISO 13849-1 et dans la structure système de base de SISTEMA. Cependant, il est important de noter qu'il existe des différences subtiles. La norme n'est pas restrictive dans sa méthodologie, mais pour la méthode simplifiée d'estimation du niveau PL, le première étape consiste en général à décomposer la structure du système en voies et en blocs dans chaque voie. Avec SISTEMA, le système est d'abord décomposé en sous-systèmes. La norme ne décrit pas de façon explicite un concept de sous-système, mais son utilisation comme décrite dans SISTEMA fournit une approche plus compréhensible et plus intuitive. Il n'y a bien sûr aucun effet sur le calcul final. SISTEMA et la norme utilisent des principes et des formules identiques. Il est intéressant de noter que l'approche par sous-système est également utilisée dans la norme EN/CEI 62061.

Le système que nous avons utilisé comme exemple n'est que l'un des cinq types d'archtitecture système de base définis par la norme. Toute personne connaissant le système des catégories reconnaîtra notre exemple comme étant représentatif de la catégorie 3 ou 4.

La norme utilise les catégories originales de la norme EN 954-1 pour ses cinq types d'architecture système. Elle les appelle des catégories d'architecture désignée (Designated Architecture Categories). Les exigences des catégories sont presque (mais pas exactement) identiques à celles de la norme EN 954-1. Les catégories d'architecture désignée sont représentées par les figures suivantes. Il est important de noter qu'elles peuvent être appliquées à un système entier ou à un sous-système. Les schémas ne doivent pas être considérés uniquement comme une strucutre physique. Ils sont à considérer plus comme une représentation graphique des exigences conceptuelles.

Un examen plus détaillé de la mise en œuvre pratique des catégories est abordé dans un chapitre ultérieur.

Figure 127 : Architecture désignée catégorie B

L'architecture désignée catégorie B doit utiliser des principes de sécurité de base (voir l'annexe de la norme EN ISO 13849-2). Le système ou le sous-système peut être défaillant en cas de défaut unique. Voir la norme EN ISO 13849-1 pour toutes les exigences.

Figure 128 : Architecture désignée catégorie 1

L'architecture désignée catégorie 1 a la même structure que la catégorie B et peut également être défaillante en cas de défaut unique. Mais, étant donné qu'elle doit également utiliser des principes de sécurité éprouvés (voir l'annexe de la norme EN ISO 13849-2), c'est moins probable que pour la catégorie B. Voir la norme EN ISO 13849-1 pour toutes les exigences.

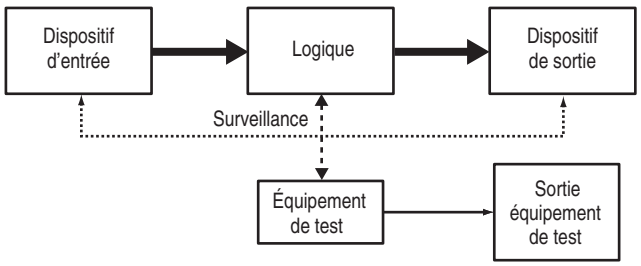


Figure 129 : Architecture désignée catégorie 2

L'architecture désignée catégorie 2 doit utiliser des principes de sécurité de base (voir l'annexe de la norme EN ISO 13849-2). Il doit également y avoir une surveillance de diagnostic via un test fonctionnel du système ou du sous-système. Le test doit être effectué au démarrage, puis périodiquement selon une fréquence équivalente à au moins cent tests pour chaque sollicitation de la fonction de sécurité. Il est à noter que cette fréquence de test constitue une exigence supplémentaires par rapport à celles définies par l'ancienne norme EN 954-1. Le système ou le sous-système peut tout de même tomber en panne si un seul défaut se produit entre les tests fonctionnels, mais cela a généralement moins de chance de se produire qu'avec la catégorie 1. Voir la norme EN ISO 13849-1 pour toutes les exigences.

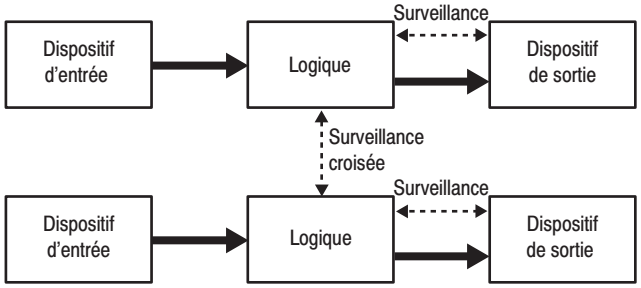


Figure 130 : Architecture désignée catégorie 3

L'architecture désignée catégorie 3 doit utiliser des principes de sécurité de base (voir l'annexe de la norme EN ISO 13849-2). Il existe également une exigence qui impose que le système/sous-système ne tombe pas en panne en cas de défaut unique. Cela signifie que le système doit tolérer un défaut unique pour sa fonction de sécurité. La façon la plus courante de satisfaire à cette exigence est d'utiliser une architecture à double voie comme illustré à la figure 130. De plus, un défaut unique doit être détecté, lorsque cela est possible. Cette exigence est identique à l'exigence originale de la catégorie 3 de la norme EN 954-1. Dans ce contexte, l'expression "lorsque c'est possible" s'est révèlée problématique. Elle signifiait que la catégorie 3 pouvait couvrir tout, d'un système redondant mais sans détection des défauts (souvent appelé de façon descriptive mais appropriée "redondance idiote") à un système redondant dans lequel tous les défauts uniques sont détectés. Cette question est abordée dans la norme EN ISO 13849-1 puisque celle-ci impose d'estimer la qualité du taux de couverture des tests de diagnostic (DC). En référence à l'annexe K ou au tableau 10. Nous voyons que plus la fiabilité [MTTFd] du système est élevée, plus le taux DC peut être faible. Cependant, DC doit être au moins de 60 % pour la catégorie 3 d'architecture.

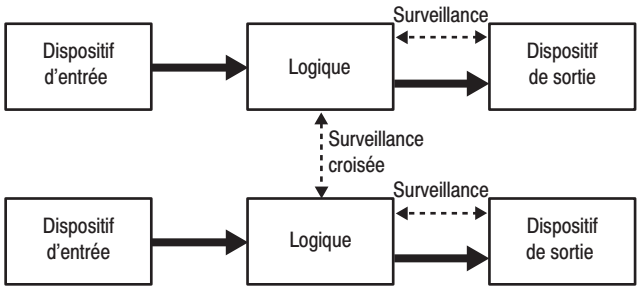


Figure 131 : Architecture désingée catégorie 4

L'architecture désignée catégorie 4 doit utiliser des principes de sécurité de base (voir l'annexe de la norme EN ISO 13849-2). Elle possède des exigences semblables à celles de la catégorie 3 mais impose une plus grande surveillance, c.-à-d. un taux de couverture des tests de diagnostic supérieur. Ceci est indiqué par les pointillés plus gras qui représentent les fonctions de surveillance. En clair, la différence entre les catégories 3 et 4 se résume au fait que pour la catégorie 3 la plupart des défauts doivent être détectés, alors que pour la catégorie 4 tous les défauts doivent l'être. Le taux de couverture des tests de diagnostic doit être au moins de 99 %. Même une accumulation de défauts ne doit pas provoquer une défaillance dangereuse.

Données de fiabilité

La norme EN ISO 13849-1 utilise des données de fiabilité quantitatives pour le calcul du niveau de performance PL obtenu par les composants de sécurité d'un système de commande. Cela représente une différence significative par rapport à la norme EN 954-1. La première question que cela soulève "où pouvons-nous obtenir ces données ?" Il est possible d'utiliser des données provenant de manuels de fiabilité reconnus, mais la norme indique clairement que la source privilégiée est le fabricant. Par conséquent, Rockwell Automation met les informations pertinentes à disposition sous la forme d'une bibliothèque de données pour SISTEMA. Ces données seront publiées sous d'autres formes en temps utile. Avant de poursuivre, nous devons examiner quels types de données sont nécessaires et également comprendre comment elles sont produites.

Le type de données par excellence requis par la norme (et par SISTEMA) pour déterminer le niveau de performance PL est PFH (probabilité de défaillance dangereuse par heure). Il s'agit des mêmes données que celles représentées par l'abréviation PFHd utilisée dans la norme CEI/EN 62061.

PL	Probabilité de défaillance dangereuse par heure moyenne (1/h)	SIL
a	$\geq 10^{-5}$ à $<10^{-4}$	Pas de correspondance
b	$\geq 3 \times 10^{-6}$ à $<10^{-5}$	1
c	$\geq 10^{-6}$ à $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ à $<10^{-6}$	2
e	$\geq 10^{-8}$ à $<10^{-7}$	3

Tableau 9

Le tableau 9 montre le rapport entre PFH et PL et SIL. Pour certains sous-systèmes, le PFH peut être disponible auprès du fabricant. Cela facilite les calculs. Le fabricant doit généralement effectuer des calculs relativement complexes et/ou des tests sur ses sous-systèmes afin de fournir cette information. Lorsque cette donnée n'est pas disponible, la norme EN ISO13849-1 fournit une alternative simplifiée basée sur le MTTFd moyen (durée moyenne de fonctionnement avant défaillance dangereuse) d'un système à une seule voie. Le niveau PL (et donc le PFH) d'un système ou sous-système peut ensuite être calculé à l'aide de la méthodologie et des formules de la norme. Cela peut même être réalisé plus facilement à l'aide de SISTEMA.

REMARQUE : il est important de comprendre que, pour un système à double voie (avec ou sans diagnostics), il n'est pas correct d'utiliser $1/PFH_D$ pour déterminer le MTTFd requis par la norme EN ISO 13849-1. La norme demande le MTTFd d'un système à une seule voie. C'est une valeur très différente du MTTFd de la combinaison des deux voies d'un sous-système à deux voies. Si le PFH_D d'un sous-système à deux voies est connu, il suffit de l'entrer directement dans SISTEMA.

MTTFd d'un système à seule voie

Cela représente le temps moyen avant l'apparition d'une défaillance qui peut conduire à la défaillance de la fonction de sécurité. Il est exprimé en années. Il s'agit d'une valeur moyenne des MTTFd des "blocs" d'un système à une seule voie et peut être appliquée à un système ou à un sous-système. La norme donne la formule suivante qui est utilisée pour calculer la moyenne de tous les MTTFd des éléments utilisés dans un système à une seule voie ou dans un sous-système.

A ce stade, la valeur ajoutée de SISTEMA devient évidente. Les utilisateurs n'ont pas à passer un temps précieux à consulter des tableaux et à calculer des formules puisque ces tâches sont réalisées par le logiciel. Les résultats finaux sont imprimés sous forme d'un rapport de plusieurs pages.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}}$$

Formule D1 de la norme EN ISO 13849-1

Dans la plupart des systèmes à double voie, les deux voies sont identiques ; par conséquent, le résultat de la formule représente l'une ou l'autre voie.

Si les voies du système/sous-système sont différentes, la norme fournit un formule pour traiter ce cas.

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

Formule 1 de la norme EN ISO 13849-1

De fait, cette formule fait la moyenne des deux moyennes. A des fins de simplification, il est également permis d'utiliser uniquement la valeur la plus défavorable pour la voie.

La norme regroupe le MTTFd en trois plages, comme suit :

Défiition du MTTFd de chaque voie	Plage du MTTFd de chaque voie
Faible	3 ans <= $MTTF_d$ < 10 ans
Moyen	10 ans <= $MTTF_d$ < 30 ans
Elevé	30 ans <= $MTTF_d$ < 100 ans

Tableau 10 : Niveaux du $MTTF_d$

Il est à noter que la norme EN ISO 13849-1 limite la possibilité d'utiliser le $MTTF_d$ de la voie unique d'un sous-système à un maximum de 100 ans, même si les valeurs réelles dérivées peuvent être bien supérieures.

Comme nous le verrons plus loin, la plage obtenue pour le MTTFd moyen est ensuite combinée avec la catégorie d'architecture désignée et le taux de couverture des tests de diagnostic (DC) afin de fournir un classement PL provisoire. Le terme provisoire est utilisé ici parce que d'autres exigences, notamment l'intégrité et des mesures systèmatiques des causes de défaillance communes, doivent toujours être satisfaites lorsque nécessaire.

Méthodes de détermination des données

Nous devons maintenant aller une étape plus loin pour aborder la façon dont les fabricants déterminent des données sous la forme PFH_D ou $MTTF_d$. Il est essentiel de comprendre cela pour utiliser les données des fabricants.

Les données peuvent être regroupées en deux types de base : 1) mécanistique (électro-mécanique, mécanique, pneumatique et hydraulique) et 2) électronique (à semi-conducteurs).

Il existe des différences fondamentales entre les mécanismes de défaillance communs de ces types de technologies. A la base, elles peuvent être résumées ainsi :

Technologie mécaniste : La défaillance est proportionnelle à la fiabilité inhérente et au taux d'utilisation. Plus le taux d'utilisation est élevé, plus un composant à de chance de se trouver dégradé et de tomber en panne. Il est à noter que ceci n'est pas la seule cause de défaillance, mais à moins de limiter le temps/cycles de fonctionnement, elle devient la cause prédominante. Il est évident qu'un contacteur qui a un cycle de commutation de une fois toutes les dix secondes fonctionnera de façon fiable bien moins longtemps qu'un contacteur identique qui fonctionne une fois par jour. Les dispositifs physiques incluent généralement des composants conçus individuellement pour une utilisation spécifique. Les composants sont forgés, moulés, coulés, usinés, etc. Ils sont combinés avec des couplages, des ressorts, des aimants, des bobines électriques, etc. afin de constituer un mécanisme. Etant donné que les composants constitutifs n'ont en général par d'historique d'utilisation dans d'autres applications, il n'est pas possible de trouver des données de fiabilité pré-exsitantes pour eux. L'estimation de PFH_D ou $MTTF_d$ pour le mécanisme est normalement basé sur des tests. Les deux normes EN/CEI 62061 et EN ISO 13849-1 mettent en avant un test appelé test B10d.

Dans le test B10d, un échantillon du dispositif (généralement au moins dix) est testé dans des conditions représentatives. Le nombre moyen de cycles de fonctionnement obtenu avant la défaillance de 10 % de l'échantillon et l'apparition de la situation dangereuse est connu comme la valeur B10d.

En pratique, il est fréquent que tous les échantillons tombent en panne en passant à un état de sécurité ; mais dans ce cas, la norme indique que la valeur B10d (danger) peut être prise comme deux fois la valeur B10 (sécurité).

Technologie électronique: Il n'existe aucune usure due à des pièces mobiles. Si l'on considère un environnement comparable aux caractéristiques électriques et de température (etc.) spécifiées, la défaillance prédominante d'un circuit électronique est proportionnelle à la fiabilité inhérente de ses composants (ou à leur manque de fiabilité). De nombreuses raisons peuvent être à l'origine de la défaillance des composants individuels : imperfection introduite pendant la fabrication, surtensions excessives, problèmes de connexion mécanique, etc. En général, les défauts des composants électroniques sont difficiles à prévoir par une analyse et ils semblent être de nature aléatoire. Par conséquent, le test d'un dispositif électronique en laboratoire ne révèle pas nécessairement les schémas typiques de défaillance à long terme.

Pour déterminer la fiabilité des dispositifs électroniques, il faut généralement utiliser l'analyse et le calcul. Il est possible de trouver des données correctes pour les composants individuels dans les manuels de données de fiabilité. Il est possible d'utiliser l'analyse pour déterminer quels modes de défaillance du composant sont dangereux. Il est permis et courant de faire la moyenne des modes de défaillance du composant comme étant à 50 % sécurisés et à 50 % dangereux. Cela donne généralement des données conservatrices.

