MACHINERY SAFEBOOK 5

Allen-Bradley

Guardmaster®

Systèmes de commande de sécurité pour les machines

Principes, normes et mise en œuvre

(Révision 5 de la série Safebook)

LISTEN. THINK. SOLVE.℠

Rockwell Automation

Systèmes de commande de sécurité pour les machines

Sommaire

Chapitre 1 : Réglementations

Directives et Législation de l'UE

Le but de ce chapitre est de servir de guide de référence à toutes les personnes concernées par la sécurité des machines, notamment par les systèmes de protection physique et de sécurité utilisés dans l'Union Européenne. Il s'adresse aussi bien aux concepteurs qu'aux utilisateurs d'équipements industriels.

Afin de promouvoir le concept de marché ouvert au sein de l'EEE (l'espace économique européen qui comprend tous les états membres de l'UE plus trois autres pays), tous les états membres ont l'obligation de promulguer des lois définissant des exigences de sécurité essentielles concernant les machines et leur utilisation.

Des machines ne se conformant pas à ces exigences ne peuvent être fournies ou importées dans les pays de l'EEE.

Il existe plusieurs directives européennes concernant la sécurité des machines et des équipements industriels. Mais les deux qui sont les plus directement applicables sont :

1 La Directive Machines

2 La directive relative à l'utilisation des équipements de travail

Ces deux directives sont étroitement liées par le fait que les exigences essentielles de santé et de sécurité (EESS) définies par la Directive Machines peuvent également être utilisées pour apprécier la sécurité des équipements dans le cadre de la directive sur l'utilisation des équipements de travail.

Ce chapitre présente les différents aspects de ces deux directives. Il est fortement conseillé à toute personne concernée par la conception, la fourniture, l'achat ou l'utilisation d'un équipement industriel dans un pays de l'EEE (et également dans certains autres pays), d'être familiarisée avec leurs critères. Tous les fournisseurs ou utilisateurs de machines dans les pays concernés risquent en effet de se voir refuser la livraison ou l'utilisation de leurs équipements s'ils ne se conforment pas ces directives.

Il existe également d'autres directives européennes ayant rapport aux machines. La plupart d'entre elles concernent en général un domaine d'application particulier. Elles ne sont donc pas prises en considération dans le cadre de ce chapitre. Mais il est important de noter que leurs exigences doivent également être respectées lorsqu'elles sont applicables. C'est le cas, par exemple : de la directive CEM 2014/30/CE et de la directive ATEX 2014/34/CE.

La Directive Machines

La directive Machines réglemente la fourniture de nouvelles machines et autres équipements incorporant des composants de sécurité. La livraison de machines non conformes aux exigences de cette directive sur le territoire de l'union européenne constitue une infraction.

Une définition extrêmement large du terme « machines » est fournie par la directive : « 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 reliés entre eux et dont au moins un est mobile, et qui sont assemblés solidairement en vue d'une application spécifique ».

Marquage CE de la machine

La directive Machines actuelle (2006/42/CE) a remplacé la version précédente (98/37/CE) fin 2009. Elle apporte des clarifications et des amendements, mais n'introduit pas de modifications radicales des exigences essentielles de santé et de sécurité (EESS) d'origine. Elle introduit quelques modifications destinées à tenir compte des évolutions technologiques et méthodologiques. Elle élargit son champ d'application à un plus grand nombre de familles d'équipements (par exemple, les engins de levage destinés aux chantiers de construction). Elle introduit par ailleurs explicitement l'exigence d'une évaluation des risques afin de déterminer les EESS applicables. De même, elle apporte des modifications aux procédures d'évaluation de conformité pour les équipements de l'Annexe IV.
Des informations détaillées et recommandations sur la définition et tous les autres aspects de la Directive Machines sont disponibles sur le site Internet officiel de l'UE :

http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery/index_en.htm

Les dispositions clés de la directive originale (98/37/CE) 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/CE) sont en vigueur depuis le 29 décembre 2009. Le fabricant ou son représentant agréé a la responsabilité de s'assurer que l'équipement fourni est conforme à la directive. Cela inclut :

- la vérification que les exigences essentielles de santé et de sécurité (EESS) applicables, telles que figurant dans l'Annexe I de la directive, sont remplies ;
- l'établissement d'un dossier technique ;
- la réalisation d'une évaluation de conformité appropriée ;
- la fourniture d'une « déclaration de conformité CE » ;
- l'apposition du marquage CE, le cas échéant ;
- la fourniture d'instructions d'utilisation de sécurité.

Exigences essentielles de santé et de sécurité

La machine doit respecter les EESS

L'Annexe 1 de la directive fournit une liste d'exigences essentielles de santé et de sécurité (désignées par EESS) auxquelles les machines doivent se conformer lorsque concernées. L'objectif de cette liste est de s'assurer que les machines présentent les caractéristiques de sécurité requises ; notamment qu'elles sont conçues et fabriquées de façon à garantir durant toutes les phases de leur existence un fonctionnement et la réalisation d'interventions de réglage et de maintenance qui ne risquent pas de porter atteinte à la sécurité des personnes. Le texte suivant propose un bref aperçu d'exigences typiques, mais il est important de prendre en considération toutes les EESS citées à l'annexe 1. Une évaluation des risques doit être réalisée afin de déterminer les EESS applicables à l'équipement considéré.

Les EESS de l'Annexe 1 fournissent une hiérarchie des mesures destinées à éliminer les risques :

(1) Sécurité inhérente à la conception. Chaque fois que c'est possible, la prévention des risques devra être incluse dans la conception de la machine. Lorsque c'est impossible, des **(2) dispositifs de protection complémentaires** devront être utilisés ; par exemple, des grilles de protection avec points d'accès interverrouillés, des barrières immatérielles de sécurité, des tapis de détection, etc. Tout risque résiduel ne pouvant être géré par l'une des méthodes ci-dessus devra être limité par des **(3) équipement de protection individuelle et/ou une formation appropriée**. Le fournisseur de la machine doit alors spécifier ce qui est approprié.

Des matériaux adaptés à l'utilisation doivent être utilisés pour la fabrication. Un éclairage adéquat et des accessoires de manutention doivent être fournis. Les commandes et systèmes de commande doivent présenter les caractéristiques de sécurité et de fiabilité requises. Les machines ne doivent pas avoir la possibilité de redémarrer intempestivement et doivent être munies d'un ou plusieurs dispositif(s) d'arrêt d'urgence. Les installations complexes dans lesquelles des processus amont ou aval sont susceptibles d'interférer sur la sécurité d'une machine, doivent être prises en compte. 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 les contraintes prévisibles. Elles ne doivent pas comporter de rebords ou de surfaces non protégés, susceptibles de causer des blessures corporelles.

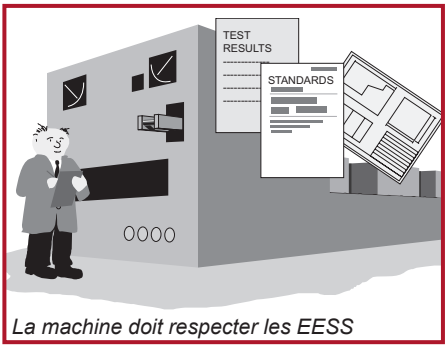
Des grilles ou des équipement de protection doivent être utilisés pour prévenir les dangers liés aux pièces en mouvement. Ces dispositifs doivent être de construction robuste et difficiles à contourner. Des dispositifs de protection fixes doivent être montés

de telle sorte qu'ils ne puissent être démontés qu'avec des outils et les fixations doivent être imperdables. Les dispositifs de protection amovibles doivent être équipés d'un système de verrouillage électrique de sécurité. Les dispositifs de protection réglables doivent pouvoir être facilement ajustés, sans nécessiter d'outils.

Les dangers liés aux alimentations électriques et à d'autres sources d'énergie, y compris d'énergie emmagasinée, doivent également être évités. Les risques de blessures corporelles dus à la température, à une explosion, au bruit, aux vibrations, aux poussières, aux gaz ou aux radiations, doivent être minimisés au maximum. Des dispositions adaptées doivent être prises pour la maintenance et les interventions courantes. Une signalisation suffisante et des dispositifs d'alarme doivent être prévus. Les machines doivent être livrées avec des instructions d'installation, d'exploitation, de réglages, etc., garantissant la sécurité.

Évaluation de conformité

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



La machine doit respecter les EESS

Une norme européenne (EN) harmonisée, publiée au Journal Officiel (JO) de l'Union Européenne sous la rubrique Directive Machines et dont la date de présomption de conformité n'est pas expirée, peut conférer une telle présomption de conformité à certaines EESS (de nombreuses normes publiées récemment au JO incluent en effet des tableaux d'équivalence indiquant les EESS couvertes.) En conséquence, lorsque l'équipement est conforme à des normes européennes harmonisées en vigueur de ce type, la démonstration de conformité aux EESS se trouve grandement simplifiée. Le fabricant bénéficie également d'une meilleure présomption de légalité. La conformité à ces normes n'est cependant pas une exigence légale. Toutefois, il est vivement conseillé de s'en servir car il peut s'avérer extrêmement complexe de démontrer la conformité par d'autres moyens. Ces normes, émises par le CEN (Comité européen de normalisation) en collaboration avec l'ISO et le CENELEC (Comité européen de normalisation électrotechnique) en collaboration avec la CEI, viennent compléter la Directive Machines.

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

Dossier technique

Le fabricant ou son représentant doit préparer un dossier technique démontrant la conformité de la machine aux EESS. Ce dossier doit contenir toutes les informations utiles : résultats d'essais, plans, caractéristiques, etc.

Il n'est pas essentiel que toutes ces informations soient imprimées de façon systématique. Mais ce dossier technique doit pouvoir être présenté en cas d'inspection par une autorité compétente (un organisme mandaté par un pays de l'UE pour vérifier la conformité des machines).

Un dossier technique doit comporter au moins les documents suivants :

1 Les plans d'ensemble de l'équipement, comprenant les schémas des circuits de commande.

2 Les plans de détail, les notes de calcul, etc., nécessaires à la vérification de la conformité de la machine aux EESS.

3. La documentation sur l'évaluation des risques, notamment la liste des exigences essentielles de santé et de sécurité applicables à la machine et une description des mesures de protection mises en place.

4 La liste des normes et autres spécifications techniques utilisées en référence, mentionnant les exigences essentielles de santé et de sécurité concernées.

5 Un descriptif des méthodes adoptées pour supprimer les risques présentés par la machine.

6 Le cas échéant, tout rapport technique ou certificat délivré par un laboratoire de test ou tout autre organisme d'homologation.

7 Si la conformité à une norme européenne harmonisée est déclarée, tout rapport technique attestant du résultat des essais.

8 Un exemplaire des instructions d'utilisation de la machine.

9 Le cas échéant, la déclaration d'incorporation concernant les éléments de la machine partiellement montés inclus dans la livraison et les notices de montage de ces éléments.

10 Le cas échéant, les copies des déclarations de conformité CE des éléments ou accessoires externes intégrés à la machine.

11 Une copie de la déclaration de conformité CE.

Pour les machines fabriquées en série, le détail des mesures internes (système d'assurance qualité, par exemple) mises en œuvre pour s'assurer que chaque équipement produit est conforme aux spécifications :

- Le constructeur devra notamment effectuer sur les composants, les assemblages ou sur la machine terminée, toutes les analyses ou essais nécessaires afin de vérifier que la conception et la construction de cette machine lui permettent d'être installée et mise en service avec toutes les garanties de sécurité.

- Le dossier technique ne doit pas nécessairement être conservé de façon permanente en un seul tenant. Mais tous ses éléments doivent pouvoir être réunis facilement pour être présentés dans un délai raisonnable. Il doit rester consultable pendant dix ans après la production du dernier exemplaire de la machine.

Concernant les sous-ensembles utilisés dans la fabrication de la machine, il n'est pas nécessaire d'inclure dans le dossier technique leurs plans détaillés ou autres informations spécifiques, à moins qu'ils soient essentiels pour le contrôle de la conformité aux EESS.

Évaluation de conformité pour les machines relevant de l'Annexe IV

Évaluations de la conformité

Certains types d'équipements sont sujets à des dispositions particulières. C'est le cas des équipements listés à l'Annexe IV de la directive, dont font partie des machines dangereuses telles que certaines machines à bois, les presses, les machines de moulage par injection, les équipements souterrains, les ponts élévateurs pour les véhicules, etc.

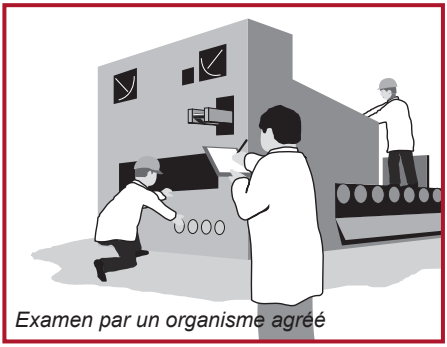
L'Annexe IV inclut également certains composants de sécurité tels les dispositifs de protection basés sur la détection de présence des personnes (ex. : barrières immatérielles) et les unités logiques assurant des fonctions de sécurité.