La norme CEI 61508 fournit des formules pouvant être utilisées pour calculer la probabilité globale de défaillance dangereuse (PFH ou PFD) du dispositif ; c.-à-d. du sous-système. Les formules sont assez complexes et prennent en compte (le cas échéant) la fiabilité des composants, le potentiel de défaillance de cause commune (facteur beta), le taux de couverture des tests de diagnostic(DC), l'intervalle entre tests fonctionnels et l'intervalle entre tests de validation. La bonne nouvelle est que ces calculs complexes sont normalement réalisés par le fabricant du dispositif. Les deux normes EN/CEI 62061 et EN ISO 13849-1 acceptent un sous-système calculé de cette façon selon CEI 61508. Le PFH_D qui en résulte peut être utilisé directement dans l'annexe K de la norme EN ISO 13849-1 ou dans l'outil de calcul SISTEMA.

Logiciel : Les défaillances logicielles sont de nature systémique. Toute défaillance est due à la façon dont le logiciel est conçu, écrit et compilé. Par conséquent toute défaillance est due au système dans lequel il est produit, pas par son utilisation. Pour gérer les défaillances, il faut donc maîtriser ce système. Les deux normes CEI 61508 et EN ISO 13849-1 définissent des exigences et des méthodologies pour cela. Il n'est pas utile d'entrer dans les détails ici, sauf à dire qu'elles utilisent le modèle en V classique.

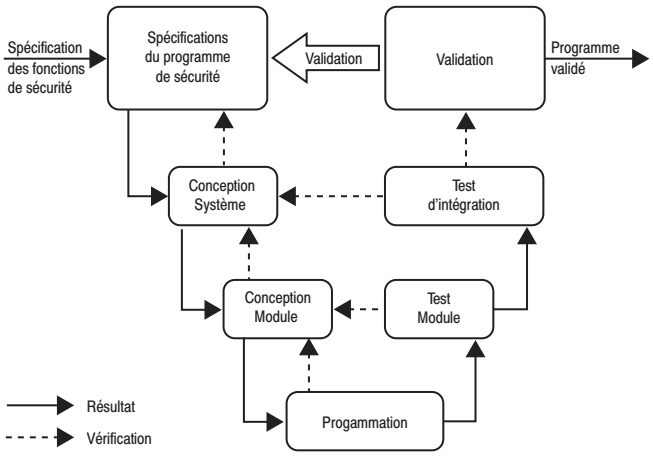


Figure 132 : modèle en V pour le développement de logiciel

Le logiciel intégré est un enjeux pour le concepteur du dispositif. L'approche habituelle consiste à développer le logiciel intégré en accord avec les méthodes formelles expliquées dans la norme CEI 61508, partie 3. En ce qui concerne le code d'application, c.-à-d. le logiciel avec lequel l'utilisateur dialogue, la plupart des dispositifs de sécurité programmables sont fournis avec des blocs fonctionnels ou des sous-programmes "certifiés". Cela simplifie la tâche de validation du code d'application mais il ne faut pas oublier que le programme d'application terminé doit toujours être validé. La façon dont les blocs sont reliés et paramétrés doit être vérifiée et validée pour s'assurer qu'elle est correcte pour la tâche prévue. Les deux normes EN ISO 13849-1 et CEI/EN 62061 fournissent des recommandations pour ce processus.

Taux de couverture de diagnostic (DC)

Nous avons déjà abordé ce sujet lorsque nous avons traité des catégories d'architecture désignée 2, 3 et 4. Ces catégories nécessitent des tests de diagnostic pour vérifier si la fonction de sécurité fonctionne toujours. L'expression "taux de couverture des tests de diagnostic" (généralement abrégé en DC) est utilisé pour caractériser l'efficacité des tests. Il est important de réaliser que DC n'est pas basé uniquement sur le nombre de composants pouvant présenter une défaillance dangereuse. Il prend en compte le taux total de défaillance dangereuse. Le symbole l (lambda) est utilisé pour ce "taux de défaillance". DC exprime la relation entre les taux d'apparition des deux types suivants de défaillance dangereuse :

- Défaillance détectée dangereuse (ldd) : Défaillances qui provoquent, ou peuvent conduire à, une perte de la fonction de sécurité, mais qui sont détectées. Après la détection, une fonction de réaction au défaut entraîne le passage du dispositif ou du système à un état de sécurité.
- Défaillance dangereuse [ld] : Toutes les défaillances qui peuvent potentiellement provoquer, ou conduire à, une perte de la fonction de sécurité. Elles incluent les défaillances qui sont détectées et celles qui ne le sont pas. Evidemment, les défaillances qui sont réellement dangereuses sont les défaillances dangereuses non détectées (appelées ldu).

DC est exprimé par la formule :

DC = ldd/ld exprimé en pourcentage.

Cela signifie que le terme DC est commun aux normes EN ISO 13849-1 et EN/CEI 62061. Cependant, la façon dont il est obtenu diffère. La deuxième norme propose d'utiliser des calculs basés sur l'analyse du mode de défaillance, alors que la norme EN ISO 13849-1 fournit une méthode simplifiée sous forme de tableaux de référence. Divers techniques de diagnostic typiques sont indiquées avec le pourcentage DC qu'elles ont pour objectif d'atteindre. Dans certains cas, un jugement rationnel est tout de même requis ; dans certaines techniques par exemple le taux de couverture des tests de diagnostic (DC) obtenu est proportionnel à la fréquence à laquelle le test est effectué. Cette approche est parfois considérée comme trop vague. Cependant, l'estimation de DC peut dépendre de nombreuses variables et quelle que soit la technique utilisée, le résultat ne peut généralement être qualifié que d'approximatif. Il est également important de comprendre que les tableaux de la norme EN ISO 13849-1 sont basés sur des recherches complètes effectuées par le BGIA sur les résultats obtenus par des techniques de diagnostic connues sur des applications réelles. Dans l'intérêt de la simplification, la norme divise DC en quatre plages de base :

<60 % = aucun

60 % à <90 % = faible

90 % à <99 % = moyen

+99 % = élevé

Cette approche par plages plutôt que par valeurs individuelles de pourcentage peut également être considérée comme plus réaliste en terme de fiabilité pouvant être atteinte. L'outil SISTEMA utilise les mêmes tableaux de référence que la norme. Avec l'augmentation de l'utilisation de composants électroniques complexes dans les dispositifs de sécurité, DC devient un facteur important. Il est probable que les révisions futures des normes clarifieront cette question. En attendant, une approche technique censée et du bon sens devraient être suffisant pour prendre la bonne décision quant à la plage DC.

Défaillance de cause commune

Dans la plupart des systèmes ou sous-systèmes à double voie (c.-à-d. tolérant un seul défaut), le principe de diagnostic est basé sur le postulat qu'il n'y aura pas de défaillances dangereuses sur les deux voies en même temps. L'expression « en même temps » est plus exact si elle est exprimée ainsi : « dans l'intervalle entre tests de diagnostic ». Si cet intervalle entre tests de diagnostic est suffisamment court (p. ex., inférieur à huit heures), il est raisonnable de supposer que deux défauts distincts et non liés ont peu de chance de se produire dans ce laps de temps. Cependant, la norme est claire sur le fait qu'il faut bien réfléchir au fait que les possibilités d'apparition de défaut sont distinctes et non liées. Par exemple, s'il est prévisible qu'un défaut sur un composant peut conduire à la défaillance d'autres composants, le total des défauts qui en résulte est considéré comme une seule défaillance.

Il est également possible qu'un événement qui entraîne la défaillance d'un composant puisse aussi provoquer la défaillance d'autres composants. Cela s'appelle « défaillance de cause commune » (CCF). La propension pour l'apparition de CCF est normalement décrite comme le facteur beta (ß). Il est très important que les concepteurs du sous-système et du système soient conscient des possibilités d'apparition de CCF. Il existe de nombreux types de CCF et, par conséquent, de nombreuses façons de les éviter. La norme EN ISO 13849-1 définit un chemin rationnel entre les extrêmes de complexité et de trop grande simplification. Comme la norme EN/CEI 62061, elle adopte une approche essentiellement qualitative. Elle fournit une liste de mesures connues pour être efficaces dans l'évitement de CCF.

Le tableau 11 présente un résumé du processus de notation.

N°	Mesure contre la CCF	Note
1	Séparation/distinction	15
2	Diversité	20
3	Conception/Application/ Expérience	20
4	Evaluation/Analyse	5
5	Compétence/Formation	5
6	Environnement	35

Tableau 11 : notation pour la défaillance de cause commune

Un nombre suffisant de ces mesures doit être mis en œuvre dans la conception d'un système ou sous-système. Il pourrait, dans une certaine mesure, être justifié de dire que la seule utilisation de cette liste n'est peut-être pas suffisante pour empêcher toute possibilité d'apparition de CCF. Cependant, si l'objectif de la liste est correctement pris en compte, il devient évident que l'esprit de ses exigences est d'inciter le concepteur à analyser les possibilités d'apparition de CCF et à mettre en œuvre les mesures d'évitement appropriées en fonction de la technologie et des caractéristiques de l'application prévue. L'utilisation de la liste renforce la prise en compte de certaines techniques fondamentales et efficaces, comme la diversité des modes de défaillance et les compétences de conception. L'outil SISTEMA de BGIA requiert également la mise en œuvre des tableaux de référence de CCF de la norme et il les met à disposition sous une forme pratique à utiliser.

Temps de mission

Le temps de mission représente le laps de temps maximum pendant lequel un sous-système, ou un système, peut être utilisé. Après ce laps de temps, il doit être remplacé. Le temps de mission doit être déclaré par le fabricant des composants. Ce temps de mission est généralement identique à l'« intervalle entres tests de validation » ou la « durée de vie » (selon la durée la plus courte) utilisé dans la norme CEI/EN62061. Le concepteur du système de sécurité doit donc prendre en compte le temps de mission des composants afin de déterminer le temps de mission de chaque fonction de sécurité. Pour les composants mécaniques, la valeur T10d indique cette durée de vie utilie en terme de nombre d'opérations. La valeur T10d est dérivée du calcul de B10d.

Défaus systémiques

Nous avons déjà abordé les données de fiabilité de sécurité quantifiées sous la forme du MTTFd et de la probabilité de défaillance dangereuse. Cependant, les choses ne se résument pas à cela. Lorsque nous avons fait référence à ces termes, nous pensions réellement aux défaillances qui semblent de nature aléatoire. En effet, la norme CEI/EN 62061 fait spécialement référence à l'abréviation PFH_D comme étant la probabilité de défaillance matérielle aléatoire. Mais il existe des types de défaillances collectivement appelées « défaillances systémiques » qui peuvent être attribuées aux erreurs commises lors de la conception ou du processus de fabrication. L'exemple classique de cela est une erreur dans le code du logiciel. Dans son annexe G, la norme définit des mesures destinées à éviter ces erreurs (et donc les défaillances). Ces mesures incluent des dispositions telles que l'utilisation de matériaux et de techniques de fabrication adaptés, l'examen, l'analyse et la simultation sur ordinateur. Il existe également des événements prévisibles et des caractéristiques pouvant apparaître dans l'environnement d'utilisation qui peuvent provoquer une défaillance si leurs effets ne sont pas maîtrisés. L'annexe G fournit également des mesures pour cela. Par exemple, il est facile de prévoir qu'il pourrait y avoir des pertes occasionnelles d'alimentation. Par conséquent, la mise hors tension des composants doit entraîner un état de sécurité pour le système. Ces mesures peuvent sembler ne relever que du bon sens, et c'est le cas, mais elles n'en sont pas moins essentielles. Toutes les autres exigences de la norme sont sans signification si l'on ne prend pas correctement en compte le contrôle et l'évitement des défaillances systémiques. Cela requiert également parfois les mêmes types de mesures que ceux utilisés pour le contrôle des défaillances matérielles aléatoires (pour atteindre le niveau PFH_D requis), comme les tests de diagnostic automatiques et l'utilisation de matériel redondant.

Exclusion de défaut

Un des principaux outils d'analyse pour les systèmes de sécurité est l'analyse des défaillances. Le concepteur et l'utilisateur doivent comprendre comment le système de sécurité se comporte en présence de défauts. De nombreuses techniques sont disponibles pour effectuer l'analyse. Par exemple, analyse d'arborescence des défauts ; analyse critique des modes et des effets des défaillances ; analyse d'arborescence des événements ; et examen de la force de charge.

Au cours de l'analyse, il est possible de découvrir certains défauts qui ne peuvent pas être détectés par les tests de diagnostic automatiques sans entraîner des coûts économiques exagérés. De plus, la probabilité que ces défauts puissent se produire peut être rendue très faible par l'utilisation de méthodes de limitation lors de la conception, de la construction et des tests. Dans ces conditions, les défauts n'ont plus besoin d'être pris en compte. L'exclusion des défauts est le fait d'écarter l'apparition d'une défaillance parce que la probabilité d'apparition de cette défaillance spécifique du SRCS est négligeable.

La norme ISO13849-1:2006 autorise l'exclusion des défauts sur la base de l'improbabilité d'apparition, de l'expérience technique généralement acceptée et des exigences techniques liées à l'application. La norme ISO13849-2:2003 fournit des exemples et des justifications pour l'exclusion de certains défauts des systèmes électriques, pneumatiques, hydrauliques et mécaniques. Les exclusions de défauts doivent être déclarées avec des justifications détaillées dans la documentation technique.

Il n'est pas toujours possible d'évaluer un système de commande de sécurité sans supposer que certains défauts peuvent être exclus. Pour plus de détails sur les exclusions de défauts, voir la norme ISO 13849-2.

Lorsque le niveau de risque est plus élevé, la justification de l'exclusion d'un défaut devient plus stricte. En général, lorsqu'un niveau de performance PLe est requis pour qu'une fonction de sécurité soit mise en œuvre par un système de commande de sécurité, il n'est pas normal de s'appuyer uniquement sur les exclusions de défauts afin d'atteindre ce niveau de performance. Cela dépend de la technologie utilisée et de l'environnement d'utilisation prévu. Il est donc essentiel que le concepteur prenne des précautions supplémentaires pour utiliser les exclusions de défauts lorsque les exigences de ce niveau de performance PL augmentent.

Par exemple, un système de verrouillage de porte qui doit atteindre un niveau PLe doit incorporer une tolérance aux pannes minimum de 1 (p. ex., deux détecteurs de position mécaniques conventionnels) pour atteindre ce niveau de performance puisqu'il n'est normalement pas justifié d'exclure les défauts ; comme par exemple des actionneurs cassés. Cependant, il peut être acceptable d'exclure les défauts, comme un court-circuit du câblage dans un panneau de commande conçu en conformité avec les normes appropriées.

Niveau de performance (Performance Level - PL)

Le niveau de performance est un niveau discret qui définit la capacité des composants de sécurité du système de commande à exécuter la fonction de sécurité.

Pour évaluer le niveau de performance PL atteint par la mise en œuvre d'une des cinq architectures désignées, 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 (taux de couverture des tests de diagnostic)
- Architecture (la catégorie)

Le tableau 12 montre le niveau PL obtenu pour diverses combinaisons. Voir l'annexe K de la norme pour plus de précisions.

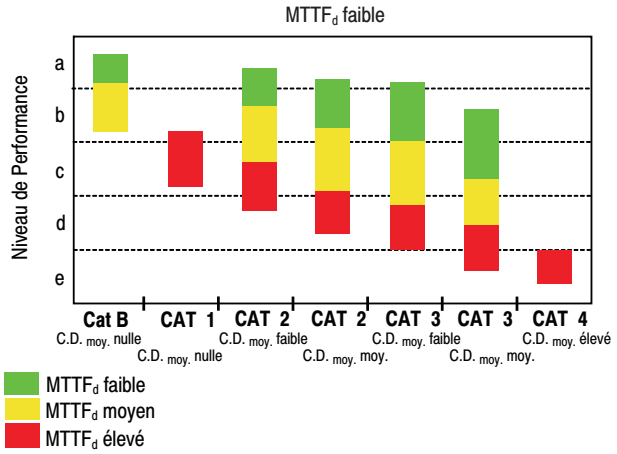


Figure 133 : détermination graphique du niveau de performance PL

Le tableau 12 montre le niveau PL obtenu pour diverses combinaisons. Voir l'annexe K de la norme pour plus de précisions.Par exemple, une application utilise l'architecture désignée catégorie 3. Si DC est compris entre 60 % et 90 %, et si le MTTFd de chaque voie est compris entre 10 et 30 ans, alors selon la figure 133, un niveau PL_d est obtenu.

D'autres facteurs sont également à prendre en considération pour atteindre le niveau PL requis. Ces exigences incluent les dispositions déjà abordées, comme pour les défaillances de cause commune, la défaillance systémique et le temps de mission.

Si le PFH_D du système ou du sous-système est connu, le tableau 12 (annexe K de la norme) peut être utilisé pour déduire le niveau PL.

$MTTF_d$ pour chaque voie	Probabilité de défaillance dangereuse par heure moyenne (1/h) et niveau de performance (PL) correspondant																	
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL				
Années	DC_{moy} = aucun		DC_{moy} = aucun		DC_{moy} = faible		DC_{moy} = moyen		DC_{moy} = faible		DC_{moy} = moyen		DC_{moy} = élevé					
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	$9,51 \times 10^{-6}$	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	$8,78 \times 10^{-6}$	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						
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				

Tableau 12 : $MTTF_d$ précis pour déterminer PL

La source du tableau 12 est le tableau K.1 de la norme ISO/EN 13849-1:2006

Visitez notre site : www.ab.com/catalogs
Publication S117-CA001A-FR-P

Conception et combinaisons de sous-systèmes

Si les niveaux PL de tout le sous-système sont connus, ils peuvent être combinés assez simplement dans un système à l'aide du tableau 13. La logique qui sous-tend ce tableau est claire. Tout d'abord, la qualité du système est définie par son élément (sous-système) le plus faible. Deuxièmement, plus il y a de sous-systèmes, plus il y a de risque de défaillance.

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

Tableau 13 : calcul PL pour sous-systèmes combinés en série

Dans le système illustré à la figure 135, les niveaux de performances les plus faibles sont pour les sous-systèmes 1 et 2. Les deux sont classés PLb. Par conséquent, en utilisant le tableau 13, nous constatons en lisant la ligne b (dans la colonne PLlow), puis la ligne 2 (dans la colonne Nlow), que le niveau PL du système est b (dans la colonne PL). Si les trois sous-systèmes étaient PLb, le niveu PL obtenu serait PLa.

Remarque : l'utilisation du tableau n'est pas obligatoire. La prérérence est donnée à l'utilisation de l'annexe K de la norme (ou de SISTEMA). Ce tableau est destiné uniquement à fournir une approche simple pour les petits systèmes.

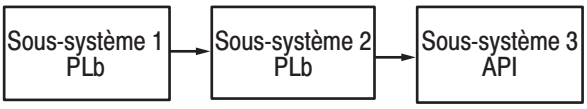


Figure 134 : combinaison de sous-systèmes en série comme un seul système PLb

Validation

La validation joue un rôle important tout au long du processus de développement et de mise en service du système de sécurité. La norme ISO/EN 13849-2:2003 définit les exigences pour la validation. Elle impose un plan de validation et aborde la validation par des techniques de test et d'analyse, comme l'analyse d'arborescence des défauts ou l'analyse critique des modes et des effets des défaillances. La plupart de ces exigences concernent le fabricant du sous-système plutôt que l'utilisateur du sous-système.

Mise en service de machine

A l'étape de la mise en service du système ou de la machine, la validation des fonctions de sécurité doit être effectuée pour chaque mode 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 au fonctionnement réel et aux caractéristiques de l'environnement. Certaines de ces caractéristiques peuvent être différentes des caractéristiques envisagées lors de la conception.

Conception de système selon CEI/EN 62061

CEI/EN 62061, « Sécurité des machines : Sécurité fonctionnelle des systèmes de commande électrique, électronique et électronique programmable », est l'implémentation spécifiques aux machines de la norme CEI/EN 61508. Elle définit des exigences relatives à la conception des systèmes de commande électrique de sécurité des machines et de sous-systèmes et dispositifs non complexes.

L'évaluation des risques permet de définir une stratégie pour la réduction des risques, qui elle-même permet d'identifier les besoins relatifs aux fonctions de commande de sécurité. Ces fonctions doivent être documentées et inclurent :

- les caractéristiques des exigences fonctionnelles ;
- les caractéristiques des exigences relatives à l'intégrité de la sécurité.

Les exigences fonctionnelles incluent des informations comme la fréquence d'opération, le temps de réponse requis, les modes de fonctionnement, les cycles de service, l'environnement d'utilisation et les fonctions de réponse aux défauts. Les exigences relatives à l'intégrité de la sécurité sont exprimées par des niveaux appelés niveaux d'intégrité de la sécurité (Safety Integrity Level - SIL). Selon la complexité du système, certains ou tous les éléments du tableau 14 doivent être pris en compte pour déterminer si la conception du système est conforme au niveau SIL requis.

Elément à prendre en compte pour SIL	Symbole
Probabilité de défaillance dangereuse par heure	PFH_D
Tolérance aux pannes matérielles	Pas de symbole
Proportion de défaillances non dangereuses	SFF
Intervalle de test de vérification	T_1
Intervalle entre tests de diagnostic	T_2
Sensibilité aux défaillances de cause commune	ß
Taux de couverture de diagnostic	DC

Tableau 14 : éléments à prendre en compte pour SIL

Sous-systèmes

Le terme « sous-système »a une signification spéciale dans la norme CEI/EN 62061. C'est le premier niveau de division d'un système selon des parties qui, si elles tombent en panne, entraînent une défaillance de la fonction de sécurité. Par conséquent, si deux interrupteurs redondants sont utilisés dans un système, aucun de ces interrupteurs ne constitue un sous-système. Le sous-système inclut les deux interrupteurs et toute fonction de test de diagnostic associée.

Probabilité de défaillance dangereuse par heure (PFH_D)

La norme CEI/EN 62061 utilise les mêmes méthodes de base que celles présentées dans la section sur la norme EN ISO 13849-1 afin de déterminer les taux de défaillance au niveau des composants. Les mêmes dispositions et méthodes concernent les composants « mécaniques » et électroniques. Dans la norme CEI/EN 62061 il n'y a aucune référence à un MTTFd en années. Le taux de défaillance par heure (λ) est soit calculé directement, soit obtenu ou dérivé de la valeur B10 dans la formule suivante :

λ = 0,1 x C/B10 (où C = le nombre de cycles d'opérations par heure)

Il existe une différence significative de méthodologie entre les normes pour déterminer le PFH_D total d'un sous-système ou d'un système. Une analyse des composants doit être entrepise pour déterminer la probabilité de défaillance des sous-systèmes. Des formules simplifiées sont fournies pour le calcul des architectures de sous-système communes (décrites plus loin). Lorsque ces formules ne sont pas adaptées, il est nécessaire d'utiliser des méthodes de calcul plus complexes, comme les modèles Markov. Les probabilités de défaillance dangereuse (PFH_D) de chaque sous-système sont alors additionnées pour déterminer le PFH_D total du système. Le tableau 15 (tableau 3 de la norme) peut alors être utilisé pour déterminer quel niveau d'intégrité de la sécurité (SIL) est adapté pour cette plage de PFH_D.

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

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

Les formules pour cette architecture prennent en considération l'agencement parallèle des éléments du sous-système et ajoute les deux éléments suivants provenant du tableau 14 :

ß (Beta) est la sensibilité aux défaillances de cause commune.

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

Tableau 15 : probabilités de défaillance dangereuse en fonction des niveaux SIL

Les données PFH_D d'un sous-système sont généralement fournies par le fabricant. Les données pour les composants et systèmes de sécurité de Rockwell Automation sont disponibles sous différentes formes, notamment sur :
http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx

Ce site Internet est mis à jour régulièrement à mesure que de nouvelles données pour d'autres composants et systèmes Rockwell Automation deviennent disponibles.

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

Pour les dispositifs électromécaniques de faible complexité, le mécanisme de défaillance est généralement lié au nombre et à la fréquence des opérations plutôt que simplement à la durée. Par conséquent, pour ces composants les données sont obtenues à partir de tests (p. ex., le test B10 décrit dans le chapitre sur la norme EN ISO 13849-1). Les informations d'application comme le nombre d'opérations prévu par an sont alors requises pour convertir B10d, ou des données similaires, en PFH_D.

REMARQUE : en général, ce qui suit est vrai (en prenant en compte un facteur pour changer les années en heures) :

$PFH_D = 1/MTTFd$

Cependant, il est important de comprendre que, pour un système à double voie (avec ou sans diagnostics), il n'est pas correct d'utiliser 1/ PFH_D pour déterminer le MTTFd requis par la norme EN ISO 13849-1. Cette norme demande le MTTFd d'un système à une seule voie. C'est une valeur très différente du MTTFd de la combinaison des deux voies d'un sous-système à deux voies.

Contraintes architecturales

La caractéristiques essentielle de la norme CEI/EN 62061 est que le système de sécurité est divisé en sous-systèmes. Le niveau d'intégrité de la sécurité matérielle pouvant être revendiqué par un sous-système est limité non seulement par le PFH_D, mais également par la tolérance aux pannes matérielles et la proportion de défaillances non dangereuses des sous-systèmes. La tolérance aux pannes matérielles est la capacité du système à exécuter sa fonction en présence de pannes. Une tolérance aux pannes de zéro signifie que la fonction n'est pas exécutée lorsqu'une seule panne se produit. Une tolérance aux pannes de un permet au sous-système d'exécuter sa fonction en présence d'une seule panne. La proportion de défaillance non dangereuse est la partie du taux de défaillance global qui n'entraîne pas une défaillance dangereuse. La combinaison de ces deux éléments est connue comme la contrainte architecturale et son résultat est la limite de déclaration SIL (SIL CL). Le tableau 16 montre le rapport entre contraintes architecturales et SILCL. Un sous-système (et donc son système) doit être conforme aux exigences PFH_D et aux contraintes architecturales, ainsi qu'aux dispositions pertinentes de la norme.

Proportion de défaillances non dangereuses (SFF)	Tolérance aux pannes matérielles		
	0	1	2
<60 %	Non autorisé, sauf en cas d'exceptions spécifiques	SIL1	SIL2
60 %…<90 %	SIL1	SIL2	SIL3
90 %…<99 %	SIL2	SIL3	SIL3
≥99 %	SIL3	SIL3	SIL3

Tableau 16 : contraintes architecturales selon les niveaux SIL

Par exemple, une architecture de sous-système qui possède une tolérance à une seule panne et une proportion de défaillances non dangereuses de 75 % est limitée à un niveau maximal SIL2, quelle que soit la probabilité de défaillance dangereuse.

Lorsque des sous-systèmes sont combinés, le niveau SIL atteint par le système SRCS est limité à un niveau inférieur ou égal au niveau SIL CL le plus bas de n'importe quel sous-systèmes impliqués dans la fonction de commande de sécurité.

Constitution du système

Pour calculer la probabilité de défaillance dangereuse, chaque fonction de sécurité doit être divisée en blocs fonctionnels, qui sont ensuite constitués en sous-systèmes. La mise en œuvre d'un système typique avec fonction de sécurité inclut un dispositif de détection raccordé à un dispositif logique lui-même raccordé à un actionneur. Cela crée un agencement de sous-systèmes en série. Comme nous l'avons déjà vu, si nous pouvons déterminer la probabilité de défaillance dangereuse de chaque sous-système et connaître son niveau SIL CL, alors la probabilité de défaillance du système est facile à calculer en additionnant les probabiités de défaillance des sous-systèmes. Ce concept est illustré à la figure 136.

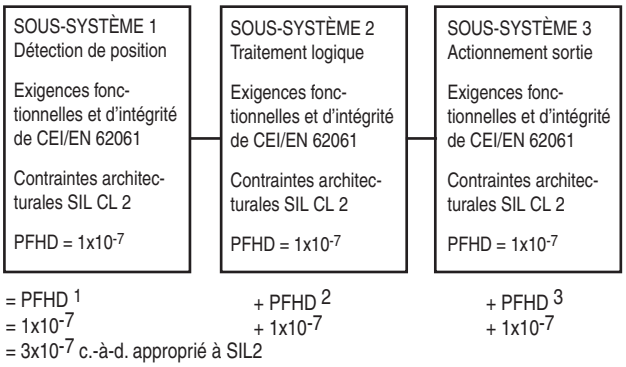


Figure 135 : exemple de combinaison de sous-systèmes

Si, par exemple, nous voulons obtenir un niveau SIL 2, chaque sous-système doit avoir un niveau SIL CL d'au moins SIL 2, et la somme du PFH_D du système ne doit pas dépasser la limite autorisée dans le tableau 15.

Conception du sous-système : CEI/EN 62061

Si un concepteur de système utilise des composants déjà « conditionnés » en sous-systèmes comme défini dans la norme CEI/EN 62061, les choses sont bien plus faciles puisque les exigences spécifiques à la conception des sous-systèmes ne s'appliquent pas. Ces exigences sont, en général, prise 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 automates de sécurité soient conformes à la norme CEI 61508 ou aux normes appropriées. Cela signifie que, pour les dispositifs qui utilisent des composants électroniques programmables complexes, toute la rigueur de la norme CEI 61508 s'applique. Ce processus peut s'avérer très rigoureux et demander un grande implication. Par exemple, l'évaluation de la PFH_D atteinte par un sous-système complexe peut être un processus très complexe qui a recours à des techniques comme la modélisation Markov, les schémas fonctionnels de fiabilité ou l'analyse d'arborescence des défauts.

La norme CEI/EN 62061 définit des exigences pour la conception de sous-systèmes de faible complexité. Ceux-ci incluent généralement les composants électriques relativement simples comme les interrupteurs de sécurité et les relais de surveillance électromécaniques. Ces exigences ne demandent pas une implication aussi forte que celles de la norme CEI 61508 mais peuvent tout de même être assez complexes.

La norme CEI/EN 62061 fournit quatre architectures logiques de sous-système avec les formules connexes pouvant être utilisées pour évaluer la PFH_D atteinte par un sous-système de faible complexité. Ces archtitectures sont des représentations purement logiques et ne doivent pas être considérées comme des architectures physiques. Les quatre architectures logiques de sous-système avec les formules connexes sont illustrées par les figures 136 à 139.

Pour une architecture de sous-système de base illustré à la figure 136, les probabilités de défaillance dangereuse sont simplement additionnées.

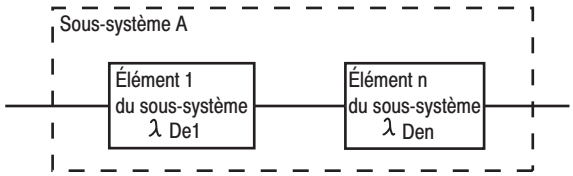


Figure 136 : archtitecture logique de sous-système A

$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$

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

Le symbole λ (lambda) est utilisé pour le taux de défaillance. Les unités du taux de défaillance sont les défaillances par heure. λD est le taux de défaillance dangereuse. λDssA est le taux de défaillance dangereuse du sous-système A. C'est la somme des taux de défaillance des éléments individuels, e1, e2, e3, jusqu'à et y compris en. La probabilité de défaillance dangereuse est multipliée par 1 heure pour créer la probabilité de défaillance en une heure.

La figure 137 montre un système avec une tolérance à une seule panne sans fonction de diagnostic. Lorsque l'architecture inclut une tolérance à une seule panne, le potentiel de défaillance de cause commune existe et doit être pris en compte. Ce qui découle de la défaillance de cause commune est brièvement décrit plus loin dans cette section.

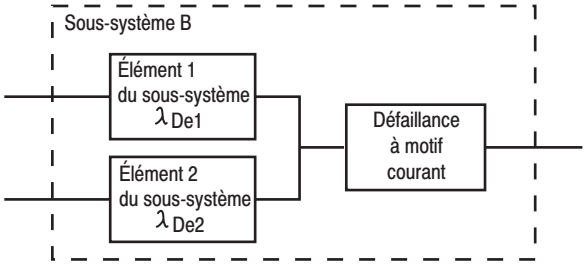


Figure 137 : archtitecture logique de sous-système B

$\lambda_{DssB} = (1-ß)2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ßx (\lambda_{De1} + \lambda_{De2}) / 2$

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

Les formules pour cette architecture prennent en considération l'agencement parallèle des éléments du sous-système et ajoute les deux éléments suivants provenant du tableau 14 :

ß (Beta) est la sensibilité aux défaillances de cause commune.