Dans le cas où une machine relevant de l'Annexe IV ne serait pas en totale conformité avec les normes européennes harmonisées applicables, son fabricant ou le représentant agréé de celui-ci doit effectuer l'une des procédures suivantes :

1. Contrôle de conformité type CE. Un dossier technique doit être préparé et un exemplaire de la machine doit être soumis à un organisme agréé (laboratoire

de test) pour subir un contrôle de conformité CE. Si la machine est jugée conforme, l'organisme lui attribuera un certificat de conformité CE. La validité de ce certificat est de cinq ans et la machine devra être réévaluée selon cette périodicité par l'organisme agréé.

2. Assurance qualité totale. Un dossier technique doit être préparé et le constructeur doit utiliser un système d'assurance qualité certifié pour la conception, la fabrication, l'inspection finale et les tests. Le système de contrôle qualité doit garantir la conformité de la machine aux dispositions de cette directive. Ce système de contrôle qualité doit être réévalué périodiquement par un organisme agréé.



Examen par un organisme agréé

Pour les machines ne relevant pas de l'Annexe IV, ou pour celles concernées par cette annexe mais totalement conformes aux normes européennes harmonisées applicables, le fabricant ou son représentant agréé a aussi la possibilité de préparer le dossier technique et de réaliser lui-même l'évaluation et la déclaration de conformité de l'équipement. Il doit exister un système de contrôle interne destiné à s'assurer que les équipements fabriqués en série restent conformes.

Organismes agréés

Un réseau d'organismes agréés communiquant entre eux et travaillant sur des bases communes est présent dans toute l'UE. Ces organismes agréés sont mandatés par les gouvernements (et non par les industriels). Des renseignements sur les organismes bénéficiant de l'agrément peuvent être obtenus à l'adresse :

http://ec.europa.eu/growth/tools-databases/nando/

Procédure de déclaration de conformité CE

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

Le marquage CE indique que la machine est conforme à tous les directives européennes applicables et que les procédures d'évaluation de conformité ont été réalisées. L'apposition du marquage CE en référence à la Directive Machines sur des machines qui ne satisferaient pas aux EESS applicables constitue une infraction.

La Déclaration de conformité CE doit contenir les informations suivantes :

- nom et adresse professionnelle complète du fabricant et, le cas échéant, de son représentant agréé ;
- nom et coordonnées de la personne habilitée à établir le dossier technique. Celle-ci doit résider dans la Communauté (dans le cas d'un constructeur se trouvant hors UE, il pourra s'agir de son « représentant agréé ») ;
- description et identification des machines, notamment : dénomination générique, fonction, modèle, type, numéro de série et nom commercial ;
- déclaration spécifiant expressément que la machine remplit toutes les conditions applicables de cette directive et, lorsque nécessaire, déclaration de même type spécifiant la conformité aux autres directives et/ou dispositions applicables à la machine ;
- le cas échéant, la mention des normes harmonisées utilisées en référence ;
- le cas échéant, la mention des autres normes et spécifications techniques utilisées en référence ;
- (pour les machines relevant de l'Annexe IV) le cas échéant, le nom, l'adresse et le numéro d'identification de l'organisme agréé qui a réalisé le contrôle de conformité CE selon l'Annexe IX, ainsi que le numéro du certificat de conformité CE ;
- (pour les machines relevant de l'Annexe IV) le cas échéant, le nom, l'adresse et le numéro d'identification de l'organisme agréé qui a certifié le système d'assurance qualité selon l'Annexe X ;
- le lieu et la date d'établissement 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'incorporation CE pour les machines partiellement terminées

Lorsque l'équipement fourni est destiné à être assemblé à d'autres composants afin de former ultérieurement une machine complète, une DÉCLARATION D'INCORPORATION doit l'accompagner. Le marquage CE ne doit PAS alors y être apposé. La déclaration doit spécifier que l'équipement ne doit pas être mis en service tant que la machine à laquelle il doit être incorporé n'a pas été déclarée conforme. Un dossier technique doit être établi et la machine partiellement terminée doit être fournie avec une documentation contenant la description des conditions à respecter pour que son incorporation dans la machine finale ne soit pas de nature à compromettre la sécurité.

Cette option n'est pas applicable aux équipements pouvant fonctionner de façon indépendante ou à ceux qui modifient la finalité d'une machine.

La Déclaration d'incorporation doit contenir les informations suivantes :

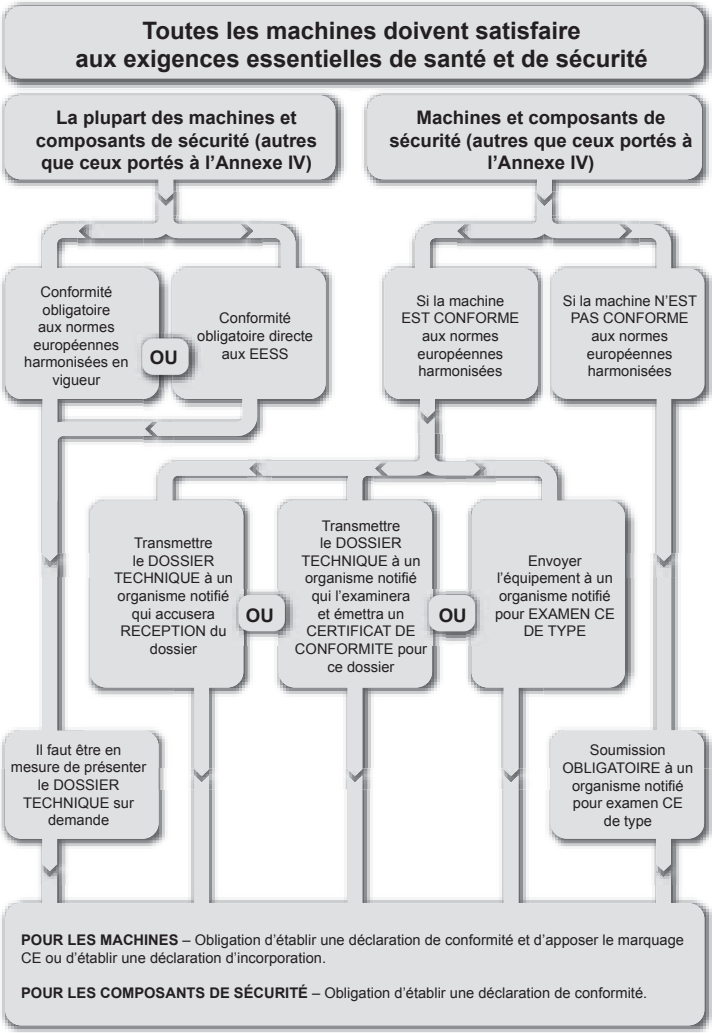
- nom et coordonnées professionnelles complètes du fabricant de la machine partiellement terminée et, si applicable, de son représentant agréé ;
- nom et coordonnées de la personne habilitée à établir le dossier technique. Celle-ci doit résider dans la Communauté (dans le cas d'un constructeur se trouvant hors UE, il pourra s'agir de son « représentant agréé ») ;
- description et identification de la machine partiellement terminée, notamment : dénomination générique, fonction, modèle, type, numéro de série et nom commercial ;
- déclaration spécifiant quelles exigences essentielles de la directive sont remplies. Cette déclaration devra mentionner également que la documentation technique jointe a été établie conformément aux réquisitions de la partie B de l'annexe VII. Le cas échéant, une déclaration de la conformité de la machine partiellement terminée à toutes les autres directives applicables devra également être incluse ;
- engagement à transmettre toutes informations pertinentes concernant la machine partiellement terminée sur demande motivée des autorités nationales. La méthode de transmission de ces informations devra être mentionnée, ainsi que les réserves de propriété intellectuelle du fabricant de la machine partiellement terminée ;
- déclaration stipulant que la machine partiellement terminée ne doit pas être mise en service tant que la machine finale à laquelle elle doit être intégrée n'a pas été déclarée conforme aux dispositions de la directive, si c'est le cas ;
- le lieu et la date d'établissement 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 provenant de l'extérieur de l'UE – Représentants agréés

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

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

Directive européenne relative à l'utilisation d'équipements de travail



Alors que la Directive Machines est destinée aux fournisseurs, cette directive (2009/104/CE) concerne les utilisateurs de machines. Elle couvre tous les secteurs industriels et impose aux employeurs des obligations générales ainsi que des exigences minimales de sécurité concernant les équipements de travail. Tous les pays de l'UE promulguent leurs propres lois pour l'application de cette directive.

Par exemple, elle est mise en œuvre au Royaume-Uni sous le nom « Provision and Use of Work Equipment Regulations » (souvent abrégé en P.U.W.E.R.). Les modalités de mise en application peuvent varier d'un pays à l'autre, mais toutes les dispositions prévues par la directive seront toujours reprises.

Les articles de la directive décrivent en détail les types d'équipements et de postes de travail concernés.

Ils définissent également des obligations d'ordre général pour les employeurs ; par exemple, la mise en place de méthodes de travail de sécurité et la fourniture d'équipements de sécurité adaptés et correctement entretenus. Les opérateurs sur machine doivent recevoir une formation et un entraînement appropriés de façon à utiliser leur machine en toute sécurité.

Les machines neuves (et les machines d'occasion provenant de l'extérieur de l'UE) livrées après le 1er janvier 1993 doivent satisfaire à toutes les directives produits applicables, par exemple la Directive Machines (sous réserve d'aménagements transitoires). Les équipements d'occasion provenant de l'extérieur de l'UE installés pour la première fois sur un poste de travail doivent être directement conformes aux exigences minimales mentionnées en annexe de la directive U.W.E. relative à l'utilisation des équipements de travail.

Remarque : une machine d'origine ou d'occasion ayant fait l'objet d'un reconditionnement ou d'une modification majeure sera considérée comme un équipement neuf. Ceci a pour but de s'assurer que les tâches effectuées par cette machines seront conformes à la Directive Machines (même si elle est uniquement utilisée en interne par l'entreprise).

La conformité de l'équipement de travail est une exigence importante de la directive. 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 implique en principe l'existence d'un programme de maintenance periodique et préventive dûment planifié. Il est recommandé d'établir un registre des opérations de maintenance et de le tenir à jour. Ceci est particulièrement important dans les cas où l'entretien et le contrôle de l'équipement sont les garants de l'efficacité permanente des dispositifs ou systèmes de protection.

L'annexe de la directive U.W.E. stipule les exigences générales minimum pour l'équipement de travail

Si l'équipement est conforme aux directives produits applicables, par exemple la Directive Machines, il sera automatiquement conforme aux exigences de conception machine correspondantes stipulées dans les exigences minimales de l'annexe.

Les états membres sont autorisés à promulguer des lois portant sur l'utilisation des équipements de travail allant au-delà des exigences minimales de la directive U.W.E. relative à l'utilisation d'équipements de travail.

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 :

https://osha.europa.eu/en/legislation/directives/3

Réglementation des États-Unis

Ce paragraphe présente certaines des réglementations relatives à la protection de sécurité des machines industrielles en vigueur aux États-Unis. Cette présentation se limite aux principes de base. Les lecteurs sont encouragés à approfondir plus en détail les exigences applicables à leur application spécifique et à prendre toutes dispositions pour s'assurer que la conception, l'utilisation et les procédures de maintenance de leurs machines répondent non seulement à leurs besoins spécifiques, mais aussi aux codes et règlements nationaux et locaux.

Nombreux sont les organismes attachés à la promotion de mesures de sécurité industrielles aux États-Unis. On trouve parmi eux :

1. des entreprises qui appliquent les réquisitions générales en vigueur aussi bien que des règles spécifiques à leur activité propre ;

2. l'OSHA (Occupational Safety and Health Administration) ;

3. des organisations industrielles comme l'Association nationale de protection contre l'incendie (NFPA), la Robotics Industries Association (RIA) et l'Association of Manufacturing Technology (AMT) ou encore l'ANSI, qui publie une liste de normes unanimement reconnues, auxquelles il convient d'ajouter des fournisseurs de produits et de solutions de sécurité comme Rockwell Automation.

L'OSHA (Occupational Safety and Health Administration)

Aux États-Unis, l'OSHA compte parmi les protagonistes les plus actifs de la sécurité industrielle. Cette administration a été créée en 1971 par une décision du Congrès américain. Cette loi fixe le cadre réglementaire des conditions d'hygiène et de sécurité du travail dans l'industrie, avec l'objectif de préserver les ressources humaines. La loi autorise le Secrétaire d'état au travail à édicter des normes obligatoires d'hygiène et de sécurité du travail, applicables aux entreprises effectuant des transactions commerciales inter-états sur le marché intérieur. Cette loi s'applique à toutes les entreprises employant de la main d'œuvre dans n'importe quel état des États-Unis, dans le district de Columbia, dans l'état libre de Puerto Rico, aux îles Vierges, aux Samoa américaines, à Guam, dans le Territoire sous tutelle des îles du Pacifique, à l'île de Wake, sur les terres du plateau continental extérieur définies dans la loi Outer Continental Shelf Lands Act, sur l'île Johnston et dans la zone du canal de Panama.

L'article 5 de la loi en définit les exigences minimales. Tout employeur a pour obligation de fournir à l'ensemble de ses employés des conditions et un cadre de travail exempts de tous les dangers connus susceptibles d'entraîner la mort ou des blessures physiques graves. Il doit par ailleurs se conformer aux normes d'hygiène et de sécurité du travail définies par la loi.

L'article 5 stipule également que tout employé doit se conformer aux normes d'hygiène et de sécurité du travail ainsi qu'à toutes les règles, réglementations et décrets promulgués en application de cette loi et définissant sa conduite et ses agissements personnels.

La loi instituant l'OSHA a fixé les responsabilités attachées à l'employeur et à l'employé. C'est une approche totalement différente de celle de la Directive Machines qui impose aux fournisseurs de mettre sur le marché des machines exemptes de risques. Aux États-Unis, un fournisseur peut très bien vendre une machine sans aucun équipement de protection. C'est à l'utilisateur qu'il revient d'ajouter l'équipement de protection destiné à sécuriser la machine. Bien que cette pratique ait été courante lors de l'adoption de la loi, la tendance actuelle est que les constructeurs incorporent directement les équipements de protection sur les machines. Il est plus économique de concevoir le système de sécurité en même temps que la machine, plutôt que de l'ajouter par la suite. Les normes actuelles incitent les constructeurs et les utilisateurs à définir les exigences de sécurité en commun de façon à ce que les machines soient à la fois plus sécurisées et plus productives.

Le Secrétaire d'état au travail a toute autorité pour entériner comme norme d'hygiène et de sécurité au travail toute norme de consensus national, ainsi que toute norme fédérale établie, sauf si cette ratification entraînait l'absence d'amélioration des conditions d'hygiène et de sécurité pour certaines catégories particulières de travailleurs.

L'OSHA est chargée de la mise en application par le biais de la publication de règlements sous le Titre 29 du Code of Federal Regulation (29 CFR). Les normes concernant les machines industrielles sont publiées par l'OSHA dans la Partie 1910 de ce Titre 29 CFR. Elles sont en libre accès sur le site Internet de l'OSHA, à l'adresse www.osha.gov. Contrairement à la plupart des autres normes qui présentent un caractère d'application volontaire, les normes OSHA ont force de loi.

Certaines des rubriques importantes pour la sécurité des machines sont listées à la suite :

A – Généralités
B – Adoption et prolongement des normes fédérales établies
C – Recommandations générales d'hygiène et de sécurité
H – Matériaux dangereux
I – Équipements de protection individuelle
J – Dispositions de protection générales vis à vis de l'environnement – inclus les systèmes de condamnation/signalisation
O – Protection par rapport aux composants en mouvement et aux machines
R – Industries particulières
S – Électricité

Certaines normes OSHA peuvent faire référence à d'autres normes de type volontaire. L'effet légal de l'incorporation par référence est que la totalité du corpus normatif est considérée comme ayant été publiée au Federal Register. Lorsqu'une norme de consensus national est incorporée par référence dans l'une des sous-parties, cette norme acquiert force de loi.

Par exemple, la NFPA 70, qui est une norme à caractère volontaire connue sous le nom de Code national électrique des États-Unis, est mise en référence dans la sous-partie S. Les exigences de la norme NFPA 70 revêtent ainsi un caractère obligatoire.

La sous-partie J de la norme 29 CFR 1910.147 concerne le contrôle des sources d'alimentation présentant un danger. Elle est couramment désignée par « norme Lockout/Tagout » (condamnation/signalisation). La norme volontaire correspondante est l'ANSI Z244.1. Essentiellement, cette norme impose que l'alimentation de la machine soit condamnée quand des opérations d'entretien ou de maintenance sont effectuées. L'objectif est d'empêcher toute remise sous tension ou démarrage intempestifs de la machine qui pourraient entraîner des dommages corporels du personnel.

Les employeurs doivent mettre en place un programme de condamnation et signalisation, et employer des procédures destinées à appliquer des moyens de condamnation ou de signalisation sur les dispositifs de coupure d'alimentation. En tout état de cause, la désactivation de la machine ou de l'équipement devra interdire toute remise sous tension, tout redémarrage ou toute libération d'énergie stockée intempestifs, afin de prévenir tout accident corporel.

Les changements et réglages d'outil mineurs, ainsi que les autres interventions de maintenance légère effectuées dans le cadre des opérations de production normales, sont concernés par la norme ANSI Z244 « Mesures alternatives » s'ils ont un caractère routinier, répétitif et font partie intégrante de l'utilisation de l'équipement en production, sous réserve que ces interventions soient effectuées en utilisant des mesures alternatives de protection suffisamment efficaces. Cet aspect est pris en charge directement par l'OSHA dans le cadre de l'exception de maintenance mineure OSHA (« OSHA Minor Servicing Exception »). Ces mesures alternatives incluent l'utilisation de systèmes de protection tels que les barrières immatérielles, les tapis de sécurité, les grilles à verrouillage de sécurité et autres dispositifs de même type connectés à un système de sécurité. La question pour le concepteur de la machine ainsi que pour son utilisateur est d'apprécier ce qui est « mineur » et ce qui a un caractère « routinier, répétitif et inhérent ». Cet aspect peut être pris en compte lors de l'évaluation des risques.

La sous-partie O concerne les machines et leur protection. Cette sous-partie regroupe les exigences générales applicables à tous types de machines, ainsi que les exigences concernant certaines machines spécifiques. Lors de sa création en 1971, l'OSHA a repris de nombreuses normes ANSI existantes. Par exemple, la B11.1 concernant les presses de type mécanique a été incorporée sous le numéro 1910.217.

La 1910.212 est la norme OSHA générale pour toute les machines. Cette norme stipule qu'un ou plusieurs dispositifs de sécurité doivent être prévus sur les machines afin de protéger l'opérateur, ainsi que les autres employés se trouvant autour, des sources de danger. Sont notamment visés les dangers liés à la zone de travail de la machine, aux points de pincement, aux parties rotatives, à la projection de copeaux et d'étincelles. Des protections doivent être fixées sur la machine lorsque c'est possible ou sur un support externe ferme lorsque c'est impossible. La protection ne doit pas constituer en elle-même une source de danger. Elle doit aussi requérir un outil pour la dépose, si un tel événement nécessite le retrait de la protection.

La « zone de travail » est la partie de la machine où l'opération est effectivement réalisée sur le matériau à transformer. Lorsque les opérations réalisées sur la zone de travail d'une machine exposent le personnel à des risques de blessures, cette zone doit être protégée. Le dispositif de protection doit être conforme aux normes applicables. En l'absence de normes particulières, il doit être conçu et réalisé de façon à empêcher l'opérateur d'engager une quelconque partie de son corps dans la zone à risque pendant le cycle de fonctionnement.

La sous-partie S (1910.399) définit les exigences électriques de l'OSHA. Aux yeux du Sous-secrétariat d'état au travail, des installations ou des équipements seront recevables et homologables selon les termes de cette sous-partie S s'ils sont approuvés, homologués, listés, étiquetés ou, plus généralement, jugés comme présentant les caractéristiques de sécurité requises par un laboratoire d'essai agréé au niveau national (« nationally recognized testing laboratory » ou NRTL).

Qu'est-ce qu'un équipement ? Il s'agit d'un terme générique regroupant le matériel en lui-même, ses accessoires, ses dispositifs de contrôle, ses auxiliaires, ses supports de montage, son appareillage divers et tout ce qui entre dans le cadre d'une installation électrique ou est raccordé à une telle installation.

Qu'est-ce qui est « listé » ? L'équipement est « listé » s'il est enregistré dans une liste (a) éditée par un laboratoire NRTL réalisant des contrôles périodiques de sa fabrication et (b) spécifiant que cet équipement est conforme aux normes nationales ou qu'il a été testé et jugé comme présentant toute sécurité dans des conditions d'utilisation définies.

Depuis août 2009, les organismes suivants sont reconnus par l'OSHA comme laboratoires NRTL :

- CSA (association canadienne de normalisation)
- 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. (TUVAM)
- TÜV Product Services GmbH (TUVPSG)
- TÜV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

L'autorité compétente (AHJ) a le dernier mot sur les aspects nécessaires. Par exemple, certains états à l'instar de New York, de la Californie et de l'Illinois ont été des exigences complémentaires.

Certains états ont adopté leurs propres OSHA locales et peuvent avoir des exigences complémentaires à celles de l'OSHA de niveau fédéral. Vingt-quatre états ainsi que Puerto Rico et les îles Vierges possèdent un programme de normalisation propre à leur territoire et approuvé par l'OSHA. Ils ont en conséquence défini leurs propres normes et leurs propres règles d'application. Pour la plupart, ces états utilisent des normes identiques à celles définies par l'OSHA au niveau fédéral. Néanmoins, certains états ont adopté des normes différant sur des points particuliers ou encore des règles d'application différentes. Les employeurs doivent établir un rapport d'incidents pour l'OSHA. L'OSHA analyse statistiquement la fréquence d'incidents et transmet ces informations à ses bureaux locaux. Elles seront utilisées pour définir les priorités d'inspection. Les principaux critères de déclenchement d'une inspection sont les suivants :

- Danger imminent
- Catastrophes et décès
- Plaintes des employés
- Industries à risque élevé
- Inspections périodiques locales
- Inspections de suivi
- Programmes thématiques nationaux et locaux

Les infractions aux normes de l'OSHA peuvent entraîner des amendes. Le barème de ces amendes pour infraction est le suivant :

- infraction grave : jusqu'à 7 000 USD par infraction
- infractions autres que grave : à l'appréciation, mais ne peut excéder 7 000 USD
- Récidive : jusqu'à 70 000 USD par infraction
- Préméditation : jusqu'à 70 000 USD par infraction
- Infractions entraînant la mort : sanctions pénales
- Refus de se conformer : 7 000 USD/jour

Réglementation canadienne

Au Canada, la sécurité industrielle est gérée au niveau de la Province. Chaque province possède et applique sa propre réglementation. Par exemple, l'Ontario a promulgué sa Loi sur la santé et la sécurité au travail, qui définit les droits et obligations de tous les intervenants sur le lieu de travail. Son objectif principal est de protéger les travailleurs contre les risques professionnels ayant des implications sur leur santé et leur sécurité. Cette loi définit des procédures de gestion des risques professionnels, ainsi que des pénalités en cas de non-conformité délibérée.

On trouve par ailleurs dans cette loi le Règlement 851, dont l'Article 7 impose une inspection d'hygiène et de sécurité préalable à la mise en service d'une machine. Cette inspection est obligatoire dans la Province de l'Ontario pour tout équipement neuf, reconditionné ou modifié. Elle doit être confirmée par un rapport établi par un ingénieur professionnel.

Chapitre 2 : Normes

Ce chapitre aborde certaines des normes internationales et nationales les plus courantes concernant la sécurité des machines. Cette liste n'a pas l'ambition d'être exhaustive mais de mettre en lumière les points de sécurité des machines faisant habituellement l'objet d'une normalisation. Il est souhaitable de lire ce chapitre conjointement à celui concernant la réglementation.

Les différents pays du monde travaillent dans le sens d'une harmonisation mondiale des normes. Ceci est particulièrement évident dans le domaine de la sécurité des machines. Les normes de sécurité concernées sont régies au niveau international par deux organismes majeurs : l'ISO et la CEI. Des normes particulières existent toujours au niveau régional et national. Elles continuent de faire valoir des exigences d'application locales. Mais, dans de nombreux pays, la tendance est à la transposition des normes internationales produites par l'ISO et la CEI.

Par exemple, les normes EN (normes européennes) sont appliquées dans tous les pays de l'EEE. Or, toutes les nouvelles normes EN sont alignées sur les normes ISO et CEI et, dans la plupart des cas, elles utilisent la même formulation. De même, les États-Unis font souvent référence aux normes CEI et ISO.

Les normes CEI traitent principalement des questions électrotechniques. L'ISO s'attache aux autres aspects. La plupart des pays industrialisés adhèrent à la CEI et à l'ISO. Les normes relatives à la sécurité des machines sont écrites par des groupes de travail comprenant des experts provenant d'un grand nombre de pays industrialisés du monde.

Dans la plupart des pays, ces normes présentent un caractère d'application volontaire, alors que les réglementations constituent une obligation légale. Cependant, les normes sont généralement utilisées comme référence pratique pour les réglementations. C'est la raison pour laquelle le domaine de la normalisation est étroitement lié à celui de la réglementation.