T1 est la valeur la plus faible entre l'intervalle entre tests de validation et la durée de vie. Le test de validité est prévu pour détecter les défauts et la dégradation du sous-système de sécurité pour que le fonctionnement normal du sous-système puisse être restauré. En termes pratiques, cela signifie généralement le remplacement (comme le terme équivalent « temps de mission » dans la norme EN ISO 13849-1).

La figure 139 donne une représentation fonctionnelle d'un système ne tolérant aucune panne avec une fonction de diagnostic. Le taux de couverture des tests de diagnostic est utilisé pour diminuer la probabilité de défaillance matérielle dangereuse. Les tests de diagnostic sont exécutés automatiquement. La définition du taux de couverture des tests de diagnostic est la même que celle donnée dans la norme EN ISO 13849-1 ; c.-à-d., le rapport entre le taux de défaillances dangereuses détectées et le taux de toutes les défaillances dangereuses.

Ces formules incluent le taux de couverture des tests de diagnostic (DC) pour chacun des éléments du sous-système. Les taux de défaillance de chacun des sous-systèmes sont réduits du taux de couverture des tests de diagnostic de chaque sous-système.

Le quatrième exemple d'architecture de sous-système est donné à la figure 139. Ce sous-système tolère une seule panne et inclut une fonction de diagnostic. Le potentiel de défaillance de cause commune doit également être pris en considération pour les systèmes tolérant une seule panne.

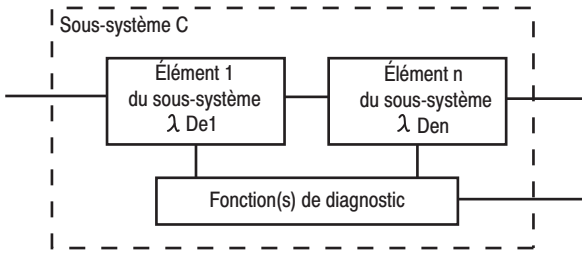


Figure 138 : archtitecture logique de sous-système C

La figure 138 donne une représentation fonctionnelle d'un système ne tolérant aucune panne avec une fonction de diagnostic. Le taux de couverture des tests de diagnostic est utilisé pour diminuer la probabilité de défaillance matérielle dangereuse. Les tests de diagnostic sont exécutés automatiquement. La définition du taux de couverture des tests de diagnostic est la même que celle donnée dans la norme EN ISO 13849-1 ; c.-à-d., le rapport entre le taux de défaillances dangereuses détectées et le taux de toutes les défaillances dangereuses.

Ces formules incluent le taux de couverture des tests de diagnostic (DC) pour chacun des éléments du sous-système. Les taux de défaillance de chacun des sous-systèmes sont réduits du taux de couverture des tests de diagnostic de chaque sous-système.

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

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

Le quatrième exemple d'architecture de sous-système est donné à la figure 139. Ce sous-système tolère une seule panne et inclut une fonction de diagnostic. Le potentiel de défaillance de cause commune doit également être pris en considération pour les systèmes tolérant une seule panne.

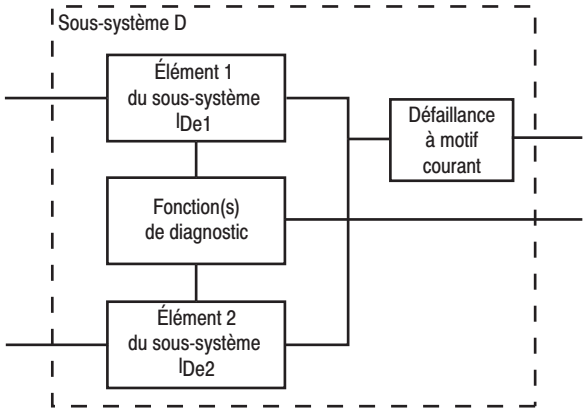


Figure 139 : archtitecture logique de sous-système D

Si les éléments du sous-système sont différents sur chaque voie, la formule suivante est utilisée :

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

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

Si les éléments du sous-système sont identiques sur chaque voie, la formule suivante est utilisée :

$\lambda_{DssD} = (1 - \beta)^2 \{ [\lambda_{De2} \times 2 \times DC] \times T_2 / 2 + [\lambda_{De2} \times \lambda_{De2} \times (1-DC)] \times T_1 \} + \beta \times (\lambda_{De}$

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

Remarquez que les deux formules utilisent un paramètre supplémentaire, **T2**, l'intervalle entre tests de diagnostic. Ceci est simplement une vérification périodique de la fonction. Il s'agit d'un test moins complet que le test de validité.

Prenez par exemple les valeurs suivantes pour l'exemple dans lequel les éléments du sous-système sont différents :

$\beta = 0,05$ — $T2 = 2$ heures
$\lambda_{De} = 1 \times 10^{-6}$ défaillances/heure — DC = 90 %
T1 = 87600 heures (10 ans)

PFH_{DssD} = 5,791E-08 défaillances dangereuses par heure. Ceci se trouve dans la plage requise pour SIL 3.

Effets de l'intervalle entre tests de validation

La norme CEI/EN 62061 indique qu'un intervalle entre tests de validation (Proof Test Interval - PTI) de 20 ans est préférable (mais pas obligatoire). Etudions l'effet de l'intervalle entre tests de validation sur le système. Si nous recaculons la formule avec T1 à 20 ans, cela donne PFH_{DssD} = 6,581E-08. Ce résultat se trouve toujours dans la plage requise pour SIL 3.Le concepteur doit garder à l'esprit que ce sous-système doit être combiné à d'autres sous-systèmes pour calculer le taux de défaillance dangereuse global.

Effet de l'analyse de défaillance de cause commune

Etudions l'effet des défaillances de cause commune sur le système. Supposons que nous prenions des mesures supplémentaires et que notre valeur β (Beta) augmente à 1 % (0,01), alors que l'intervalle entre tests de validation reste à 20 ans. Le taux de défaillance dangereuse augmente à 2,71E-08, ce qui signifie que le sous-système est désormais plus adapté à une utilisation dans un système SIL 3.

Défaillance de cause commune (CCF)

La défaillance de cause commune signifie que plusieurs défauts provoqués par une cause unique entraînent une défaillance dangereuse. Les informations relatives à CCF ne sont généralemnet requises que par le concepteur du sous-système, généralement le fabricant. Elles sont utilisées pour les formules destinées à estimer la PFH_D d'un sous-système. Elles ne sont généralement pas requises à l'étape de la conception du système.

L'annexe F de la norme CEI/EN62061 fournit une approche simple pour l'estimation de CCF. Le tableau 17 présente un résumé du processus de notation.

N°	Mesure contre la CCF	Note
1	Séparation/distinction	25
2	Diversité	38
3	Conception/Application/Expérience	2
4	Evaluation/Analyse	18
5	Compétence/Formation	4
6	Environnement	18

Tableau 17 : notation pour les mesures contre la défaillance de cause commune

Des points sont accordés pour l'emploi de mesures spécifiques contre la CCF. Les notes sont additionnées pour déterminer le facteur de défaillance de cause commune, qui est indiqué au tableau 18. Le facteur beta est utilisé dans la formule d'architecture simplifiée du sous-système pour influencer le taux de défaillance, comme cela a déjà été montré.

Note globale	Facteur de défaillance de cause commune (ß)
<35	10 % (0,1)
35…65	5 % (0,05)
65…85	2 % (0,02)
85…100	1 % (0,01)

Tableau 18 : facteur beta pour la défaillance de cause commune

Taux de couverture des tests de diagnostic (DC)

Des tests de diagnostic automatiques sont utilisés pour diminuer la probabilité de défaillance matérielle dangereuse. Etre capable de détecter toutes les défaillances matérielles dangereuses serait idéal, mais en pratique la valeur maximale est réglée à 99 % (également exprimée comme 0,99).

Le taux de couverture des tests de diagnostic est le rapport entre la probabilité de défaillances dangereuses détectées et la probabilité de défaillances dangereuses totales.

Probabilité de défaillances dangereuses détectées, λ_{DD}

DC =

Probabilité de défaillances dangereuses totales, λ_{Dtotal}

Tolérance aux pannes matérielles

La tolérance aux pannes matérielles représente le nombre de pannes qu'un système peut supporter avant qu'ils ne créent une défaillance dangereuse. Par exemple, une tolérance aux pannes matérielles de un signifie que deux pannes peuvent entraîner la perte de la fonction de sécurité mais pas une seule.

Gestion de la sécurité fonctionnelle

La norme définit des exigences pour la commande correcte des activités de planification, de gestion de projet et techniques nécessaires pour créer un système de commande électrique de sécurité.

Intervalle entre tests de validation

L'intervalle entre tests de validation représente le laps de temps après lequel un sous-système doit être totalement vérifié ou remplacé pour s'assurer qu'il est « comme neuf ». En pratique, dans le secteur des machines, cela se fait par remplacement. L'intervalle entre tests de validation est donc généralemnet identique à la durée de vie. La norme EN ISO 13849-1 appelle cela le temps de mission.

Un test de validation est une vérification qui peut détecter les défauts et les dégradations dans un système SRCS de sorte qu'il peut être restauré pour être aussi proche que possible d'un état « comme neuf ». Le test de validation doit détecter 100 % des défaillances dangereuses. Les voies distinctes doivent être testées séparément.

A l'inverse des tests fonctionnels de diagnostic qui sont effectués automatiquement, les tests de validation sont généralement effectués manuellement et hors ligne. Le test fonctionnel de diagnostic est généralement effectué souvent (généralement à un intervalle de quelques heures), alors que le test de validation est effectué peu souvent (généralement au bout de plusieurs années). Par exemle, les circuits qui vont jusqu'à un interrrupteur de sécurité sur une grille de protection peuvent subir un test fonctionnel automatique pour détecter les courts-circuits et les circuits ouverts grâce à un test de diagnostic (p. ex., par impulsion).

L'intervalle entre tests de validation doit être déclaré par le fabricant. Parfois, le fabricant indique une plage pour différents intervalles entre tests de validation.

Proportion de défaillances non dangereuses (SFF)

La proportion de défaillances non dangereuses est similaire au taux de couverture des tests de diagnostic (DC), mais prend également en compte toute tendance inhérente à tomber en panne en se mettant en état de sécurité. Par exemple, en cas de rupture de fusible, il y a une défaillance mais il est très probable que cette défaillance soit un circuit ouvert qui, dans la plupart des cas, est une défaillance « sécurisée ». SFF est (la somme du taux de défaillances « sécurisées » plus le taux des défaillances dangereuses détectées) divisée par (la somme du taux de défaillances « sécurisées » plus le taux des défaillances dangereuses détectées et non détectées). Il est important de comprendre que les seuls types de défaillances à prendre en considération sont ceux qui peuvent avoir un effet sur la fonction de sécurité.

La plupart des dispositifs mécaniques de faible complexité, comme les boutons d'arrêt d'urgence et les interrupteurs de sécurité, ont (pris individuellement) une SFF relativement faible. La plupart des dispositifs électroniques de sécurité ont une conception qui inclut la redondance et la surveillance, une SFF supérieure à 90 % est donc courante, bien que cela soit généralement complètement dû au taux de couverture des tests de diagnostic.

La valeur SFF est généralement fournie par le fabricant.

La proportion de défaillances non dangereuses (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 taux de défaillances sécurisées,
$\Sigma\lambda_S + \Sigma\lambda_D$ = le taux de défaillances global,
λ_{DD} = le taux de défaillances dangereuses détectées,
λ_D = le taux de défaillances dangereuses.

Défaillance systémique

La norme définit des exigences pour le contrôle et l'évitemment des défaillances systémiques. Ces défaillances diffèrent des défaillances matérielles aléatoires qui sont des pannes qui se produisent de façon aléatoire, généralement provoquées par une dégradation des composants matériels. Les types de défaillances systémiques typiques sont les erreurs de programmation logicielle, les erreurs de conception matérielle, les erreurs dans les caractéristiques requises et autres procédures opérationnelles. Exemples des étapes nécessaires pour éviter les défaillances systémiques :

- sélection, combinaison, agencement, assemblage et installation corrects de composants ;
- recours à des bonnes pratiques d'ingénierie ;
- respect des caractéristiques et des instructions d'installation données par le fabricant ;
- assurer la compatibilité entre les composants ;
- résister aux conditions ambiantes ;
- utilisation de matériaux adaptés.

Structure des systèmes de contrôle-commande de sécurité

Présentation

Ce chapitre aborde des questions et principes généraux relatifs à la structure qui doivent être pris en considération lors de la conception d'un système de commande de sécurité, quelle que soit la norme suivie. Il s'appuie sur les catégories de la norme EN 954-1 parce que ces catégories définissent principalement la structure des systèmes de commande.

Remarque : peu de temps avant la publication de ce texte, le CEN (Comité européen de normalisation) a annoncé que la date finale pour la présomption de conformité à la norme EN 954-1 serait étendue jusque fin 2011 afin de faciliter la transition vers des normes plus récentes. Ceci remplace la date originale qui était fixée au 29 décembre 2009.

Pour les informations les plus récentes sur l'utilisation et l'état de la norme EN 954-1, visitez : *http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx*. En attendant, il est recommandé d'utiliser l'extension de la période de transition pour passer aux nouvelles normes (EN ISO 13849-1 ou CEI/EN 62061) en temps utile.

Catégories de systèmes de contrôle-commande

Les « catégories » des systèmes de contrôle-commande viennent de l'ancienne norme EN 954-1:1996 (ISO13849-1:1999). Cependant, elles sont toujours souvent utilisées pour décrire les systèmes de commande de sécurité et font toujours partie intégrante de la norme EN ISO13849-1, comme abordé dans la section « Présentation de la sécurité fonctionnelle des systèmes de contrôle-commande ».

Il existe cinq catégories qui décrivent la performance de réaction à un défaut d'un système de commande de sécurité. Voir le tableau 19 pour un résumé de ces catégories. Les remarques suivantes concernent le tableau.

Remarque 1 : la catégorie B n'a pas de mesures spéciales pour la sécurité mais elle constitue la base pour les autres catégories.

Remarque 2 : les défauts multiples de cause commune ou étant la conséquence inévitable du premier défaut doivent être comptés comme un seul défaut.

Remarque 3 : l'examen d'un défaut peut être limité à deux défauts combinés si c'est justifiable mais les circuits complexes (p. ex., circuits à microprocesseurs) peuvent nécessiter plus de défauts combinés pour être pris en compte.

La catégorie 1 est destinée à la prévention des défauts. Elle peut être obtenue en s'appuyant sur des principes de conception, des composants et des matériaux adaptés. La simplicité de principe et de conception, avec des matériaux aux caractéristiques stables et prévisibles, sont les clés de cette catégorie.

Les catégories 2, 3 et 4 requièrent que si des défauts ne peuvent pas être évités, ils doivent être détectés et les mesures appropriées prises.

La redondance, la diversité et la surveillance sont les clés de ces catégories. La redondance est la duplication de la même technique. La diversité est l'utilisation de deux techniques différentes. La surveillance est la vérification de l'état des dispositifs et la mise en œuvre de mesures appropriées en fonction de l'état. La méthode habituellement utilisée, mais ce n'est pas la seule, pour la surveillance est la duplication des fonctions critiques de sécurité et des opérations de comparaison.

Structure des systèmes de contrôle-commande de sécurité

Résumé des exigences	Comportement du système
Catégorie B (voir la remarque 1) Les composants de sécurité des systèmes de commande machine et/ou leur équipement de protection, ainsi que leurs éléments, doivent être conçus, fabriqués, sélectionnés, assemblés et assortis selon les normes applicables aux conditions de fonctionnement attendues. Les principes de sécurité de base s'appliquent.	Lorsqu'un défaut se produit, il peut provoquer une perte de la fonction de sécurité.
CATEGORIE 1 Les exigences de la catégorie B s'appliquent, en plus du recours à des composants et des principes de sécurité éprouvés.	Identique à celui décrit pour la catégorie B, mais avec une meilleure fiabilité de la fonction de sécurité. (Plus la fiabilité est élevée, moins il y a de risque de défaut.)
CATEGORIE 2 Les exigences de la catégorie B et le recours à des principes de sécurité éprouvés s'appliquent. La ou les fonctions de sécurité doivent être vérifiées au démarrage de la machine et périodiquement par le système de commande de la machine. Si un défaut est détecté, un état de sécurité doit être initié ou, si cela n'est pas possible, une alarme doit être envoyée. La norme EN ISO 13849-1 présuppose que le taux de test est au moins 100 fois plus fréquent que le taux de sollicitation. La norme EN ISO 13849-1 présuppose que le MTTFd de l'équipement de test externe est supérieur à la moitié du MTTFd de l'équipement fonctionnel testé.	La perte de la fonction de sécurité est détectée par la vérification. L'apparition d'un défaut peut entraîner la perte de la fonction de sécurité entre les intervalles de vérification.
CATEGORIE 3 (voir les remarques 2 & 3) Les exigences de la catégorie B et le recours à des principes de sécurité éprouvés s'appliquent. Le système doit être conçu de façon à ce qu'un seul défaut sur n'importe lequel de ses composants ne provoque pas une perte de la fonction de sécurité. Le cas échéant, un seul défaut doit être détecté.	Lorsqu'un seul défaut se produit, la fonction de sécurité est toujours exécutée. Certains défauts, mais pas tous, sont détectés. Une accumulation de défauts non détectés peut entraîner la perte de la fonction de sécurité.
Catégorie 4 (voir les remarques 2 & 3) Les exigences de la catégorie B et le recours à des principes de sécurité éprouvés s'appliquent. Le système doit être conçu de façon à ce qu'un seul défaut sur n'importe lequel de ses composants ne provoque pas une perte de la fonction de sécurité. Le défaut unique est détecté lors de la sollicitation suivante de la fonction de sécurité, ou avant celle-ci. Si la détection n'est pas possible, une accumulation de défauts ne doit pas provoquer la perte de la fonction de sécurité.	Lorsqu'un seul défaut se produit, la fonction de sécurité est toujours exécutée. Les défauts sont détectés à temps pour éviter la perte des fonctions de sécurité.

Tableau 19 : Catégories de performance de la sécurité

Catégorie B

La catégorie B définit les exigences de base de tout système de commande ; qu'il s'agisse d'un système de commande de sécurité ou pas de sécurité. Un système de commande doit être utilisé 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 est prévu pendant une durée spécifiée et dans des conditions définies.

La catégorie B nécessite la mise en application de principes de base relatifs à la sécurité. La norme ISO 13849-2 définit les principes de base pour la sécurité des systèmes électriques, pneumatiques, hydrauliques et mécaniques. Les principes électriques sont résumés ci-dessous :

- sélection, combinaison, agencements, assemblage et installation corrects (c.-à-d. conforme aux instructions du fabricant) ;
- compatibilité des composants avec les tensions 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 démarrage imprévisibles ;
- fixation sûre des dispositifs d'entrée (p. ex., montage des dispositifs de verrouillage) ;
- protection du circuit de commande (selon NFPA79 & IEC60204-1) ;
- jointure protective correcte.

Le concepteur doit sélectionner, installer et assembler selon les instructions du fabricant. Ces dispositifs doivent fonctionner selon les tensions et intensités nominales prévues. Les conditions ambiantes prévues, comme la compatibilité électromagnétique, les vibrations, les chocs, la contamination et les projections d'eau doivent être prises en considération. Le principe de mise hors tension est utilisé. La protection contre les transitoires est installée entre 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.

Catégorie 1

La catégorie 1 requiert que le système soit conforme aux exigences de la catégorie B et, en plus, qu'il utilise des composants éprouvés. La norme EN ISO 13849-2 donne des informations sur ce que sont des composants éprouvés pour les systèmes mécaniques, pneumatiques et électriques. L'annexe D traite des composants électriques.

Les composants sont considérés comme étant éprouvés s'ils ont été utilisés avec satisfaction dans de nombreuses applications similaires. Les nouveaux composants de sécurité sont considérés comme étant éprouvés s'ils sont conçus et vérifiés conformément aux normes appropriées. Le tableau 20 liste certains composants électriques et leurs normes respectives.

Composant éprouvé	Norme
Interrupteur avec mode à déclenchement positif (ouverture directe)	CEI 60947-5-1
Dispositifs 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 à couplage mécanique	CEI 60947-5-1
Contacteur auxiliaire (p. ex., contacteur, contacteur auxiliaire, relais à guidage réciproque)	EN 50205 CEI 60204 – 1, CEI 60947 – 5 – 1
Transformateur	CEI 60742
Câble	CEI 60204-1
Dispositifs de verrouillage	ISO 14119
Thermostat	CEI 60947-5-1
Pressostat	CEI 60947-5-1 + exigences pneumatiques ou hydrauliques
Dispositif ou équipement de commande et de commutation protectrice (CPS)	CEI 60947-6-2
Automate programmable	CEI 61508

Tableau 20 : Normes pour les composants éprouvés

Si l'on installait des composants éprouvés sur notre système de catégorie B, l'interrupteur de fin de course serait remplacé par un interrupteur à broche à ouverture directe et le contacteur serait surdimensionné pour une meilleure protection contre la soudure des contacts.

La figure 140 montre les modifications apportées au système simple de catégorie B pour obtenir une catégorie 1. Le dispositif de verrouillage et le contacteur jouent les rôles clés dans l'isolement de l'énergie de l'actionneur lorsque l'accès à la zone dangereuse est nécessaire. L'interrupteur à broche est conforme aux exigences de la norme CEI 60947-5-1 pour les contacts à ouverture directe, ce qui est indiqué par le symbole de la flèche dans un cercle. Grâce aux composants éprouvés, la probabilité que l'énergie soit isolée est plus grande pour le système de catégorie 1 que pour le système de catégorie B. L'utilisation de composants éprouvés est prévue pour empêcher une perte de la fonction de sécurité. Même avec ces améliorations, la présence d'un seul défaut peut toujours provoquer la perte de la fonction de sécurité.

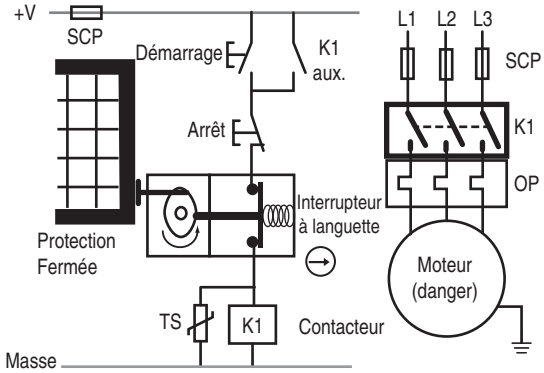


Figure 140 : système de catégorie 1 ou système de sécurité simple

Les catégories B et 1 ont pour base la prévention. La conception a pour objectif d'éviter toute situation de danger. Lorsque seule la prévention ne suffit pas pour fournir une réduction suffisante des risques, la détection des défauts doit être utilisée. Les catégories 2, 3 et 4 sont basées sur la détection des défauts, avec des exigences plus strictes pour atteindre des niveaux de réduction des risques plus élevés.

Catégorie 2

En plus d'être conforme aux exigences de la catégorie B et d'avoir recours à 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 défauts sur les composants de sécurité du système de commande. Si aucun défaut n'est détecté, la machine peut être exploitée. Si des défauts sont détectés, le test doit initier une commande pour amener la machine à un état de sécurité.

La figure 141 montre un schéma fonctionnel de système de catégorie 2. L'équipement qui effectue le test peut faire partie intégrante du système de sécurité ou peut être un équipement distinct.

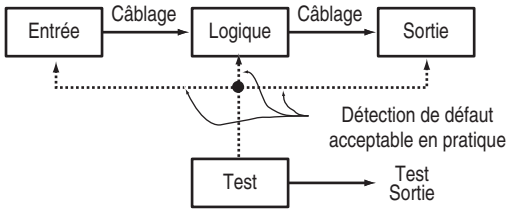


Figure 141 : schéma fonctionnel de la catégorie 2

Les tests doivent être effectués :

- lors de la première mise sous tension de la machine ;
- avant l'initialisation d'une source de danger ; et
- régulièrement si c'est jugé nécessaire lors de l'évaluation des risques.

Remarque : la norme EN ISO 138491-1 présuppose qu'un test de la fonction de sécurité doit avoir un ratio de 100:1. L'exemple donné ne passerait pas ce test.

Les mots « lorsque c'est possible » et « raisonnablement faisable » indiquent que tous les défauts ne sont pas détectables. Puisqu'il s'agit d'un système à une voie (c.-à-d., un fil raccorde l'entrée à la logique et à la sortie), un seul défaut peut provoquer la perte de la fonction de sécurité. Dans certains cas, la catégorie 2 ne peut pas être totalement appliquée à un système de sécurité parce que tous les composants ne peuvent pas être vérifiés.

La figure 140 montre le système simple de catégorie 1 amélioré pour être conforme à la catégorie 2. Un relais de surveillance (MSR) effectue les tests. A la mise sous tension, le MSR vérifie ses composants internes, si aucun défaut n'est détecté, il vérifie l'interrupteur à broche en supervisant le cycle des contacts. Si aucun défaut n'est détecté et que la grille de protection est fermée, le MSR vérifie le dispositif de sortie : les contacts à couplage mécanique du contacteur. Si aucun défaut n'est détecté et que le contacteur est désactivé (OFF), le MSR active sa sortie interne et connecte la bobine de K1 au bouton d'arrêt. A ce stade, les composants du système de commande de la machine qui ne sont pas des composants de sécurité, le circuit de démarrage/arrêt/verrouillage, peuvent démarrer ou arrêter la machine.

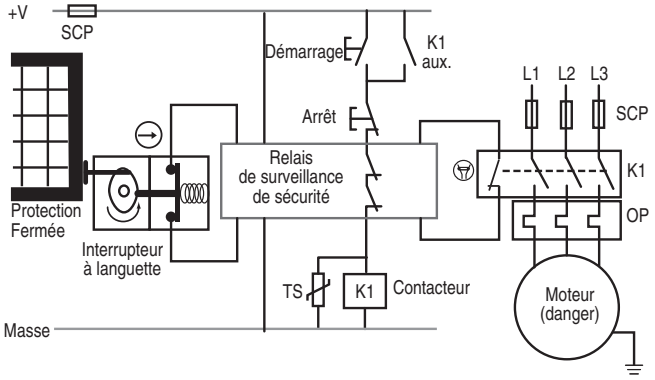


Figure 142 : système de sécurité de catégorie 2

L'ouverture de la grille de protection désactive les sorties du MSR. Lorsque la grille est refermée, le MSR répète les vérifications du système de sécurité. Si aucun défaut n'est découvert, le MSR active sa sortie interne. Le MSR permet à ce circuit d'être conforme à 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 effectué lors de la première mise sous tension et avant l'initialisation de la source du danger.

Grâce à ses capacités logiques inhérentes, un système de sécurité à base d'automate de sécurité (sécurité automate conforme à CEI 61508) peut être conforme à la catégorie 2.

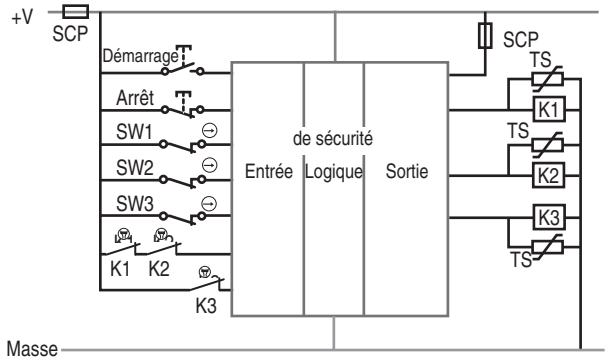


Figure 143 : système de sécurité complexe de catégorie 2

Structure des systèmes de contrôle-commande de sécurité

La figure 143 montre un exemple de système complexe qui utilise un automate de sécurité. Un automate de sécurité est conforme aux exigences des équipements dits éprouvés puisqu'il est conçu en conformité à une norme appropriée. Les contacts à couplage mécanique des contacteurs sont reliés à l'entrée de l'automate pour les tests. Ces contacts peuvent être raccordés en série à une borne d'entrée ou à des bornes d'entrée individuelles, selon le programme logique.

Bien que les composants de sécurité éprouvés soient utilisés, un seul défaut se produisant entre les vérifications peut provoquer la perte de la fonction de sécurité. Par conséquent, les systèmes de catégorie 2 sont utilisés dans les applications où le risque est moins élevé. Lorsqu'une tolérance aux pannes plus élevée est nécessaire, le système de sécurité doit être de carégorie 3 ou 4.

Catégorie 3

En plus d'être conforme aux exigences de la catégorie B et d'avoir recours aux principes de sécurité éprouvés, la catégorie 3 requiert la réussite de la fonction de sécurité en présence d'un défaut unique. Le défaut doit être détecté au moment de, ou avant, la sollicitation suivante de la fonction de sécurité, lorsque cela est raisonnablement possible.

Là encore, nous retrouvons l'expression « raisonnablement possible ». Cela couvre les défauts qui ne sont peut-être pas détectés. Tant que le défaut non détectable ne provoque pas la perte de la fonction de sécurité, cette fonction peut être conforme à la catégorie 3. Par conséquent, une accumulation de défauts non détectés peut provoquer la perte de la fonction de sécurité.

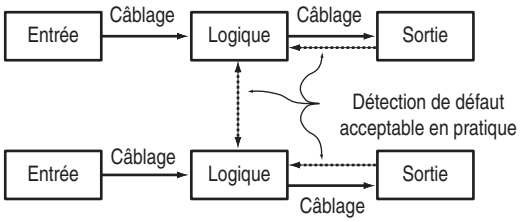


Figure 144 : schéma fonctionnel de la catégorie 3

La figure 144 montre un schéma fonctionnel qui explique les principes du système de catégorie 3. La redondance combinée à une surveillance croisée raisonnablement possible et une surveillance des sorties est utilisée pour assurer la fonction de sécurité.

La figure 145 montre un exemple de système de catégorie 3. Un jeu de contacts redondant est ajouté à l'interrupteur de sécurité à broche. Le relais de surveillance (MSR) contient en interne des circuits redondants qui se surveillent réciproquement. Un jeu de contacteurs redondant coupe l'alimentation du moteur. Les contacteurs sont surveillés par le MSR par le biais des contacts à couplage mécanique « raisonnablement possible ».

La détection des défauts 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 à double voie ? Quels sont les modes de défaillance du MSR ? Quels sont les modes de défaillance des contacteurs K1 et K2 ? Quels sont les modes de défaillance du câblage ?

L'interrupteur à broche est conçu avec des contacts à ouverture directe. Par conséquent, nous savons que l'ouverture de la grille de protection doit ouvrir un contact soudé. Cela résoud un mode de défaillance. Existe-t-il d'autres modes de défaillance ?