ISO (Organisation internationale de normalisation)

L'ISO est une organisation non gouvernementale regroupant des organismes de normalisation nationaux de la plupart des pays du monde (157 à la date de publication de ce document). Son secrétariat central, situé à Genève en Suisse, coordonne le réseau. L'ISO produit des normes ayant pour but de rendre la conception, la fabrication et l'utilisation des machines plus efficace, plus sûre et plus écologique. Ces normes contribuent également à rendre les échanges internationaux plus simples et plus équitables. Les normes ISO sont identifiables par les trois lettres ISO.

Les normes ISO destinées aux machines sont réparties en trois catégories, de la même façon que les normes EN : A, B et C (voir la section relative aux normes européennes harmonisées EN, à la suite).

Pour plus d'informations, il est possible de visiter le site de l'ISO à l'adresse :*www.iso.org.*

CEI (Commission électrotechnique internationale)

La CEI établit et édite des normes internationales dont les domaines d'application sont l'électricité, l'électronique et les technologies connexes. Par l'intermédiaire de ses membres, la CEI encourage la coopération internationale sur toutes les questions de normalisation liées à l'électrotechnique ; de même que sur des sujets connexes, comme l'évaluation de la conformité aux normes électrotechniques.

Pour plus d'informations, on visitera le site de la CEI :*www.iec.ch*

Normes européennes harmonisées (EN)

Il s'agit de normes communes à tous les pays membres de l'EEE. Elles sont émises par les organismes de normalisation européens : le CEN et le CENELEC. Leur application procède d'une démarche volontaire. Néanmoins, leur utilisation pour la conception et la fabrication d'un équipement constitue le moyen le plus direct de démontrer la conformité de cet équipement aux EESS de la Directive Machines.

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

NORMES de type A : couvrent des aspects généraux applicables à tous types de machines.

NORMES de type B : se subdivisent en 2 groupes.
NORMES du Groupe B1 : concernent certains aspects particuliers de la sécurité et de l'ergonomie des machines.
NORMES du Groupe B2 : concernent les composants de sécurité et les dispositifs de protection.

NORMES Type C : concernent des types ou groupes particuliers de machines.

Il est important de noter que la conformité à une norme de la catégorie C confère automatiquement une présomption de conformité aux EESS concernées par cette norme. En l'absence d'une norme de catégorie C adaptée, on pourra recourir aux normes de catégories A et B pour démontrer partiellement ou totalement la conformité aux EESS en mettant en évidence la conformité à certains chapitres de ces normes.

Des accords de collaboration ont été conclus entre le CEN/CENELEC et d'autres organismes comme l'ISO et la CEI. Ceci devrait entraîner à terme une harmonisation des normes à l'échelle mondiale. Dans la plupart des cas, on trouve une équivalence des normes EN dans les systèmes CEI ou ISO. En général les deux textes sont identiques et les différences régionales sont mentionnées dans l'avant-propos de la norme.

Pour consulter la liste complète des normes EN relatives à la sécurité des machines, se reporter au site :

http://ec.europa.eu/growth/single-market/european-standards/

Normes des États-Unis

Normes OSHA

Dans la mesure du possible, l'OSHA promulgue des normes nationales de consensus ou des normes fédérales établies en tant que normes de sécurité. Le caractère contraignant affecté aux normes incorporées par référence (par exemple, par l'utilisation du verbe « devoir » qui implique une obligation légale), leur confère la même force légale que les normes classées en Partie 1910. C'est par exemple le cas de la norme de consensus national NFPA 70 qui est enregistrée comme document de référence dans l'Annexe A de la sous-partie S (« électricité ») de la Partie 1910 du Titre 29 CFR. La NFPA 70 est à l'origine une norme volontaire développée par la NFPA (National Fire Protection Association). Elle est également désignée par l'acronyme NEC (National Electric Code). En conséquence, toutes les dispositions obligatoires du NEC prennent force de loi sous l'effet de l'OSHA.

Normes ANSI

L'ANSI (American National Standards Institute) est l'organisme de normalisation des États-Unis. Il a pour mission d'administrer et de coordonner le système de normalisation volontaire du secteur privé aux États-Unis. C'est un organisme associatif privé, à but non-lucratif, regroupant diverses composantes des secteurs privé et public.

L'ANSI n'élabore pas lui-même les normes. Il facilite cette élaboration en favorisant le consensus entre des groupes d'experts. Il veille entre autres à ce que ces groupes d'experts respectent les principes de base du consensus ainsi qu'une méthodologie appropriée, et qu'ils fassent preuve de l'esprit d'ouverture nécessaire.
Ces normes sont classées en deux catégories : les normes d'application et les normes de construction. Les normes d'application définissent le mode de mise en œuvre d'un système de protection sur une machine. On en trouvera des exemples dans la norme ANSI B11.1, qui apporte des informations sur l'utilisation de protections sur les presses mécaniques, ainsi que dans la norme ANSI/RIA R15.06, qui décrit les dispositifs de sécurité applicables aux robots.

NFPA (National Fire Protection Association)

La NFPA (association nationale de protection contre les incendies) a été créée en 1896. Sa mission est de réduire la menace que font peser les incendies sur la qualité de vie. Pour cela elle encourage l'élaboration de codes et de normes basés sur un consensus scientifique, la recherche et la formation sur les incendies ainsi que sur les questions de sécurité connexes. La NFPA est le promoteur d'un grand nombre de normes visant à l'accomplissement de cette mission. Deux d'entre elles sont particulièrement importantes pour la sécurité industrielle : le National Electric Code (NEC) et l'Electrical Standard for Industrial Machinery (ESIM).

La NFPA a soutenu le développement du NEC depuis 1911. Le document fondateur du code date de 1897. Il est le résultat des efforts combinés de diverses parties prenantes comme les compagnies d'assurance, le secteur électrique, celui de l'architecture et d'autres encore qui s'y rattachent. Le NEC a été actualisé un grand nombre de fois depuis. En pratique, il est remis à jour environ tous les trois ans.

L'Article 670 du NEC reprend quelques aspects concernant les machines industrielles. Il renvoie notamment le lecteur à la norme NFPA 79 (ou « ESIM ») définissant les normes électriques pour les machines industrielles.

La norme NFPA 79 est applicable aux équipements, appareillages ou systèmes électriques/électroniques des machines industrielles. Elle a pour objet de définir des recommandations détaillées destinées à garantir la sécurité des personnes et des biens, concernant la mise en œuvre des équipements électriques et électroniques, des appareillages ou systèmes faisant partie intégrante des machines industrielles. Officiellement approuvée par l'ANSI en 1962, la NFPA 79 est tout à fait comparable dans son contenu à la norme CEI 60204-1.

Les machines qui ne sont pas spécifiquement concernées par les normes OSHA sont néanmoins tenues d'être exemptes de tous les risques connus susceptibles de causer la mort ou des blessures graves. Ces machines doivent être conçues et entretenues de façon à satisfaire ou surpasser les exigences des diverses normes industrielles applicables. C'est normalement la norme NFPA 79 qui s'applique à ces machines non spécifiquement concernées par les normes OSHA.

Normes canadiennes

Les normes CSA sont le reflet d'un consensus national entre les fabricants et les utilisateurs ; c'est-à-dire, entre les constructeurs, les consommateurs, les revendeurs, les syndicats, les organisations professionnelles et les agences gouvernementales. Ces normes sont largement utilisées dans l'industrie et le commerce. Elles sont souvent reprises par les administrations municipales, provinciales et fédérales dans leurs réglementations propres. C'est particulièrement le cas dans les domaines de la santé, de la sécurité, du bâtiment et de la construction, ainsi que dans celui de l'environnement.

Des particuliers, des entreprises et des associations de tout le Canada apportent leur participation à l'élaboration des normes CSA. Ils fournissent leur temps bénévolement au Comité du CSA et soutiennent les objectifs de l'association en tant que membres donateurs. Les plus de 7 000 bénévoles du Comité et les 2 000 membres donateurs constituent l'ensemble des membres du CSA.

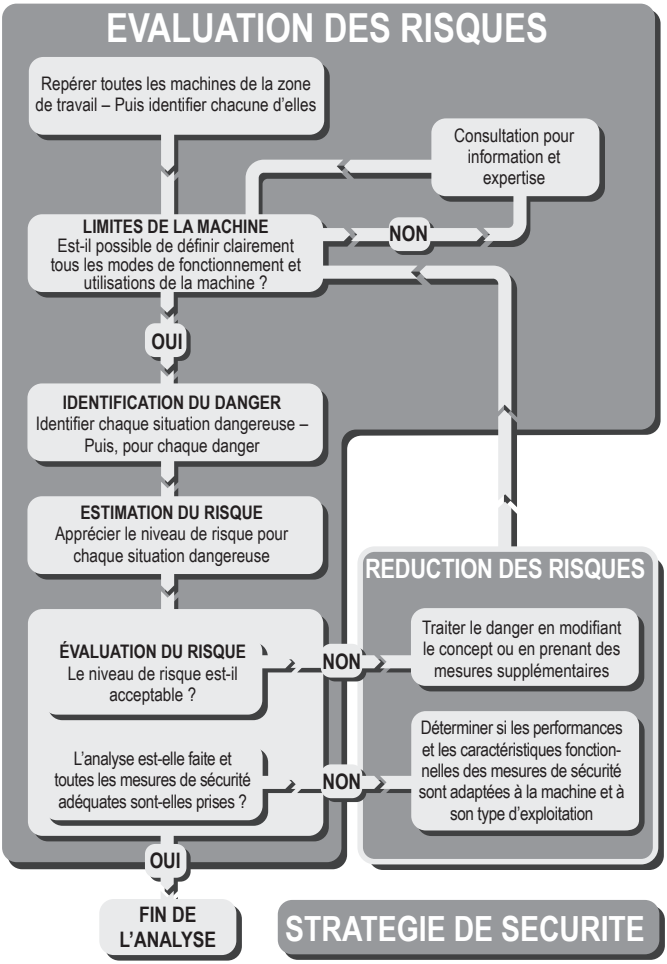
Le Conseil canadien des normes est l'organisme coordonnateur du système de normes au niveau national. Il est constitué par une fédération d'organismes indépendants et autonomes travaillant en commun pour définir et améliorer un système de normalisation volontaire dans l'intérêt national.

Normes australiennes

La plupart de ces normes sont très proches des normes ISO/CEI/EN correspondantes.
Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001
Téléphone : +61 2 8206 6000
E-mail :mail@standards.org.au – Site Internet : *www.standards.org.au*

Chapitre 3 : Stratégie de sécurité

D'un point de vue purement fonctionnel, plus une machine est performante dans l'exécution de ses tâches de transformation, meilleure elle est. Pourtant, pour qu'elle soit viable, elle doit également être sûre. La sécurité doit en effet être prise en compte de façon prioritaire.
Pour définir une stratégie de sécurité efficace, deux étapes clés et interactives sont nécessaires, comme schématisé ci-dessous.



L'ÉVALUATION DES RISQUES est basée sur la bonne compréhension des limites et des possibilités fonctionnelles de la machine. Elle doit prendre en compte également les interventions qui pourront s'avérer nécessaires sur la machine tout au long de sa vie.

La **RÉDUCTION DES RISQUES** peut alors être réalisée (si elle est nécessaire) et des mesures de sécurité sont définies à partir des informations collectées dans la phase d'évaluation des risques. Ce processus constitue la base de la STRATÉGIE DE SÉCURITÉ destinée à la machine.

Consécutivement à ce processus, une approche systématique veille à ce que tous les aspects soient pris en compte et à ce que le principe dominant ne soit pas noyé dans les détails. L'ensemble du processus doit être documenté. Ceci garantit une plus grande rigueur dans la démarche et permet également à des personnes externes d'en vérifier les résultats.

Ce chapitre s'adresse aussi bien aux constructeurs qu'aux utilisateurs de machines. Le constructeur doit s'assurer que sa machine peut être utilisée en toute sécurité. L'évaluation des risques doit commencer dès la phase de conception de la machine. Elle doit prendre en compte prévisionnellement toutes les interventions humaines qui seront susceptibles d'être réalisées sur la machine. Cette approche de prise en compte des tâches liées à l'exploitation de la machine dès le stade initial de l'évaluation des risques est très importante. Si l'on prévoit, par exemple, qu'il sera nécessaire d'effectuer régulièrement des réglages sur les parties en mouvement de la machine, il doit être possible d'anticiper les mesures qui permettront de réaliser ces opérations en toute sécurité dès la phase de conception. Si ces mesures ne sont pas intégrées dès le début, il peut s'avérer difficile, voire même impossible, de les mettre en œuvre ultérieurement. Comme il faudra de toute façon réaliser des réglages des éléments en mouvement, cette intervention risquera fort d'être effectuée dans des conditions non sécurisées ou inefficaces (ou encore, les deux). Une machine dont toutes les tâches d'exploitation potentielle auront été prises en considération dans l'évaluation des risques sera une machine plus sûre et plus performante.

L'utilisateur (ou l'exploitant) doit s'assurer que les machines dans leur environnement d'exploitation présentent toutes les garanties de sécurité. Même si une machine a été déclarée sûre par son constructeur, il est de la responsabilité de l'utilisateur de procéder tout de même à une évaluation des risques afin de déterminer si cet équipement peut être effectivement considéré comme sûr dans son environnement particulier. Les machines sont en effet souvent utilisées dans des conditions qui n'ont pas été prévues par le constructeur. Par exemple, l'utilisation d'une fraiseuse dans l'atelier d'un lycée professionnel nécessitera des précautions supplémentaires par rapport à son utilisation dans un atelier de mécanique industrielle. Il est aussi possible que des machines individuelles sûres soient combinées ensemble d'une manière telle qu'elles présenteraient alors un risque.

Il faut avoir à l'esprit également que lorsqu'un utilisateur industriel fait l'acquisition de plusieurs machines élémentaires séparées pour les intégrer dans un même processus de fabrication, il devient de fait le constructeur de la machine combinée résultant de cette intégration.

Voyons maintenant les étapes essentielles du processus de définition d'une stratégie de sécurité adaptée. La démarche suivante est applicable aussi bien dans le cadre d'un ensemble de production existant que pour une machine neuve indépendante.

Évaluation des risques

L'erreur serait de considérer l'évaluation des risques comme une contrainte. C'est en fait une procédure très utile. Elle apporte des informations d'importance vitale. Elle permet à l'utilisateur ou au concepteur de prendre des décisions rationnelles quant aux options disponibles pour assurer la sécurité de la machine.

Cette démarche est traitée dans différentes normes. La norme (EN) ISO 12100, Sécurité des machines – Principes généraux de conception – Évaluation du risque et réduction du risque, contient les recommandations les plus largement utilisées mondialement. Un rapport technique ISO : ISO/TR 14121-2 est également disponible. Il propose des recommandations pratiques et des exemples de méthodes d'évaluation des risques.

Quelle que soit la méthode utilisée pour évaluer les risques, une équipe pluridisciplinaire obtiendra généralement un résultat dont la portée sera plus large et plus nuancée qu'une personne unique.

L'évaluation des risques est un processus itératif. Il devra être renouvelé aux différentes étapes du cycle de vie de la machine. Les données à prendre en compte varieront en effet selon la phase du cycle de vie. Par exemple, le fabricant de la machine aura accès pour son évaluation des risques à tous les détails concernant les mécanismes internes et les matériaux de construction. Mais il ne pourra faire qu'une estimation approximative des conditions d'environnement finales dans lesquelles cette machine sera utilisée. L'utilisateur effectuant cette même évaluation n'aura pas, pour sa part, forcément accès aux détails techniques approfondis, mais il connaîtra parfaitement toutes les caractéristiques de l'environnement de fonctionnement de la machine. Idéalement, le résultat d'une première évaluation servira de point de départ pour la suivante.

Détermination des limites de la machine

Elle suppose la collecte et l'analyse de toutes les informations concernant les pièces, les mécanismes et les fonctions d'une machine. Il sera également nécessaire de prendre en compte les différents types d'interventions humaines sur la machine ainsi que l'environnement dans lequel elle sera utilisée. L'objectif est d'obtenir une vision claire du fonctionnement la machine et de son utilisation.

Lorsque des machines séparées se trouvent associées mécaniquement ou à travers un même système de commande, elles doivent être considérées comme une machine unique ; sauf si elle sont organisées en « zones » dans le cadre d'un dispositif de sécurité adapté.

Il est très important de prendre en compte toutes les limites et les phases du cycle de vie de la machine (installation, mise en route, maintenance, démantèlement), l'utilisation et

le fonctionnement correct ainsi que les conséquences d'une mauvaise utilisation ou d'un dysfonctionnement raisonnablement prévisible.

Identification des tâches et des dangers

Toutes les sources de danger présentées par la machine doivent être identifiées et listées par nature et emplacement. Les types de danger comprennent l'écrasement, le cisaillement, l'enchevêtrement, l'éjection de pièces, les fumées, les radiations, 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 risques. Cette démarche met en exergue les zones de convergence possibles entre un risque et une personne, par exemple une situation dangereuse. On établira alors la liste de ces situations potentiellement dangereuses. Il est possible qu'un même danger produise différents types de situations dangereuses selon la qualification des personnes ou la nature de la tâche impliquée. Par exemple, l'intervention d'un technicien de maintenance expérimenté et correctement formé peut avoir des conséquences différentes de celle d'un agent de nettoyage non qualifié et n'ayant aucune connaissance de la machine. Dans cette situation, si chacun des cas a été enregistré et traité séparément, il peut être concevable de justifier des mesures de protection différentes pour le technicien de maintenance et pour l'agent de nettoyage. Si les deux cas n'ont pas été dissociés lors de l'enregistrement et traités séparément, il conviendra de retenir le cas le plus défavorable. Le technicien de maintenance et l'agent de nettoyage bénéficieront tous deux des mêmes mesures de protection.

Parfois, il est nécessaire de réaliser une évaluation des risques sur une machine existante disposant déjà de mesures de protection (par exemple, une machine dont les parties en mouvement présentant un danger sont déjà protégées par une grille de sécurité à interverrouillage). Les parties en mouvement constituent un danger potentiel qui pourra devenir un danger réel en cas de défaillance du dispositif d'interverrouillage de sécurité. À moins que ce système d'interverrouillage de sécurité ait déjà été validé (par exemple, par une évaluation des risques ou par une conception conforme à une norme en vigueur), il sera donc ignoré.

Estimation du niveau de risque

C'est l'un des aspects les plus cruciaux du processus d'évaluation des risques. Il existe différentes façons d'aborder ce sujet. Les pages suivantes présentent les principes de base.

Toute machine exposée à des situations potentiellement dangereuses présente des risques d'évènement dangereux (par exemple, de blessure). Plus le niveau de ces risques sera élevé, plus il sera important de prendre des mesures pour y remédier. Pour certains dangers particuliers, le risque pourra être si faible qu'il sera possible de le tolérer. Mais, pour d'autres types de danger, le niveau du risque sera si élevé qu'il faudra prendre les mesures les plus draconiennes pour s'en protéger. En conséquence, pour décider à bon escient de l'opportunité et du niveau des mesures à prendre par rapport à un risque, il faut pouvoir le quantifier.

Le risque est souvent considéré uniquement du point de vue de la gravité des blessures potentielles en cas d'accident. Cependant, il convient de prendre en compte à la fois la gravité de ces blessures éventuelles ET la probabilité qu'elles surviennent pour apprécier correctement le niveau de risque existant.

ISO TR 14121-2 « Appréciation du risque – Lignes directrices pratiques et exemples de méthodes » présente différentes méthodes de quantification du risque. Il existe des différences de terminologie et de systèmes de notation, mais toutes les méthodes sont liées aux principes exposés dans la norme (EN) ISO 12100. Le texte suivant expose les principes de base de quantification du risque et vise à offrir une assistance indépendamment de la méthodologie employée. Il suit généralement les paramètres donnés par l'outil hybride au niveau de la clause 6.5 de la norme ISO TR 14121-2.

Les facteurs suivants sont pris en compte :
- LA GRAVITE DES BLESSURES POTENTIELLES.
- LA PROBABILITÉ POUR QU'ELLES SURVIENNENT.

Cette probabilité de survenance se décline en au moins deux facteurs distincts :
- LA FRÉQUENCE D'EXPOSITION.
- LA PROBABILITÉ DE BLESSURE.

Le facteur de probabilité proprement dit est souvent subdivisé en d'autres facteurs, notamment ceux qui suivent :
- PROBABILITÉ DE SURVENANCE.
- POSSIBILITÉ DE PRÉVENTION.

Il convient d'utiliser toutes les informations et expériences disponibles. Toutes les étapes du cycle de vie de la machine sont à prendre en considération. Pour éviter de rendre les décisions trop complexes, celles-ci devront donc être basées sur le cas le plus défavorable pour chaque facteur. Il faut également faire appel au bons sens. Les décisions doivent considérer ce qui est réalisable, réaliste et plausible. C'est à ce stade qu'une approche pluridisciplinaire s'avère utile.

À ce stade, vous ne devez généralement pas prendre en compte les systèmes de protection existants. Si l'estimation du niveau de risque montre qu'un système de protection s'impose, des méthodologies décrites plus loin dans ce chapitre, pourront être utilisées pour en déterminer les caractéristiques nécessaires.

Gravité des blessures potentielles

Pour cette appréciation, nous supposons que l'accident ou l'incident s'est produit. Une étude attentive du danger révélera la blessure la plus grave qu'il puisse engendrer.

Rappel : on considère pour cette appréciation que la blessure est inévitable. Seule sa gravité entre en ligne de compte. Vous présumez que l'opérateur est exposé directement au mouvement ou au processus dangereux. La gravité des blessures doit être évaluée conformément aux facteurs stipulés dans la méthodologie choisie.

Par exemple, comme suit :
- décès, perte d'un œil ou d'un bras
- effet permanent, par ex., perte de doigts.
- effet réversible nécessitant des soins médicaux
- effet réversible nécessitant des premiers soins

Fréquence d'exposition

La fréquence d'exposition exprime la périodicité selon laquelle l'opérateur ou le personnel de maintenance se trouve exposé au danger. La fréquence d'exposition aux risques peut être classifiée conformément aux facteurs stipulés dans la méthodologie choisie.

Par exemple, comme suit :
- supérieure à une fois par heure
- entre une fois par heure et une fois par jour
- entre une fois par jour et une fois toutes les deux semaines
- entre une fois toutes les deux semaines et une fois par an
- moins d'une fois par an

Probabilité de blessures

Vous présumez que l'opérateur est exposé directement au mouvement ou au processus dangereux. La probabilité d'occurrence d'un événement dangereux peut être classifiée conformément aux facteurs stipulés dans la méthodologie choisie. En prenant en compte les caractéristiques de la machine, les comportements humains escomptés et d'autres facteurs, il est possible de classifier la probabilité d'une occurrence.

Par exemple, comme suit :
- négligeable
- rare
- possible
- probable
- très élevée

Possibilité de prévention

En prenant en compte les interactions des personnes avec la machine et d'autres caractéristiques telles que la vitesse de démarrage du mouvement, la possibilité d'éviter des blessures peut être classifiée conformément aux facteurs stipulés dans la méthodologie choisie.

Par exemple, comme suit :
- probable
- possible
- impossible

Une fois toutes les rubriques traitées, les résultats sont entrés au niveau du graphique ou du tableau employé pour la quantification du risque. Il en résulte une forme d'évaluation quantifiée des risques associés aux différents dangers d'une machine. Ces informations peuvent ensuite servir à prendre des décisions sur les risques à réduire afin d'atteindre un niveau acceptable de sécurité.

Réduction de risque

Maintenant, nous devons considérer chaque machine et ses risques respectifs à tour de rôle et prendre des mesures pour faire face à tous ses dangers.

Hiérarchie des mesures de réduction de risque
Trois méthodes de base sont à considérer/utiliser, dans l'ordre de priorité suivant :

1. Éliminer ou réduire les risques le plus en amont possible (conception et construction de machines intrinsèquement sûres).
2. Mettre en place des dispositifs de protection et des mesures de protection complémentaires pour tous les risques qui ne peuvent pas être éliminés à la conception.
3. Fournir des informations pour une utilisation sûre, y compris des panneaux d'avertissement et des signaux d'alarme. De même, information concernant tout risque résiduel et la nécessité d'éventuelles formations spécifiques ou d'équipements de protection individuelle.

Chaque mesure de la hiérarchie doit être prise en compte en commençant par le haut et utilisée dans la mesure du possible. Cela entraînera habituellement l'utilisation d'une combinaison de mesures.

Élimination des risques (conception intrinsèquement sûre)

Lors de la phase de conception de la machine, il sera possible d'éviter de nombreux risques possibles en tenant soigneusement compte de facteurs comme les matériaux, les exigences d'accès, les surfaces chaudes, les méthodes de transmission, les points de piégeage, les niveaux de tension, etc.

Par exemple, s'il n'est pas nécessaire d'accéder à une zone dangereuse, la solution sera de la protéger intérieurement dans la machine ou par une quelconque enceinte de protection, fermée et fixe.

Systèmes et mesures de protection

Si l'accès est requis, alors la vie devient un peu plus difficile. Il sera nécessaire de s'assurer que l'accès ne peut être obtenu que lorsque la machine est sûre. Des mesures de protection telles que des grilles de protection interconnectées et/ou des systèmes de déclenchement seront nécessaires. Le choix du dispositif ou du système de protection à utiliser devra être majoritairement déterminé par les caractéristiques de fonctionnement de la machine. Ceci est extrêmement important car un système qui

compromet le rendement de la machine pourra lui-même faire l'objet d'enlèvement ou de contournement non autorisé.