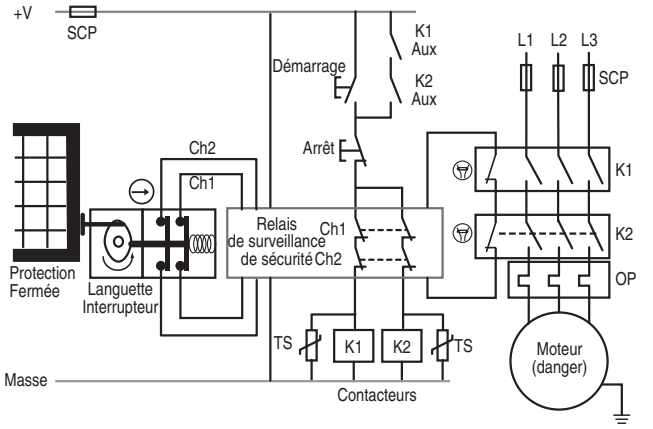


Figure 145 : système de catégorie 3

L'interrupteur à ouverture directe est généralement conçu avec un ressort de rappel. Si la tête est retirée ou arrachée, les contacts de sécrité reviennent en position fermée (sécurisée) grâce au ressort. De nombreux interrupteurs de sécurité sont conçus avec des têtes amovibles afin de faciliter l'installation sur différentes applications. La tête peut être retirée et tournée pour être positionnnée dans deux à quatre positions différentes.

Une défaillance se produit lorsque les vis de fixation de la tête ne sont pas serrées correctement. Dans ce cas, les vibrations de la machine peuvent entraîner le déserrage de ces vis. Avec la poussée du ressort, la tête élimine la pression exercée sur les contacts de sécurité et ces contacts se ferment. Par la suite, l'ouverture de la grille de protection n'ouvre pas les contacts de sécurité et une défaillance dangereuse se produit.

Le mécanisme d'actionnement dans l'interrupteur doit également être examiné. Quelle est la probabilité qu'une défaillance d'un seul composant entraîne la perte de la fonction de sécurité ? Une pratique courante consiste à utiliser des interrupteurs à broche avec deux contacts dans les circuits de catégorie 3. Cette pratique doit être basée sur l'exclusion de la défaillance unique de l'interrupteur à ouvrir les contacts de sécurité. Cela est considéré comme « exclusion de défaut » et est abordé plus loin dans ce chapitre.

Un relais de surveillance (MSR) est souvent évalué par un tiers et se voit attribué une catégorie (et/ou un niveau PL et SIL CL). Le MSR inclut souvent la capacité d'utiliser deux voies, la surveillance transversale des voies, la surveillance de dispositif externe et la protection contre les courts-circuits. Aucune norme spécifique n'existe pour fournir des recommandations sur la conception ou l'utilisation des relais de surveillance. L'évaluation des MSR a pour objectif de définir leur capacité a exécuter la fonction de sécurité selon la norme EN ISO 13849-1 ou l'ancienne norme EN 954-1. La classification du MSR doit être identique ou supérieure à la classification du système dans lequel il est utilisé.

Deux contacteurs permettent de s'assurer que la fonction de sécurité est remplie par les dispositifs de sorties. Avec une protection contre les surcharges et les courts-circuits, la probabilité de défaillance du contacteur à cause de contacts soudés est faible mais pas nulle. Un contacteur peut également tomber en panne avec ses contacts de commutation de l'alimentation restant fermés en raison d'une armature bloquée. Si un contacteur tombe en panne en créant un état dangereux, le deuxième contacteur coupe l'alimentation de la source du danger. Le MSR détecte le contacteur défaillant lors du cycle suivant de la machine. Lorsque la grille de protection est fermée et que le bouton de démarrage est enfoncé, les contacts à couplage mécanique du contacteur défaillant restent ouverts et le MSR ne peut pas fermer ses contacts de sécurité, ce qui révèle le défaut.

Visitez notre site : www.ab.com/catalogs
Publication S117-CA001A-FR-P

Défauts non détectés

Avec un système de catégorie 3, il peut exister des défauts ne pouvant pas être détectés mais ils ne doivent pas, à eux seuls, entraîner la perte de la fonction de sécurité.

Lorsque les défauts peuvent être détectés, nous devons savoir si, dans certains circonstances, ils pourraient être masqués ou remis à zéro involontairement par l'activation d'autres dispositifs du système.

La figure 146 montre une approche souvent utilisée pour raccorder plusieurs dispositifs à un relais de surveillance. Chaque dispositif contient deux contacts à ouverture directe normalement fermés. Ces dispositifs peuvent être une combinaison de dispositifs de verrouillage ou de boutons d'arrêts d'urgence. Cette approche permet de faire des économies sur le coût du câblage puisque les dispositifs d'entrées sont raccordés en série. Supposons qu'un court-circuit de produit sur un des contacts Sw2, comme illustré. Ce défaut peut-il être détecté ?

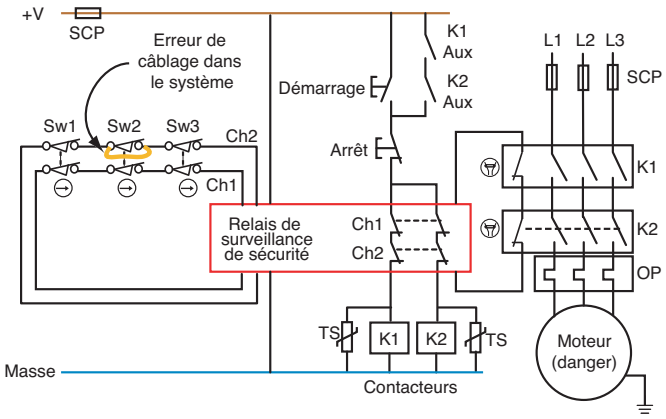


Figure 146 : connexion en série des dispositifs d'entrées

Si l'interrupteur Sw1 (ou Sw3) est ouvert, les deux voies Ch1 et Ch2 sont en circuit ouvert et le MSR coupe l'alimentation de la source du danger. Si Sw3 est alors ouvert puis refermé, le défaut sur ses contacts n'est pas détecté parce qu'il n'y a pas de changement d'état sur le MSR : les deux voies Ch1 et Ch2 restent ouvertes. Si Sw1 (ou Sw3) est alors fermé, la source du danger peut être redémarrée en appuyant sur le bouton de démarrage. Dans ces circonstances, le défaut n'a pas entraîné la perte de la fonction de sécurité mais il n'a pas été détecté, il reste dans le système et un défaut ultérieur (un court-circuit sur le deuxième contact de Sw2) pourrait entraîner la perte de la fonction de sécurité.

Si uniquement Sw2 a été ouvert et fermé, sans activation des autres interrupteurs, la voie Ch1 s'ouvre et la voie Ch2 reste fermée. Le MSR met hors tension la source du danger parce que la voie Ch1 a été ouverte. Lorsque Sw2 se ferme, le moteur ne peut pas être démarré par un appui sur le bouton de démarrage, ceci parce que la voie Ch2 n'a pas été ouverte. Le défaut est détecté. Cependant, si pour une raison quelconque, Sw1 (ou Sw3) est alors ouvert et fermé, les circuits des deux voies Ch1 et Ch2 sont ouverts puis fermés. Cette séquence simule l'effacement du défaut et entraîne une remise à zéro involontaire du MSR.

Ceci pose la question de quel taux de couverture des tests de diagnostic (DC) peut être atteint par les interrupteurs individuels dans cette structure lorsque la norme EN ISO 13849-1 ou CEI 62061 est utilisée. Au moment de la publication de ce document, il n'existe pas de recommandation spécifique définitive sur ce sujet, mais un DC de 60 % est généralement utilisé à condition que les interrupteurs soient testés individuellement à des moments opportuns pour révéler les défauts. S'il est prévisible qu'un ou plusieurs interrupteurs ne sera jamais testé individuellement, alors son DC devrait être décrit comme étant zéro. Au moment de la plublication de ce document, la norme EN ISO 13849-2 est en cours de révision. Lorsqu'elle sera publiée, il est possible qu'elle fournisse d'autres recommandations à ce sujet.

La connexion en série des contacts mécaniques est limitée à la catégorie 3 parce qu'elle peut conduire à la perte de la fonction de sécurité en raison d'une accumulation de défauts. D'un point de vue pratique, la réduction du DC (et donc du SFF) limite les niveaux PL et SIL maximum pouvant être atteints à PLd et SIL2.

Il est intéressant de noter que ces caractéristiques d'une structure de catégorie 3 ont toujours nécessité une prise en compte mais qu'elles sont mises en évidence par les nouvelles normes relatives à la sécurité fonctionnelle.

La figure 147 montre un circuit de catégorie 3 qui utilise un variateur de vitesse de sécurité. Les développements récents de la technologie des variateurs, associés à la mise à jour des normes EN/IEC 60204-1 et NFPA79, permettent d'utiliser les variateurs de sécurité dans les circuits d'arrêt d'urgence sans avoir recours à un sectionneur électromécanique de l'actionneur (p. ex. le moteur).

Un appui sur l'arrêt d'urgence ouvre les sorties du MSR. Cela envoie un signal d'arrêt au variateur, retire le signal de validation et ouvre l'alimentation de la commande de gâchette. Le variateur exécute un arrêt de catégorie 0 – suppression immédiate de l'alimentation du moteur. Cette fonction s'appelle « arrêt sécurisé du couple ». Le variateur atteint une catégorie 3 parce qu'il a des signaux redondants pour couper l'alimentation du moteur : validation et un relais à guidage réciproque. Le relais à guidage réciproque fournit un retour raisonnablement pratique à l'actionneur. Le variateur lui-même est analysé pour vérifier qu'un seul défaut ne provoque pas la perte de la fonction de sécurité.

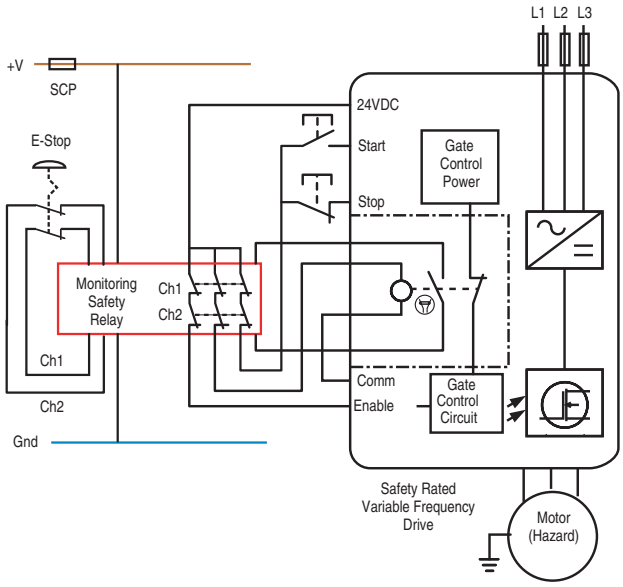


Figure 147 : variateurs de sécurité avec arrêt d'urgence de catégorie 3

La figure 148 donne un exemple de défaut de câblage, de court-circuit, entre la sortie de sécurité de la voie 2 du MSR et la bobine du contacteur K1. Tous les composants fonctionnent correctement. Ce défaut de câblage peut se produire avant la mise en service de la machine ou ultérieurement pendant la maintenance ou au cours d'une mise à niveau. Ce défaut peut-il être détecté ?

Structure des systèmes de contrôle-commande de sécurité

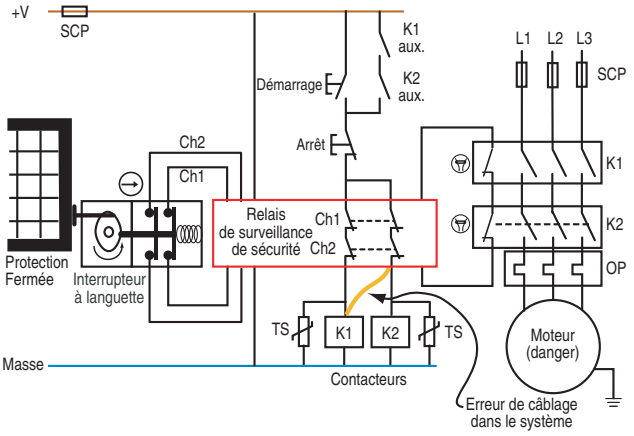


Figure 148 : exemple 1 de défaut de câblage

Comme le montre la figure, ce défaut ne peut pas être détecté par le système de sécurité. Heureusement, il ne peut pas à lui seul provoquer la perte de la fonction de sécurité. Ce défaut, ainsi que le défaut entre la voie Ch1 et K2, doit être détectée pendant la mise en service ou au cours des vérifications suivant le travail de maintenance. La liste des exclusions de défauts possibles donnée dans le tableau D4 de l'annexe D de la norme EN ISO 13849-2 indique clairement que ces types de défauts peuvent être exclus si l'équipement est contenu dans une armoire électrique et qu'à la fois l'armoire et le câblage sont conformes aux exigences de la norme CEI/EN 60204-1. Le rapport technique conjoint de EN ISO 13849-1 et CEI 62061 indique également clairement que cette exclusion de défaut peut être prise en compte jusqu'à, et y compris, PLe et SIL3. Elle peut également être utilisée pour la catégorie 4.

La figure 149 donne un autre exemple de défaut de câblage. Ce défaut se produit entre le contact à couplage mécanique de K2 et l'entrée de surveillance du MSR. Ce défaut peut-il être détecté ?

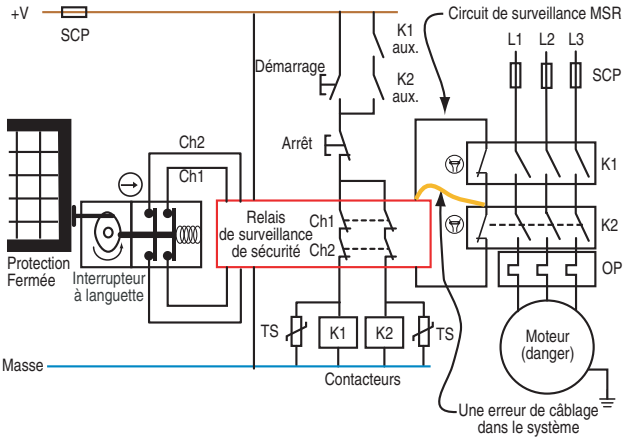


Figure 149 : réarmement manuel surveillé pour détecter les défauts

Comme le montre la figure, ce défaut ne peut pas être détecté par le système de sécurité. Le circuit de surveillance du MSR est un circuit en série qui doit être fermé avant le démarrage. Tant que le circuit est fermé, le MSR croit que tous les dispositifs surveillés sont désactivés et prêts à fonctionner. Dans cet exemple, un contacteur K1 soudé ou bloqué ne sera pas détecté ; il sera masqué par le court-circuit. Avec deux contacteurs, la fonction de sécurité est effectuée par K2, si K1 est défaillant. Un MSR sans réarmement manuel surveillé peut remplacer le MSR avec réarmement automatique pour détecter ce type de défaut. Ce type de MSR requiert un changement d'état sous forme de signal à front montant ou descendant, comme abordé dans l'exemple suivant et également dans la section « Mesures de protection et équipement complémentaire ».

La figure 150 montre la même situation que la figure 149, à l'exception du circuit de surveillance du MSR qui a changé de fonction et est passé d'automatique à manuel surveillé. Cela est accompli dans le MSR par une modification du câblage ou par des changements de modèle. Le réarmement manuel surveillé peut détecter ce type de défaut parce que le circuit de surveillance doit être ouvert au moment où la grille de protection est fermée. Après la fermeture de la grille, le bouton de réarmement doit être enfoncé. Dans de nombreux relais (mais pas dans tous), les sorties du MSR sont activées lorsque le bouton de réarmement est relâché. Cet impératif de changement d'état signifie que le relais ne peut pas être « trompé » et se réarmer à cause d'un blocage permanent du bouton de réarmement ou qu'il ne peut pas être réarmé involontairement par un court-circuit.

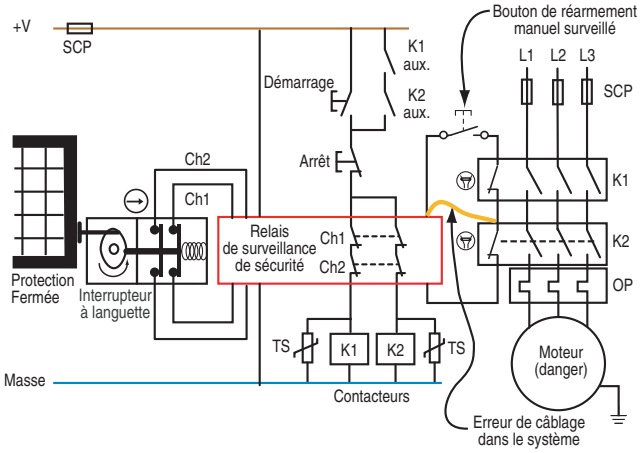


Figure 150 : réarmement manuel surveillé pour détecter les défauts

La figure 151 montre un défaut d'entrée entre voies. Un défaut se produit entre la voie 1 et la voie 2 au niveau de l'entrée du MSR. Avec huit connexions pour les deux voies, il existe de nombreuses façons de créer un défaut entre les voies. Ce défaut peut-il être détecté ?

La détection de ce défaut dépend du type de MSR. Les MSR avec microprocesseur utilisent la détection des défauts par test à impulsion (voir l'explication plus loin) et certains MSR utilisent des entrées complémentaires. Une entrée est rappelée à la source +V, et la deuxième entrée est rappelée à la masse. Dans les deux cas, le court-circuit du câblage est détecté immédiatement et l'entrée de sécurité du MSR est désactivée, ce qui coupe l'alimentation de la source du danger.

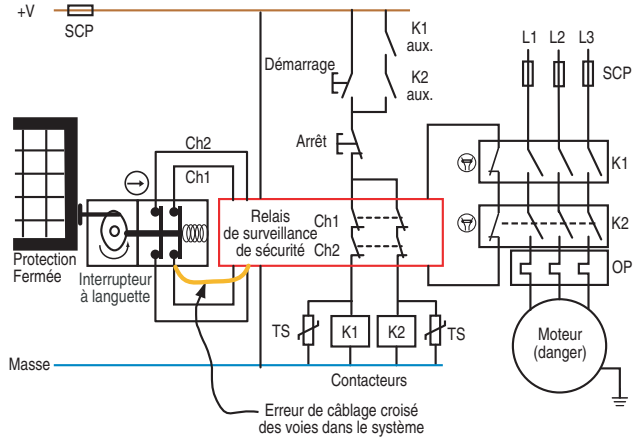


Figure 151 : défaut d'entrée entre voies

Détection de défaut par test à impulsion

Les circuits de sécurité sont conçus pour faire circuler le courant lorsque le système de sécurité est actif et que la source du danger est protégée. Le test par impulsion est une technique dans laquelle le courant du circuit chute à zéro pendant un temps très court. Ce temps est trop court pour que le circuit de sécurité réagisse et qu'il désactive le danger, mais suffisant pour être détecté par un système à microprocesseur. Les impulsions sur les voies sont décalées l'une par rapport à l'autre. Si un défaut de court-circuit transversal se produit, le microprocesseur détecte les impulsions sur les deux voies et envoie une commande de désactivation de la source du danger.

La figure 152 illustre ce principe. Cette technique détecte également les courts-circuits au +V de l'alimentation. Les relais de surveillance à microprocesseur et les systèmes à base d'automate de sécurité utilisent le test par impulsion.

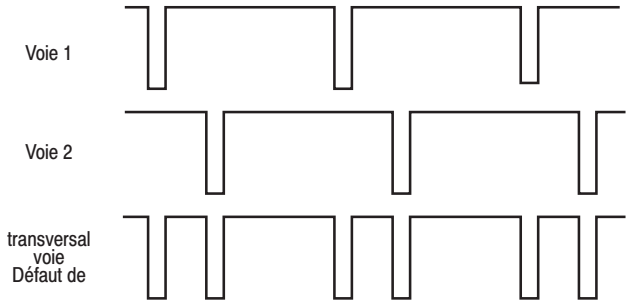


Figure 152 : défaut entre voies avec test par impulsion

La figure 153 montre un agencement dans lequel deux sorties de l'automate sont configurées pour le test par impulsion. Des impulsions alternées sont connectées à chaque voie activée par des interrupteurs mécaniques. Cette approche détecte les défauts entre voies, ainsi que les défauts vers l'alimentation et la terre. Ce test par impulsion est requis par la catégorie 3 parce qu'il est raisonnablement possible de détecter les défauts entre voies de cette façon.

Les défauts décrits ci-dessus ne sont qu'un sous-ensemble des défauts qui doivent être pris en compte. Les courts-circuits au +V, à la terre, les courts-circuits avec d'autres circuits et les conditions de circuit ouvert doivent être évalués. De plus, la classification des composants et leur performance doivent être pris en considération.

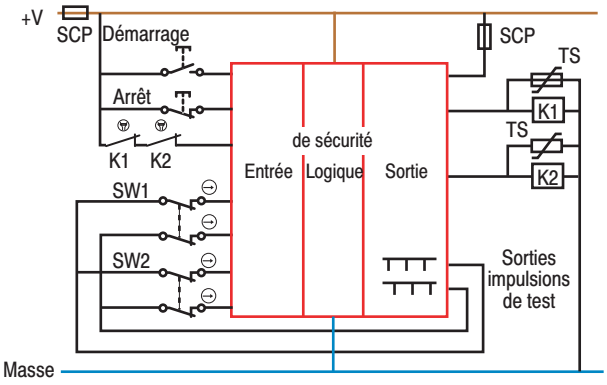


Figure 153 : automate de sécurité utilisant le test par impulsion pour la détection des défauts

La figure 154 montre une variante d'agencement avec automate de sécurité. Dans certains cas, le raccordement d'un dispositif non classé de sécurité à un système de sécurité est nécessaire et bénéfique. Si les sorties sont de type PNP, elles peuvent être connectées directement à l'entrée de l'automate de sécurité. Si elles sont à double voie, elles peuvent être considérées comme conformes aux exigences raisonnables de la catégorie 3.

Un autre point à prendre en compte pour les modules d'automate de sécurité est le nombre d'entrées. Parfois, une ou deux entrées supplémentaires peuvent être nécessaires, mais l'espace panneau ne permet pas d'installer un bloc supplémentaire. Dans ce cas, les dispositifs d'entrée peuvent être raccordés en série (p. ex., SW1 et SW2) et tout de même être conformes aux exigences de la catégorie 3. La contre-partie est la perte d'information sur quel interrupteur est actionné, à moins qu'un contact supplémentaire ne soit utilisé et connecté au système de commande de la machine.

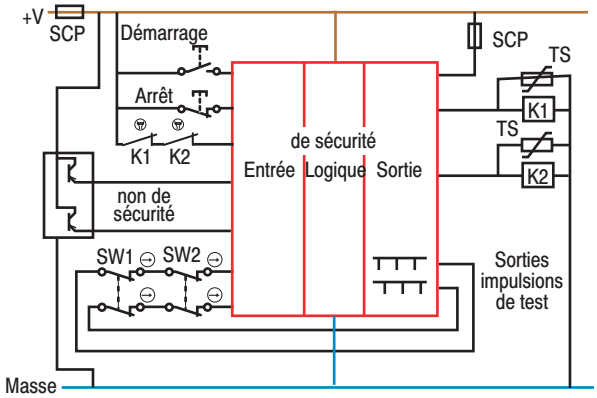


Figure 154 : entrées complexes conformes à la catégorie 3 avec un automate de sécurité

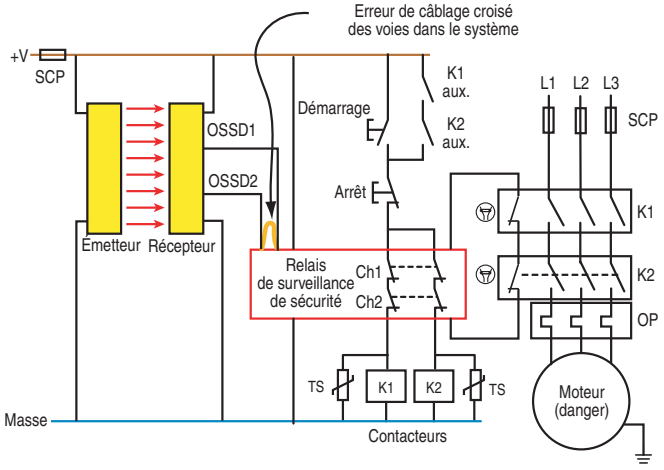


Figure 155 : défaut de câblage entre voies avec barrières immatérielles

La figure 155 montre un exemple de système de sécurité avec barrières immatérielles (sorties OSSD à semi-conducteurs).

Dans cet exemple, le défaut de câblage est détecté avec le test par impulsion sur la barrière immatérielle. La détection du défaut est immédiate et la barrière immatérielle désactive sa sortie.

Catégorie 4

Comme la catégorie 3, la catégorie 4 impose que le système de sécurité soit conforme à la catégorie B, qu'il ait recours à des principes de sécurité et exécute la fonction de sécurité en présence d'un seul défaut. A l'inverse de la catégorie 3 pour laquelle une accumulation de défauts peut conduire à la perte de la fonction de sécurité, la catégorie 4 nécessite que la fonction de sécurité soit exécutée même en présence d'une accumulation de défauts. En pratique, la prise en compte d'une accumulation de deux défauts peut être suffisante, bien que 3 défauts puissent être nécessaires dans certains cas en raison de la complexité.

La figure 156 montre le schéma fonctionnel de la catégorie 4. La surveillance des deux dispositifs de sorties et la surveillance transversale sont requises, et pas uniquement lorsque c'est raisonnablement possible. Cela facilite la distinction entre la catégorie 4 et la catégorie 3.

Structure des systèmes de contrôle-commande de sécurité

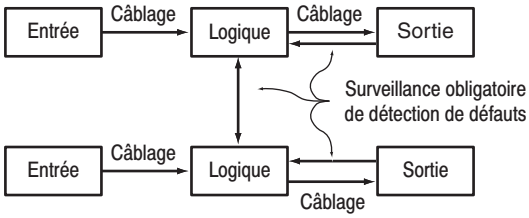


Figure 156 : schéma fonctionnel de la catégorie 4

La figure 157 donne un exemple de circuit de catégorie 4 avec un interrupteur de sécurité sans contact à deux voies.

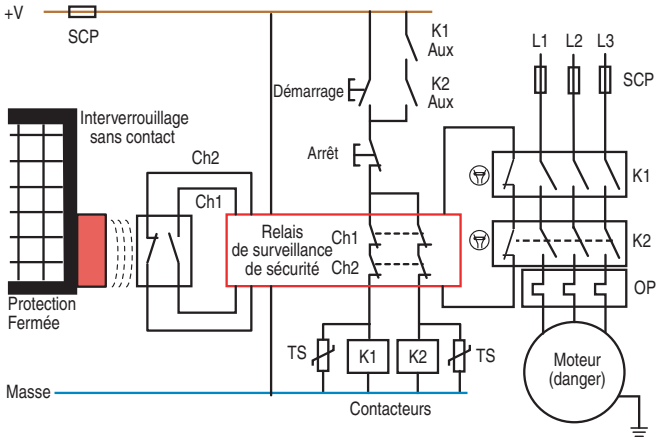


Figure 157 : système avec dispositif de verrouillage sans contact de catégorie 4

Jusqu'à récemment, les interrupeurs de sécurité à broche étaient parfois utilisés dans les circuits de catégorie 4. Pour utiliser un interrupteur à broche dans un circuit à deux voies, il est nécessaire d'exclure les points de défaillance unique potentiels sur la broche mécanique d'activation et le couplage de l'interrupteur. Cependant, le rapport technique conjoint des normes EN ISO 13849-1 et CEI 62061 a défini clairement que ce type d'exclusion de défaut ne doit pas être utilisé dans les systèmes PLe ou SIL 3.

Si le concepteur du système de sécurité préfère utiliser des interrupteurs de sécurité à broche, alors deux interrupteurs peuvent être utilisés pour être conforme à la catégorie 4. La figure 158 présente un exemple utilisant deux interrupteurs de sécurité à broche avec contacts à ouverture directe.

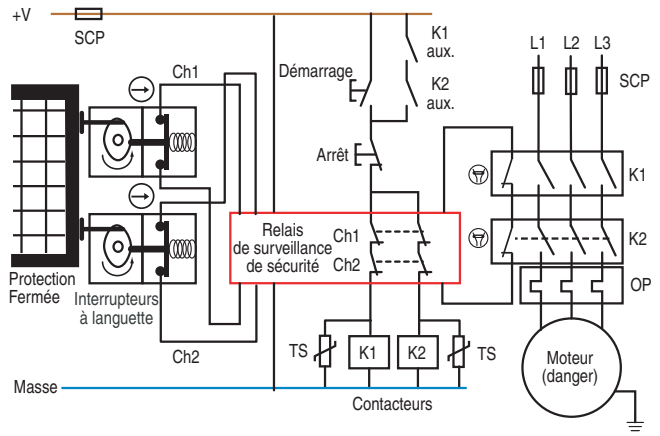


Figure 158 : catégorie 4 avec interrupteurs à broche redondants

Le relais de surveillance lui-même doit être classé de catégorie 4, et les deux contacteurs de sortie, qui utilisent des contacts à couplage mécanique, doivent être surveillés.

La figure 159 montre un relais de surveillance modulaire avec un interrupteur sans contact raccordé à chaque module d'entrée. Si le relais de sécurité est classé en catégorie 4, cet agencement de dispositifs d'entrée est conforme à la catégorie 4. Remarquez qu'avec cette approche modulaire, le relais de sécurité est à base de microprocesseur et utilise la vérification par impulsion pour détecter les défauts transversaux.

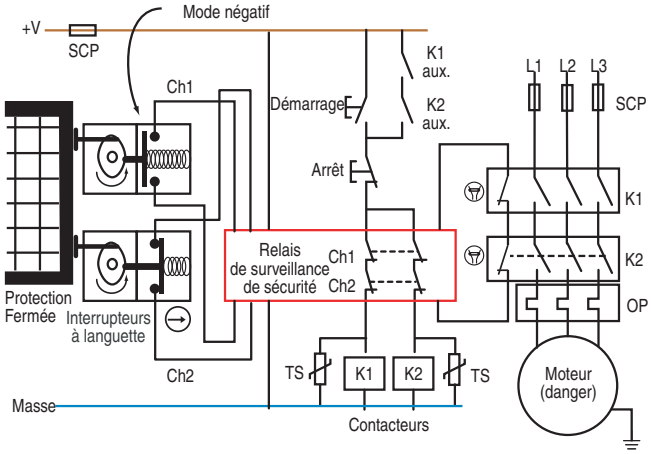


Figure 159 : système de relais de sécurité modulaire de catégorie 4

Classification des composants et du système

Les catégories peuvent être utilisées pour la classification des composants de sécurité (dispositifs), ainsi que pour la classification des systèmes. Cela génère une certaine confusion qui peut être clarifiée par une compréhension des composants et de leurs capacités. En étudiant les exemples précédents, nous constatons qu'un composant comme un interrupteur de sécurité classé en catégorie 1 peut être utilisé seul dans un système de catégorie 1, et qu'il peut également être utilisé dans un système de catégorie 2 si une surveillance supplémentaire des fonctions est fournie. Il peut également faire partie d'un système de catégorie 3 ou 4 si deux de ces composants sont utilisés ensemble avec une fonction de diagnostic fournie par un relais de surveillance.

Certains composants, comme les relais de surveillance et les automates de sécurité programmables, ont leurs propres diagnostics internes et font une auto-vérification afin d'assurer un bon fonctionnement. Ils peuvent donc être classés comme des composants de sécurité conformes aux catégories 2, 3 et 4 sans avoir recours à des mesures supplémentaires.

Considération sur les défauts

L'analyse de la sécurité requiert une analyse extensive des défauts, et une très bonne connaissance du fonctionnement du système de sécurité en présence de défauts si nécessaire. Les normes ISO 13849-1 et ISO 13849-2 fournissent des détails sur la prise en compte des défauts et des exclusions de défaut.

Si un défaut entraîne la défaillance d'un autre composant, le premier défaut et les défauts suivants sont considérés comme un seul défaut.