L'une des interactions les plus impliquées et les plus complètes entre les personnes et les machines est pendant la maintenance, le dépannage et la réparation. Pour les interventions mineures et routinières, il peut être possible d'utiliser des mesures de protection axées sur les systèmes de sécurité (voir la description ci-après) pour garantir cette dernière. Mais, selon toutes les réglementations, il est parfaitement clair que pour tous les types d'interventions concernant notamment une maintenance, des réparations, un démontage ou des interventions importantes sur les circuits d'alimentation, des équipements en place doivent garantir l'isolement électrique et la dissipation de l'énergie (parfois, y compris la force gravitationnelle) sur la machine. Cela permet de réduire le risque de redémarrage intempestif et d'éliminer l'exposition à des sources d'énergie. Cet aspect est traité dans de nombreuses réglementations et normes. Par exemple, reportez-vous au texte précédent de la section « Réglementation des États-Unis », qui décrit les réglementations et normes de « condamnation/signalisation ». Les normes européennes et ISO EN 1037 et ISO 14118 « Prévention des redémarrages intempestifs » contiennent aussi des exigences en la matière. En matière de technologie électrique, les normes CEI/EN 60204-1 et NFPA 79 fournissent aussi des recommandations et exigences. Bien évidemment, il est impératif d'avoir un système de travail approprié, qui garantisse le respect de toutes les procédures correctes.

La section suivante décrit certaines mises en œuvre types.

Prévention des remises sous tension imprévisibles

La prévention des remises sous tension imprévisibles est abordée par diverses normes. C'est par exemple le cas des normes ISO 14118, EN 1037, ISO 12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 et AS 4024.1603. Ces normes ont un leitmotiv commun : la principale méthode pour empêcher toute mise sous tension imprévisible est de retirer l'énergie du système et de verrouiller le système à l'état désactivé. L'objectif est de permettre aux personnes de pénétrer en toute sécurité dans les zones dangereuses de la machine.

Condamnation/signalisation

Les nouvelles machines doivent être construites avec des dispositifs d'isolement d'énergie verrouillables. Les dispositifs s'appliquent à tous les types d'énergie, notamment électrique, hydraulique, pneumatique, gravitationnelle et les lasers. La condamnation implique le verrouillage des dispositifs de coupure d'énergie. Le verrouillage ne doit être enlevé que par son propriétaire ou par un superviseur dans des conditions contrôlées. Lorsque plusieurs personnes doivent travailler sur la machine, chaque individu doit appliquer ses verrouillages aux dispositifs d'isolement d'énergie. Chaque verrouillage doit être identifiable par son propriétaire.

Aux États-Unis, la signalisation (« tagout ») est une alternative à la condamnation (« lockout ») pour les machines anciennes qui n'ont jamais été équipées de dispositifs

de verrouillage. Dans ce cas, la machine est arrêtée et une étiquette est apposée pour prévenir tout le personnel de ne pas redémarrer la machine tant que la personne qui a apposé l'étiquette travaille sur la machine. Depuis 1990, les machines qui sont modifiées doivent être mises à niveau pour inclure un dispositif d'isolement d'énergie verrouillable.

Un dispositif d'isolation d'énergie est un dispositif mécanique qui empêche physiquement la transmission ou la libération d'énergie. Ces dispositifs peuvent prendre la forme d'un disjoncteur, d'un sectionneur, d'un interrupteur à commande manuelle, d'une combinaison fiche/prise femelle ou d'une vanne manuelle. Les dispositifs d'isolement électriques doivent commuter tous les conducteurs d'alimentation non mis à la terre et aucun pôle ne peut fonctionner indépendamment.

L'objectif de la condamnation et de la signalisation est d'empêcher un démarrage imprévisible de la machine. Un démarrage imprévisible peut être le résultat de différentes causes : une défaillance du système de commande, une action malencontreuse sur une commande de démarrage, un capteur, un contacteur ou une vanne ; la restauration de l'alimentation après une interruption, ou toutes autres causes internes ou externes. Une fois la procédure de condamnation ou de signalisation réalisée, la dissipation de l'énergie doit être vérifiée.

Systèmes d'isolation de sécurité

Les systèmes d'isolation de sécurité exécutent un arrêt automatique sans perte de données de la machine et fournissent également une méthode simple de condamnation de son alimentation. Cette approche est particulièrement adaptée pour les grandes machines et les systèmes de fabrication, notamment lorsque les sources d'énergie sont multiples et situées à un niveau supérieur ou dans un lieu éloigné.

Interrupteurs de charge

Pour l'isolement local des dispositifs électriques, des commutateurs peuvent être placés juste en amont du dispositif qui doit être isolé et verrouillé.. Les interrupteurs de charge Série 194E sont un exemple de produits capables d'assurer un tel isolement avec verrouillage.

Systèmes à clés captives

Les systèmes de clés captives sont une autre méthode pour mettre en œuvre un système de verrouillage. De nombreux systèmes de clés captives commencent par un dispositif d'isolation d'énergie. Lorsque l'interrupteur est coupé par la clé « primaire », l'énergie électrique à la machine est retirée simultanément de tous les conducteurs d'alimentation non mis à la terre. La clé primaire peut ensuite être retirée et transférée à un endroit où l'accès à la machine est nécessaire. Divers composants peuvent être ajoutés pour répondre à des besoins de condamnation plus complexes.

Mesures alternatives à la condamnation

Les procédures de condamnation et de signalisation doivent être utilisées pour le dépannage ou la maintenance des machines. Les interventions sur la machine pendant les opérations de production normales sont couvertes par des mesures de protection telles que des systèmes de grille de protection à verrouillage. La différence entre l'entretien/la maintenance et les opérations normales de production n'est pas toujours claire.

Certains réglages mineurs et tâches d'entretien, effectués dans le cadre des opérations normales de production, ne nécessitent pas nécessairement une condamnation de la machine. On citera par exemple, les chargements et déchargements de matériaux, les changements et les réglages mineurs d'outils, l'entretien des niveaux de lubrification et l'élimination des déchets. Ces tâches doivent être routinières, répétitives et intégrales à l'utilisation de l'équipement pour la production, et le travail est effectué en utilisant des mesures alternatives, comme des dispositifs de protection qui fournissent une protection efficace. Ces dispositifs de protection incluent notamment les grilles à verrouillage de sécurité, les barrières immatérielles et les tapis de sécurité. Lorsqu'ils sont utilisés avec un système logique de sécurité et des dispositifs de sortie appropriés, les opérateurs pourront accéder en toute sécurité aux zones dangereuses de la machine dans le cadre des tâches de production normales et des opérations d'entretien mineures.

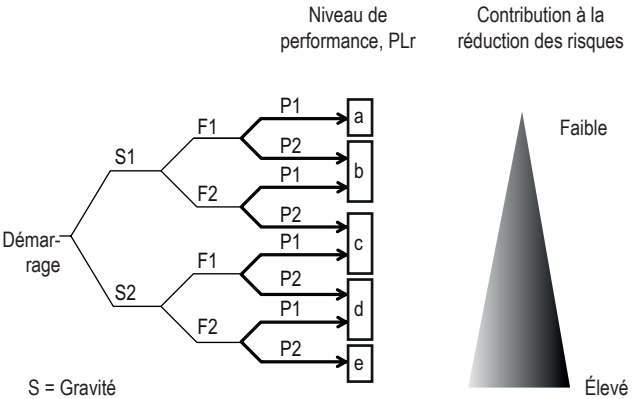
Dans ce cas, la sécurité de la machine dépendra de l'application correcte et du bon fonctionnement du système de protection même en conditions de défaut. Le bon fonctionnement du système doit maintenant être considéré. Dans chaque type, il y aura vraisemblablement un choix de technologies avec divers degrés de performance de surveillance, de détection ou de prévention des défauts.

Idéalement, chaque système de protection serait parfait sans aucune possibilité d'échouer à la survenue d'une condition dangereuse. En pratique cependant, nous sommes contraints par les limites actuelles des connaissances et des matériaux. Une autre contrainte bien réelle est le coût. Sur la base de ces facteurs, il devient évident que nous devons trouver un moyen de correler l'étendue des mesures de protection au niveau de risque obtenu à l'étape de l'estimation du risque.

Quel que soit le type de dispositif de protection choisi, il faut se rappeler qu'un « système relatif à la sécurité » peut contenir de nombreux éléments, y compris le dispositif de protection, le câblage, le dispositif de commutation de l'alimentation et parfois des parties du système de commande opérationnelle de la machine. Tous les éléments constitutifs de ce système (les dispositifs de protection, leur installation, leur câblage, etc.) doivent présenter les caractéristiques de performance requises selon leur conception et leur technologie. Les normes CEI/EN 62061 et (EN) ISO 13849-1 définissent une hiérarchie de niveaux de performance pour les composants de sécurité dans les systèmes de commande. Elles fournissent dans leurs annexes des méthodes d'évaluation des risques permettant de déterminer le niveau d'intégrité nécessaire pour les systèmes de protection.

Systèmes de commande de sécurité pour les machines

La norme (EN) ISO 13849-1:2015 propose une représentation graphique évoluée des risques dans son Annexe A.



Doit être défini pour chaque fonction de sécurité !

La norme CEI 62061 propose également dans son Annexe A une méthode d'évaluation de la forme présentée ci-dessous.

Evaluation des risques et mesures de sécurité

N° du document :

Partie de :
- ☐ Pré-évaluation des risques
- ☐ Evaluation intermédiaire des risques
- ☐ Suivi d'évaluation des risques

Produit : _____
Fourni par : _____
Date : _____

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

Conséquences	Gravité Se	Classe Cl					Fréquence et durée, Fr		Probabilité d'événement dangereux, Pr		Prévention Av	
		3–4	5–7	8–10	11–13	14–15						
Décès, perte d'un œil ou d'un bras		SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 heure	5	Défaillance	5		
Effet permanent, perte de doigts			OM	SIL 1	SIL 2	SIL 3	> 1 h – < = jour	5	Probable	4		
Effet réversible, soins médicaux				OM	SIL 1	SIL 2	>1 jour – < = 2 sem.	4	Possible	3	Impossible	5
Effet réversible, premiers soins					OM	SIL 1	> 2 sem. – < = 1 an	3	Rarement	2	Possible	3
							> 1 an	2	Négligeable	1	Probable	1

N° série	N° danger	Danger	Se	Fr	Pr	Av	Ci	Mesure de sécurité	Sûr

Commentaires

L'utilisation de l'une ou l'autre de ces méthodes doit donner des résultats équivalents. Chaque méthode est conçue pour tenir compte du contenu détaillé de la norme à laquelle elle appartient.

Dans les deux cas, il est extrêmement important que les directives fournies dans le texte de la norme soient utilisées. Le graphique ou le tableau des risques ne doivent pas être utilisés hors de ce contexte ou de façon trop simpliste.

Évaluation

Après avoir sélectionné la mesure de protection et avant de la mettre en œuvre, il est important de refaire une évaluation du risque. Cette étape de la procédure est souvent oubliée. Il se peut que si nous installons une mesure de protection, les opérateurs de la machine peuvent se sentir totalement et complètement protégé contre le risque initialement envisagé.
Parce qu'ils n'ont plus la conscience initiale du danger, ils peuvent intervenir avec la machine d'une manière différente. Ils peuvent être exposés au danger plus souvent, ou ils peuvent entrer plus loin dans la machine, par exemple. Cela signifie qu'en cas de défaillance de la mesure de protection, le risque sera encore plus grand que celui envisagé initialement. C'est ce risque réel qui doit être estimé. Par conséquent, l'estimation du risque doit être répétée en tenant compte de tout changement prévisible dans la façon dont les gens peuvent intervenir avec la machine. Le résultat de cette évaluation servira à vérifier si les mesures de protection définies sont bien adaptées dans les faits. Pour plus d'informations, il est recommandé de se reporter à l'Annexe A de la norme CEI/EN 62061.

Formation, équipement de protection individuelle, etc.

Il est primordial que les opérateurs reçoivent la formation nécessaire sur les procédures de travail sécurisé applicables à leur machine. Cela ne signifie pas que les autres mesures peuvent être omises. Il n'est pas acceptable de simplement dire à un opérateur qu'il ne doit pas s'approcher des zones dangereuses (comme alternative à la mise en place de protections).

Il peut également être nécessaire que l'opérateur utilise des équipements tels que des gants spéciaux, des lunettes de protection, des respirateurs, etc. Le concepteur de machines doit préciser quel type d'équipement est nécessaire. L'utilisation d'équipements de protection individuelle ne constitue généralement pas la première méthode de protection, mais complétera les mesures indiquées ci-dessus. Il sera aussi généralement nécessaire d'avoir des panneaux et marquages afin de faciliter la sensibilisation à tout risque résiduel.

Chapitre 4 : Mise en œuvre des mesures de protection

Lorsque l'évaluation des risques montre qu'une machine ou un procédé présente un risque de blessure, le danger doit être éliminé ou circonscrit. Le moyen d'y parvenir dépendra du type de machine et du danger. Les mesures de protection du système de commande de sécurité associées à des dispositifs de protection empêchent l'accès à un risque ou empêchent les mouvements dangereux dans une zone de danger lorsqu'elle celle-ci est accessible. Des exemples typiques de mesures de protection de système de commande de sécurité sont abordés plus loin et incluent les dispositifs de protection à verrouillage, les barrières immatérielles, les tapis de sécurité, les commandes bimanuelles et les poignées « homme mort ».

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

Interdiction d'accès par enceinte de protection fermée fixe

Si le danger se trouve dans une partie de la machine qui ne nécessite pas d'accès, une protection doit être fixée de façon permanente à la machine. La dépose de ce type de protection doit nécessiter des outils. Les protections fixes doivent pouvoir : 1) résister à leur environnement d'exploitation, 2) contenir des projectiles si nécessaire, et 3) ne pas créer de dangers en ayant par exemple des arêtes vives. Les protections fixes peuvent laisser un espace libre à l'endroit de leur raccordement à la machine, ou être ajourées du fait de l'utilisation d'un treillis métallique.

Des hublots offrent des moyens pratiques de surveillance des performances d'une machine. Le matériau des hublots devra être choisi avec soin. Les interactions chimiques avec les liquides de coupe, les rayons ultraviolets et simplement le vieillissement pourraient entraîner leur dégradation au fil du temps.

La taille des ouvertures ne doit pas permettre à l'opérateur d'atteindre la source de danger. Le tableau O-10 de la norme OHSA 1910.217 (f) (4) des États-Unis, la norme ISO 13854, le tableau D-1 de la norme ANSI B11.19, le tableau 3 de la norme CSA Z432, ainsi que la norme AS4024.1 fournissent des instructions sur la distance à respecter entre ces ouvertures et la source de danger.

Détection d'accès

Des mesures de protection peuvent être utilisées pour détecter l'accès à un danger. Lorsque la détection est choisie comme méthode de réduction des risques, le concepteur doit comprendre qu'un système de sécurité complet doit être utilisé ; le dispositif de protection seul n'assure pas la réduction des risques nécessaire. Ce système de sécurité sera généralement constitué de trois éléments principaux : 1) un dispositif d'entrée qui détecte l'accès au danger, 2) un dispositif logique qui traite les signaux provenant du capteur, contrôle l'état du système de sécurité et active ou désactive des dispositifs de sortie, et 3) un dispositif de sortie commandant l'actionneur (par exemple, un moteur).

Dispositifs de détection

De nombreux dispositifs sont disponibles pour détecter la présence d'une personne entrant ou se trouvant dans une zone dangereuse. Le meilleur choix pour une application particulière dépendra de plusieurs facteurs :

- les facteurs environnementaux susceptibles d'altérer la fiabilité du détecteur ;
- la fréquence d'accès ;
- le délai de neutralisation de la source de danger ;
- la nécessité de terminer le cycle de la machine, et ;
- le confinement des projectiles, des liquides, des brouillards, des vapeurs, etc.

Des protections mobiles correctement sélectionnées peuvent être interverrouillées pour assurer une protection contre les projectiles, les liquides, les brouillards et autres types de dangers, et sont souvent utilisées lorsque l'accès au danger est peu fréquent. Des protections interverrouillées peuvent également être verrouillées pour interdire l'accès jusqu'à l'arrêt complet de la machine ou lorsque l'arrêt de la machine au milieu d'un cycle n'est pas souhaitable.

Les dispositifs de détection de présence, tels que les barrières immatérielles, les tapis et les scrutateurs laser, permettent l'accès rapide et facile à la zone dangereuse. Ils sont souvent retenus lorsque les opérateurs doivent fréquemment accéder à la zone dangereuse. Ces types de dispositifs ne protège cependant pas contre les projectiles, les brouillards, les liquides ou autres types de danger.

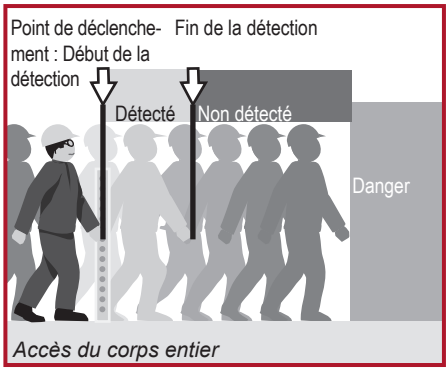
Le meilleur choix de mesure de protection est un dispositif ou un système qui fournit la protection maximale avec le minimum d'entrave au fonctionnement normal de la machine. Tous les aspects de l'utilisation de la machine doivent être pris en compte. L'expérience montre qu'un système de protection compliqué à utiliser est davantage susceptible d'être démonté ou contourné.

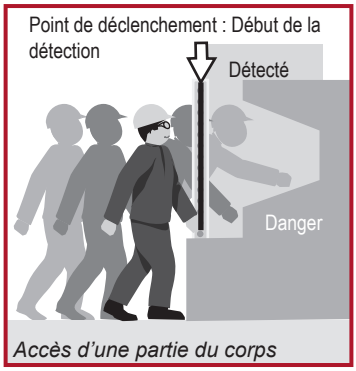
Dispositifs de détection de présence

La norme CEI 62046 fournit des recommandations utiles sur l'application des dispositifs de détection de présence. Son utilisation est recommandée. Lorsqu'on décide comment protéger une zone ou une aire, il est important de bien comprendre quelles sont les fonctions de sécurité requises. En général, il y aura au moins deux fonctions.

- Couper ou désactiver l'alimentation lorsqu'une personne pénètre dans la zone dangereuse.
- Empêcher la remise sous tension ou la réactivation de cette alimentation une fois que la personne se trouve à l'intérieur de la zone dangereuse.

À première vue, elles peuvent sembler être une seule et même chose, mais bien qu'elles soient évidemment liées, et sont souvent réalisées par le même équipement, elles sont en fait deux fonctions de sécurité distinctes. Pour réaliser la première fonction nous devons utiliser un certain type de dispositif déclencheur. Autrement dit, un dispositif qui détecte qu'une partie d'une personne a dépassé un certain point et envoie un signal de coupure de l'alimentation. Si la personne est alors en mesure de continuer au-delà de ce point de déclenchement et que sa présence n'est plus détectée alors la deuxième fonction (prévention de la remise sous tension) risquera de ne pas être assurée.





La figure présente un exemple d'accès du corps complet. Le dispositif de déclenchement est une barrière immatérielle montée verticalement. Les grilles de protection interconnectées peuvent également être considérées comme des dispositifs déclencheurs simples lorsque rien n'est prévu pour empêcher la grille d'être refermée après que la personne soit entrée dans la zone dangereuse.

Si l'accès du corps complet n'est pas possible, c'est-à-dire que la personne ne peut poursuivre au-delà du point de déclenchement, sa présence sera toujours détectée et la deuxième fonction (prévention de la remise sous tension) sera assurée. Pour les applications de détection partielle du corps, les mêmes types de dispositifs assurent le déclenchement et la détection de présence. La différence réside uniquement dans le type de l'application.

Les dispositifs de détection de présence sont utilisés pour détecter la présence de personnes. La gamme de dispositifs inclut des barrières immatérielles de sécurité, des barrières de sécurité simple faisceau, des scrutateurs laser de sécurité et des tapis de sécurité. Pour tous les dispositifs de détection de présence la taille de la zone de détection et le positionnement du dispositif doivent prendre en compte la distance de sécurité requise.

Barrières immatérielles de sécurité

Les barrières immatérielles de sécurité sont tout simplement décrites comme des détecteurs de présence photoélectriques spécialement conçus pour protéger le personnel des blessures liées au mouvement dangereux de la machine. Également appelés dispositifs de protection optoélectronique actifs (AOPD, Active Opto-electronic Protective Devices) ou équipements de protection électrosensible (ESPE, Electro Sensitive Protective Equipment), les barrières immatérielles proposent une sécurité optimale, tout en autorisant une productivité supérieure. Elles sont particulièrement adaptées aux applications dans lesquelles le personnel doit fréquemment et facilement accéder à une zone de fonctionnement dangereuse.
Les barrières immatérielles sont conçues et testées conformément aux normes CEI 61496-1 et -2.

Scrutateurs laser de sécurité

Les scrutateurs laser de sécurité utilisent un miroir pivotant qui diffuse des impulsions lumineuses sur un arc de cercle, créant ainsi un plan de détection. L'emplacement de l'objet

est déterminé par l'angle de rotation du miroir. Utilisant la technique du « temps de trajet » d'un faisceau de lumière invisible réfléchi, le scrutateur peut aussi détecter la distance qui le sépare de l'objet. En intégrant la distance mesurée et l'emplacement de l'objet, le scrutateur laser peut déterminer la position exacte de l'objet.

Tapis de sécurité sensibles à la pression

Ces dispositifs sont utilisés pour la protection d'une zone au sol autour d'une machine. Un réseau de tapis interconnectés peut être disposé tout autour de la zone dangereuse. Toute pression détectée en n'importe quel point de ce réseau (par exemple le pas d'un opérateur) entraînera la coupure de la source d'alimentation par le dispositif de contrôle du tapis. Les tapis sensibles à la pression sont fréquemment utilisés dans des zones fermées contenant plusieurs machines, par exemple des cellules de fabrication flexible ou autres applications robotiques. Lorsque l'accès à la cellule est nécessaire (pour les réglages ou la programmation du robot, par exemple), ces dispositifs empêchent les déplacements dangereux si l'opérateur s'écarte de la zone de sécurité. Il est important de prévenir tout mouvement du ou des tapis par une fixation appropriée et sûre.

Bourrelets sensibles à la pression

Ces dispositifs se présentent sous forme de bourrelets pouvant être montées sur le rebord d'une pièce mobile, telle qu'un plateau de machine ou une porte motorisée, présentant un risque d'écrasement ou de sectionnement.

Si la pièce mobile heurte l'opérateur (et inversement), le bourrelet sensible flexible sera comprimé et déclenchera une commande pour couper l'alimentation de la machine. Les bourrelets sensibles peuvent également être utilisés comme protection en cas de risque de coincement de l'opérateur. Si cela se produit, le contact avec le bourrelet sensible entraînera la coupure de l'alimentation de la machine.

Les barrières immatérielles, les scrutateurs, les tapis de sol et les bourrelets sensibles sont classés comme « dispositifs déclencheurs ». Ils n'interdisent pas l'accès. Ils se bornent à le « détecter ». Ils dépendent entièrement de leur capacité à détecter et à commuter pour assurer la sécurité. En général, ils ne sont adaptés qu'aux machines qui s'arrêtent assez rapidement après avoir coupé la source d'alimentation. Parce qu'un opérateur peut marcher et atteindre directement la zone de danger, il est évidemment nécessaire que le temps d'arrêt du mouvement soit inférieur à celui requis pour que l'opérateur atteigne le danger après le déclenchement du dispositif.

Interrupteurs de sécurité

Lorsque l'accès à la machine est peu fréquent ou lorsqu'il existe une possibilité d'éjection de pièces, il est souvent préférable d'utiliser des protections mobiles (manœuvrables). La protection est interconnecté avec la source d'alimentation de l'organe dangereux afin que cette alimentation se trouve désactivée lorsque grille de protection est ouverte.

Cette approche suppose le montage d'un interrupteur de sécurité sur la grille de protection. La commande d'alimentation de la source de danger est interfacée avec le circuit de l'interrupteur. La source d'alimentation est le plus souvent électrique, mais elle peut également être pneumatique ou hydraulique. Lorsque le mouvement (l'ouverture) de la grille de protection

est détecté, l'interrupteur de sécurité coupe la source d'alimentation, soit directement, soit par l'intermédiaire d'un contacteur de puissance (ou d'une vanne).

Certains interrupteurs de sécurité incorporent en outre un système de verrouillage qui bloque la grille en position fermée et interdit son ouverture tant que la machine n'est pas passée en condition de sécurité.

Dans la majorité des applications, l'utilisation combinée d'une protection mobile et d'un interrupteur de sécurité, avec ou sans verrouillage, constitue la meilleure solution en termes de fiabilité et de coût. La norme (EN) ISO 14119 fournit des recommandations utiles sur la sélection de tous les types de dispositifs de protection à verrouillage. Son utilisation est recommandée.

Il existe une grande variété d'interrupteurs de sécurité, notamment :

- **les interrupteurs de sécurité à broche** – ces dispositifs utilisent un actionneur en forme de broche qui est inséré ou retiré de l'interrupteur pour fonctionner ;

- **les interrupteurs de sécurité à came** – ces dispositifs se placent sur l'axe de la charnière d'une grille de sécurité et sont actionnés par son ouverture ;

- **les interrupteurs de sécurité à verrouillage** – dans certaines applications il est nécessaire de verrouiller la barrière en position fermée ou de retarder son ouverture. Les dispositifs répondant à cette exigence sont appelés interrupteurs de sécurité à verrouillage. Ils conviennent aux machines dont l'arrêt n'est pas instantané. Mais ils peuvent également apporter un niveau de protection supplémentaire à nombre d'autres types de machine.