Si plusieurs défauts se produisent en raison d'une seule cause, ces défauts sont considérés comme un seul défaut. Cela s'appelle un défaut de cause commune.

L'apparition de plusieurs défauts en même temps est considérée comme très improbable et n'est pas prise en compte dans l'analyse. Un postulat de base consiste à considérer qu'un seul défaut se produira entre les sollicitations de la fonction de sécurité, à condition que les intervalles entre les appels à cette fonction ne soient pas trop longs.

Exclusions de défaut

L'ancienne norme EN 954-1, et les normes EN ISO 13849-1 et CEI 62061 plus récentes permettent toutes de recourir aux exclusions de défaut pour déterminer la classification d'un système de sécurité s'il peut être démontré que l'apparition d'un défaut est extrêmement peu probable. Il est important que lorsque des exclustions de défaut sont utilisées elles soient correctement justifiées et qu'elles soient valables pour toute la durée de vie du système de sécurité. Plus le risque contre lequel le système de sécurité protège est élevé, plus la justification requise pour l'exclusion d'un défaut est stricte. Cela a toujours provoqué une certaine confusion sur les types d'exclusion de défaut qui peuvent ou non être utilisés. Comme nous l'avons déjà vu dans ce chapitre, les normes et documents de recommandations récents ont clarifiés certains aspects de ce problème.

En général, lorsqu'une fonction de sécurité devant être mise en œuvre par un système de sécurité est classée PLe ou SIL3, il n'est pas normal de s'en remettre uniquement aux exclusions de défaut pour atteindre ce niveau de performance. Cela dépend de la technologie utilisée et de l'environnement d'utilisation prévu. Il est donc essentiel que le concepteur prenne des précautions supplémentaires pour utiliser les exclusions de défaut lorsque les exigences de ce niveau de performance PL ou SIL augmentent. Par exemple, l'exclusion de défaut ne peut pas être utilisée pour les aspects mécaniques des détecteurs de position électromécaniques et des interrupteurs manuels (p. ex., un dispositif d'arrêt d'urgence) pour obtenir un système classé PLe ou SIL3. Les exclusions de défaut pouvant être appliquées à des conditions de défaut mécanique spécifiques (p. ex., usure/corrosion, rupture) sont décrites dans le tableau A.4 de la norme ISO 13849-2. Par conséquent, un système de verrouillage de grille qui doit atteindre un niveau PLe ou SIL3 doit incorporer une tolérance aux pannes minimum de 1 (p. ex., deux détecteurs de position mécaniques conventionnels) pour atteindre ce niveau de performance puisqu'il n'est normalement pas justifié d'exclure les défauts ; comme par exemple des actionneurs cassés. Cependant, il peut être acceptable d'exclure des défauts, comme un court-circuit sur le câblage d'un panneau de commande conçu conformément aux normes appropriées.

Des informations complémentaires sur les exclusions de défaut seront fournies dans un révision à venir de la norme EN ISO 13849-2.

Catégories d'arrêt selon les normes CEI/EN 60204-1 et NFPA 79

Lorsque l'on parle de système de commande de sécurité, le terme « catégorie » a deux significations et cela porte à confusion. Jusqu'à présent, nous avons abordé les catégories définies par la norme EN 954-1. Elles correspondent à une classification des performances du système de sécurité dans certaines conditions.

Il existe également une classification appelée « catégories d'arrêt » qui est définie dans les normes CEI/EN 60204-1 et NFPA 79. Il existe trois catégories d'arrêt.

La catégorie d'arrêt 0 requiert le retrait immédiat de l'alimentation des actionneurs. Cela est parfois considéré comme un arrêt non contrôlé parce que, dans certains circonstances, le mouvement peut prendre un certain temps pour s'arrêter puisque le moteur peut se mettre en roue libre pour s'arrêter.

La catégorie d'arrêt 1 requiert que l'alimentation soit maintenue afin de pouvoir freiner jusqu'à l'arrêt complet, ensuite intervient le retrait de l'alimentation de l'actionneur.

Avec la catégorie d'arrêt 2, il n'est pas obligatoire que l'alimentation de l'actionneur soit coupée.

Remarquez que seules la catégorie d'arrêt 0 ou 1 peut être utilisée comme arrêt d'urgence. Le choix entre les deux catégories doit être dicté par une évaluation des risques.

Tous les exemples de circuits présentés jusqu'à présent dans ce chapitre utilisaient une catégorie d'arrêt 0. Une catégorie d'arrêt 1 est obtenue avec une sortie temporisée pour la coupure finale de l'alimentation. Une grille interconnectées avec verrouillage accompagne souvent un système d'arrêt de catégorie 1. Cela permet de maintenir la grille verrouillée en position fermée jusqu'à ce que la machine soit dans un état de sécurité (c.-à-d., qu'elle soit arrêtée).

L'arrêt d'une machine sans une prise en compte correcte de l'automate programmable peut avoir des conséquences sur le redémarrage et peut provoquer des dégâts sérieux sur les outils ou la machine. Un automate standard (non classé de sécurité) ne peut pas être utilisé seul pour une tâche d'arrêt de sécurité ; par conséquent, d'autres approches doivent être envisagées.

Deux solutions possibles sont indiquées ci-dessous :

1. Relais de sécurité avec commande de contournement temporisée

La figure 160 montre un système câblé qui permet un arrêt selon une séquence correcte afin de protéger la machine et le programme.

Un relais de sécurité avec des sorties à déclenchement immédiat et temporisé est utilisé (p. ex., MSR138DP). Les sorties à déclenchement immédiat sont raccordées aux entrées du dispositif programmable (p. ex., automate) et les sorties temporisées sont raccordées au contacteur. Lorsque l'interrupteur de sécurité est actionné, les sorties immédiates du relais de sécurité sont commutées. Cela signale au système programmable qu'il doit exécuter un arrêt selon une séquence correcte. Lorsqu'un délai court mais suffisant pour permettre le déroulement de ce processus, la sortie temporisée du relais de sécurité est commutée et isole le contacteur principal.

Remarque : tout calcul fait pour déterminer le temps d'arrêt total doit prendre en compte la temporisation de la sortie du relais de sécurité. Cela est particulièrement important lorsque ce facteur est utilisé pour déterminer le positionnement des dispositifs par rapport au calcul de la distance de sécurité.

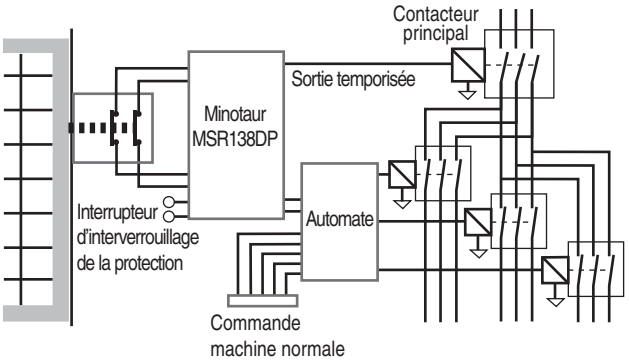


Figure 160 : sorties temporisées pour un arrêt programmé

2. automate de sécurité

Les fonctions logiques et de temporisation requises peuvent être mises en œuvre en utilisant un automate (de sécurité) ayant un niveau d'intégrité de la sécurité approprié. En pratique, cela serait réalisé en utilisant un automate de sécurité comme le SmartGuard ou GuardLogix.

Structure des systèmes de contrôle-commande de sécurité

Exigences du système de contrôle de la sécurité américain

Aux Etats-Unis, les impératifs du système de contrôle de la sécurité sont décrits dans différentes normes, mais deux documents se distinguent : ANSI B11.TR3 et ANSI R15.06.

Le rapport technique ANSI B11.TR3 définit quatre niveaux caractérisés par le niveau de réduction des risques que chacun peut permettre. Ci-dessous sont présentés les exigences de chaque niveau.

Niveau de réduction des risques le plus faible

Dans la norme ANSI B11.TR3, les protections qui offrent la plus faible réduction des risques incluent les dispositifs électriques, électroniques, hydrauliques et pneumatiques et les systèmes de commande connexes qui utilisent une configuration à une seule voie. Implicite dans les exigences est l'obligation d'utiliser des dispositifs de sécurité. Ceci est très proche de la catégorie 1 de la norme ISO13849-1.

Réduction des risques faible/intermédiaire

Dans la norme ANSI B11.TR3, les protections qui fournissent une réduction des risques faible/intermédiaire incluent les systèmes de commande avec une redondance pouvant être vérifiée manuellement pour s'assurer du fonctionnement du système de sécurité. Si l'on considère les exigences pures, le système utilise une redondance simple. L'utilisation d'une fonction de vérification n'est pas requise. Sans vérification, l'un des composants de sécurité redondants peut tomber en panne et le système de sécurité ne le détecterait pas. Cela aurait pour résultat un système à une seule voie. Ce niveau de réduction des risques est semblable à la catégorie 2 lorsque la vérification est utilisée.

Réduction des risques élevée/intermédiaire

Dans la norme ANSI B11.TR3, les protections qui fournissent une réduction des risques élevée/intermédiaire incluent les systèmes de commande ayant une redondance avec auto-vérification au démarrage pour s'assurer du fonctionnement du système de sécurité. Pour les machines qui sont démarrées chaque jour, l'auto-vérification constitue une amélioration significative pour l'intégrité de la sécurité par rapport au système purement redondant. Pour les machines qui fonctionnent 24h/24, 7j/7, l'auto-vérification est une amélioration marginale, au mieux. Avec l'utilisation de la surveillance périodique du système de sécurité, ce niveau est similaire aux exigences de la catégorie 3.

Réduction des risques la plus élevée

La norme ANSI B11.TR3 permet la réduction des risques la plus élevée avec les systèmes de commande ayant une redondance avec auto-vérification permanente. L'auto-vérification doit vérifier le fonctionnement du système de sécurité. Le défi du concepteur du système de sécurité est de définir ce qui est permament. De nombreux systèmes de sécurité exécutent leurs vérifications au démarrage et lorsqu'un le système de sécurité est sollicité.

Par ailleurs, certains composants exécutent une auto-vérification permanente. Les barrières immatérielles, par exemple, allument et éteignent leurs DEL de façon séquentielle. Grâce à cette auto-vérfication permanente, si un défaut se produit, la barrière immatérielle désactive ses sorties avant que le système de sécurité ne soit sollicité. Les relais et automate de sécurité à microprocesseur sont d'autres composants qui exécutent une auto-vérification permanente.

L'exigence d'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 miicroprocesseur. La vérification doit être exécutée au démarrage et après chaque sollicitation du système de sécurité. Ce niveau de réduction des risques est similaire à la catégorie 4 de la norme ISO13849-1.

Normes relatives aux robots : Etats-Unis et Canada

Les normes relatives aux robots aux Etats-Unis (ANSI RIA R15.06) et au Canada (CSA Z434-03) sont très similaires. Les deux possèdent quatre niveaux, qui sont similaires aux catégories de la norme EN954-1:1996 et qui sont décrits ci-dessous.

Simple

A ce niveau le plus bas, les systèmes de sécurité simples doivent être conçus et construits avec des circuits à une voie reconnus ; ils peuvent également être programmables.

Au Canada, ce niveau est limité uniquement à la signalisation.

Le défi pour le concepteur du système de sécurité est de définir ce qui est « reconnu ». Qu'est-ce qu'un circuit à une voie reconnu ? Par qui le système est-il reconnu ?

Cette catégorie simple est la plus proche de la catégorie B de la norme EN954-1:1996.

Une voie

Il s'agit du niveau suivant d'un système de commande de sécurité à une voie qui :

- est un dispositif matériel ou est un dispositif logiciel/firmware de sécurité ;
- inclut des composants de sécurité ;
- est utilisé conformément aux recommandations du fabricant ; et
- utilise des circuits éprouvés.

Un exemple de circuit éprouvé est un dispositif à contact à ouverture électromécanique à une voie qui commande un arrêt dans un état désactivé.

Etant un système à une voie, une seule défaillance de composant peut provoquer la perte de la fonction de sécurité.

Cette catégorie est la plus proche de la catégorie 1 de la norme EN954-1:1996.

Dispositif logiciel/firmware de sécurité

Bien que les systèmes matériels ait été la méthode préférée pour la protection des robots, les dispositifs logiciels/firmware deviennent un choix populaire en raison de leur capacité à gérer des systèmes complexes. Les dispositifs logiciels/firmware (automates ou contrôleurs de sécurité) sont autorisés à condition qu'ils soient classés de sécurité. Ce classement exige que la défaillance d'un seul composant de sécurité ou firmware n'entraîne pas la perte de la fonction de sécurité. Lorsque le défaut est détecté, les actions automatiques suivantes du robot sont empêchées jusqu'à ce que le défaut soit corrigé.

Pour obtenir un classement de sécurité, le dispositif logiciel/firmware doit être testé par rapport à une normes agréée dans un laboratoire agréé. Aux Etats-Unis, OSHA publie une liste à jour des laboratoires d'essais agréés au niveau national (NRTL). Au Canada, le Conseil canadien des normes (CCN) publie une liste similaire.

Une voie avec surveillance

Les systèmes de commande de sécurité à une voie avec surveillance doivent être conformes aux exigences relatives à la voie unique, être classés de sécurité et utiliser la vérification. La vérification de la fonction de sécurité doit être exécutée au démarrage de la machine et régulièrement en cours de fonctionnement. La vérification automatique est préférable à la vérification manuelle.

L'opération de vérification autorise le fonctionnement si aucun défaut n'est détecté ou elle génère un signal d'arrêt si un défaut est détecté. Un avertissement doit être émis s'il reste un danger après l'arrêt du mouvement. Bien sûr, la vérification elle-même ne doit pas créer de situation dangereuse. Lorsque le défaut à été détecté, le robot doit rester dans un état de sécurité jusqu'à ce que le défaut soit corrigé.

Une voie avec surveillance est proche de la catégorie 2 de la norme EN954-1:1996.

Commande fiable

Le plus haut niveau de réduction des risques dans les normes relatives aux robots aux Etats-Unis et au Canada est obtenu par des systèmes de commande de sécurité conformes aux exigences relatives à une commande fiable. Les systèmes de commande de sécurité à commande fiable sont des architectures à double voie avec surveillance. La fonction d'arrêt du robot ne doit pas être empêchée par la défaillance d'un seul composant, notamment la fonction de surveillance.

La surveillance doit générer une commande d'arrêt lors de la détection d'un défaut. Un avertissement doit être émis s'il reste un danger après l'arrêt du mouvement. Le système de sécurité doit rester dans un état de sécurité jusqu'à ce que le défaut soit corrigé.

De préférence, le défaut doit être détecté au moment de la défaillance. Si cela n'est pas possible, la défaillance doit être détectée lors de la sollicitation suivante du système de sécurité.

Les défaillances de cause commune doivent être prises en compte s'il existe une probabilité significative qu'une telle défaillance se produise.

Les exigences canadienne sont différentes des exigences américaines ; en effet il existe deux exigences supplémentaires au Canada. Premièrement, le système de commande de sécurité doit être indépendant des systèmes de commande normaux. Deuxièmement, le système de sécurité doivent être difficiles à neutraliser ou à contourner sans que cela ne soit détecté.

Les systèmes à commande fiable sont les plus proches des catégories 3 et 4 de la norme EN 954-1:1996.

Commentaires sur la commande fiable

L'aspect le plus fondamental de la commande fiable est sa tolérance à un seul défaut. Les exigences indiquent comment le système de sécurité doit réagir en présence « d'un seul défaut », de « tout défaut unique » ou de « toute défaillance d'un seul composant ».

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

L'objectif de la commande fiable est clairement l'exécution de la fonction de sécurité en présence d'un défaut. Si le défaut est détecté, le système de sécurité doit exécuter une action de sécurité, avertir du défaut et empêcher le fonctionnement de la machine jusqu'à ce que le défaut soit corrigé. Si le défaut n'est pas détecté, la fonction de sécurité doit tout de même être exécutée en cas de sollicitation.

Remarques