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

- **Verrouillages de position (interrupteurs de fin de course)** – des actionneurs utilisant une came à déplacement linéaire ou rotatif constituent généralement le principe de ces interrupteurs de fin de course (ou de position) à mode positif. Ils sont généralement utilisés sur les grilles de protection coulissantes.

- **Interrupteurs à clé captive** – les clés captives peuvent servir pour le verrouillage du signal de commande comme pour le verrouillage de l'alimentation. Dans le cas d'un verrouillage du circuit de commande, l'interrupteur de verrouillage envoie une commande d'arrêt à un dispositif (relais) intermédiaire. À son tour, celui-ci agit sur un autre dispositif permettant de couper l'alimentation de l'actionneur. Dans le cas d'un verrouillage de l'alimentation, la commande d'arrêt interrompt directement la source d'alimentation des actionneurs de la machine.

Dispositifs d'interface opérateur

Fonction d'arrêt – Aux États-Unis, au Canada, en Europe et au niveau international, il existe une harmonisation des normes décrivant les catégories d'arrêt des machines ou des systèmes de fabrication.

REMARQUE : ces catégories sont différentes de celles définies par la norme ISO 13849-1. Pour des détails complémentaires, voir les normes NFPA 79 et CEI/EN 60204-1. Les arrêts sont classés en trois catégories :

La **Catégorie 0** correspond à une coupure instantanée de l'alimentation des actionneurs de la machine. On considère dans ce cas que l'arrêt n'est pas contrôlé. Une fois l'alimentation coupée, aucune action de freinage de type électrique ne pourra en effet être utilisée. Ceci se traduira par un arrêt en roue libre des moteurs jusqu'à leur immobilisation définitive qui surviendra après une période relativement longue. Dans certains cas, des produits en cours de traitement pourront tomber de la machine car ses organes internes de transfert et de maintien ne seront plus alimentés. Des moyens d'arrêt mécanique (freins), n'utilisant pas d'énergie électrique, peuvent cependant être employés dans le cadre d'un arrêt de Catégorie 0. Un arrêt de Catégorie 0 sera prioritaire sur des arrêts de Catégorie 1 ou de Catégorie 2.

La **Catégorie 1** correspond à un arrêt contrôlé avec maintien de l'alimentation sur les actionneurs de la machine pour pouvoir forcer cet arrêt. Une fois l'arrêt effectif, l'alimentation est alors coupée sur les actionneurs. Cette catégorie d'arrêt permet d'interrompre rapidement un mouvement présentant un danger en utilisant un freinage électrique, puis de couper l'alimentation des actionneurs. Cette approche peut aboutir à un arrêt plus rapide et mieux contrôlé, qui peut ensuite accélérer le redémarrage. REMARQUE : l'édition 2016 de la norme CEI/EN 60204-1 développe les types d'arrêt de Catégorie 1.

La **Catégorie 2** correspond à un arrêt contrôlé avec maintien de l'alimentation sur les actionneurs de la machine. Une procédure d'arrêt de production normale est considérée comme un arrêt de Catégorie 2.

Ces catégories d'arrêt doivent s'appliquer à chaque fonction d'arrêt. Une fonction d'arrêt désigne l'action réalisée par la partie sécurité d'un système de commande en réponse à un signal d'entrée. Seules les catégories 0 ou 1 sont concernées. Ces fonctions d'arrêt doivent être prioritaires sur les fonctions de démarrage correspondantes. Le choix de la catégorie d'arrêt à appliquer à chaque fonction d'arrêt doit être déterminé par l'évaluation des risques.

Fonction d'arrêt d'urgence

La fonction d'arrêt d'urgence doit être configurée comme un arrêt de Catégorie 0 ou 1, en fonction de l'évaluation des risques. Elle doit pouvoir être initiée par une action humaine unique. Une fois déclenchée, elle sera prioritaire sur toutes les autres fonctions et modes de fonctionnement de la machine. Son objectif est de couper l'alimentation le plus vite possible sans créer de dangers supplémentaires. Chaque fois qu'il existe un risque de danger pour les opérateurs sur une machine, celle-ci doit être munie d'un dispositif d'arrêt d'urgence facilement et rapidement accessible. Le dispositif d'arrêt d'urgence doit être opérationnel en permanence et disponible instantanément. Les pupitres opérateur doivent être équipés d'au moins un tel dispositif d'arrêt d'urgence. Des dispositifs d'arrêt d'urgence supplémentaires peuvent être implantés en d'autres endroits selon les besoins. Ces dispositifs d'arrêt d'urgence se présentent sous diverses formes. Les interrupteurs à boutons-poussoirs et les systèmes d'arrêt d'urgence à câble sont des exemples de dispositifs parmi les plus fréquemment utilisés.

Il n'y a pas si longtemps, il était encore obligatoire d'utiliser des composants électromécaniques câblés pour ces circuits d'arrêt d'urgence. Les évolutions récentes des normes, comme celles

apportées par les normes CEI 60204-1 et NFPA 79, ont introduit la possibilité d'utiliser pour le circuit d'arrêt d'urgence des automates de sécurité et autres formes de logique électronique, sous réserve qu'ils soient conformes aux normes applicables telles que la norme CEI 61508.

Les dispositifs d'arrêt d'urgence sont considérés comme des équipements de protection complémentaires. Il n'entrent pas dans la catégorie des dispositifs de protection principaux car ils n'empêchent pas l'accès à une source de danger et ne détectent pas l'intrusion dans une zone dangereuse. Ils s'appuient sur l'interaction humaine.

Pour plus d'informations sur les dispositifs d'arrêt d'urgence, il est possible de consulter les normes ISO/EN 13850, CEI 60947-5-5, NFPA 79 ou encore CEI 60204-1, AS 4024.1 et Z432-94.

Boutons-poussoirs d'arrêt d'urgence

Lorsqu'un bouton-poussoir est utilisé en guise de dispositif d'arrêt d'urgence, il doit avoir une forme de champignon, et être rouge avec un fond jaune. Lorsque le dispositif d'arrêt d'urgence est actionné, il doit rester enclenché et la commande d'arrêt ne devra pas être générée tant que ce verrouillage n'est pas réalisé. Le réarmement de ce dispositif d'arrêt d'urgence ne doit pas créer de situation dangereuse. Le redémarrage de la machine devra faire l'objet d'une action distincte et délibérée de l'opérateur.

Une nouvelle technique désormais employée avec ces dispositifs d'arrêt d'urgence est l'auto-surveillance. Un contact supplémentaire est alors rajouté à l'arrière du dispositif. Il a pour but de contrôler la présence des composants à l'arrière du panneau. On parle alors de bloc de contact à auto-surveillance. Il s'agit d'un contact actionné par un ressort qui se ferme quand le bloc de contact est mis en place sur le panneau.

Arrêts d'urgence à câble

Dans le cas de machines comme des convoyeurs, il est souvent plus pratique et plus efficace d'utiliser un système d'arrêt d'urgence à câble courant tout le long de la zone dangereuse. Ce type de dispositif utilise un câble en acier raccordé à des interrupteurs verrouillables à traction. Dès qu'une traction est exercée sur le câble dans n'importe quelle direction et en n'importe quel point de sa longueur, elle déclenche l'interrupteur qui coupe l'alimentation de la machine.

Ces dispositifs doivent être capables de détecter à la fois les tensions exercées sur le câble et sa détension. La détection de détension du câble vérifie qu'il n'est pas coupé et qu'il est opérationnel.

La longueur du câble a une incidence sur les performances du dispositif. Pour les petites longueurs, l'interrupteur de sécurité est monté à une extrémité et un ressort de tension est fixé à l'autre extrémité. Pour les grandes longueurs, un interrupteur de sécurité doit être placé à chaque extrémité du câble afin de garantir qu'une action unique de l'opérateur permette bien de déclencher la commande d'arrêt. L'utilisation de vis à œil positionnées judicieusement pour soutenir et guider le câble est essentielle. La force nécessaire de commande par câble ne doit pas excéder 200 N (45 lbs) ou une distance de 400 mm (15,75 in.) à une position centrée entre deux vis à œil. Il est important de respecter les instructions du fabricant pour obtenir des performances opérationnelles appropriées.

Commandes bimanuelles

L'utilisation de commandes nécessitant les deux mains (ou commandes bimanuelles) constitue une solution traditionnellement utilisée pour empêcher l'accès à la machine lorsque celle-ci présente un danger. Deux commandes doivent être actionnées simultanément (à moins de 0,5 secondes d'intervalle) pour pouvoir démarrer la machine. Ceci assure que les deux mains de l'opérateur sont mobilisées dans une zone sécurisée (en l'occurrence, sur les commandes). Par conséquent elles ne peuvent pas se trouver dans la zone dangereuse. Les commandes doivent être activées en continu pendant les conditions dangereuses. Le fonctionnement de la machine doit cesser dès qu'une des commandes est relâchée. Si l'une des commandes est relâchée, l'autre devra l'être également avant de pouvoir redémarrer la machine. Cela constitue un « anti-contournement » et évite que la commande à deux mains soit transformée en commande à une main.

Un système bimanuel est très largement tributaire de la rigueur de détection des défauts par son système de commande et de surveillance. Il est de ce fait essentiel que des réquisitions très précises aient été définies pour cela lors de la conception de ce système. Les performances d'un système de sécurité bimanuel sont classées par types selon la norme ISO 13851 (EN 574). Comme on le voit dans le tableau ci-dessous, ces types sont eux-même rattachés aux Catégories de la norme ISO 13849-1. Les types les plus courants en matière de sécurité des machines sont les types IIIB et IIIC. Le tableau suivant montre les relations existant entre les types et les catégories de performance de sécurité.

Exigences	Types				
	I	II	III		
			A	B	C
Actionnement synchrone			X	X	X
Utilisation de la Catégorie 1 (selon l'ISO 13849-1)	X		X		
Utilisation de la Catégorie 3 (selon l'ISO 13849-1)		X		X	
Utilisation de la Catégorie 4 (selon l'ISO 13849-1)					X

Tableau des exigences de la norme ISO 13851

L'organisation ergonomique du pupitre doit empêcher toute manœuvre inappropriée (actionnement par la main et le coude, par exemple). Ceci peut être obtenu par un espacement adapté ou par des écrans de séparation. La machine ne doit pas pouvoir enchaîner deux cycles consécutifs sans que les deux boutons de commande aient d'abord été relâchés puis actionnés à nouveau. Ceci fournit une fonction « anti-répétition » et est destiné à empêcher le blocage simultané des deux boutons afin de laisser tourner la machine en continu. Le relâchement de l'un des deux boutons doit entraîner l'arrêt de la machine.

L'utilisation d'une commande bimanuelle doit être envisagée avec discernement car elle n'écarte généralement pas tous les risques existants. La commande bimanuelle ne protège d'autre part que la personne qui l'utilise. Cet opérateur doit donc être à même de surveiller tous les accès à la zone dangereuse, les autres personnes ne bénéficiant pas nécessairement d'une protection.

La norme ISO 13851 (EN 574) fournit des recommandations supplémentaires concernant les commandes bimanuelles.

Poignées de sécurité

Les poignées de sécurité sont des commandes qui font parfois partie d'une stratégie d'autorisation qui permet à un opérateur de pénétrer dans une zone dangereuse alors que le moteur dangereux fonctionne à une vitesse de sécurité, ce uniquement si l'opérateur maintient la commande de la poignée de sécurité en position d'activation. Ces poignées de sécurité peuvent utiliser des interrupteurs à deux ou trois positions. Les interrupteurs à deux positions sont désactivés lorsqu'ils ne sont pas actionnés et activés lorsqu'ils sont actionnés. Les interrupteurs à trois positions sont désactivés lorsqu'ils ne sont pas actionnés (position 1), sont activés lorsque leur actionneur est maintenu en position centrale (position 2) et sont désactivés lorsque l'actionneur est poussé au-delà de la position médiane (position 3). De plus, lors du retour de la position 3 à la position 1, le circuit de sortie ne doit pas se refermer lors du passage par la position 2.

Ces poignées de sécurité doivent être utilisées en parallèle à d'autres fonctions de sécurité. Un exemple type de leur application est le passage du mouvement en fonctionnement lent sécurisé. Lorsqu'une poignée de sécurité est utilisée, un signal doit indiquer qu'elle est active.

Dispositifs logiques

Les dispositifs logiques jouent un rôle central dans la partie sécurité du système de commande. Ces dispositifs assurent le contrôle et la surveillance du système de sécurité et autorisent le démarrage de la machine ou l'exécution des commandes d'arrêt de cette machine.

Il existe toute une gamme de dispositifs logiques permettant de créer une architecture de sécurité adaptée à la complexité et aux fonctionnalités requises par la machine. Des petits relais de surveillance de sécurité câblés seront plus économiques pour les petites machines sur lesquelles un dispositif logique dédié simple est nécessaire pour assurer la fonction de sécurité. Des relais de surveillance de sécurité modulaires et configurables seront préférables dans le cas où des dispositifs de protection variés et nombreux, ainsi qu'une commande de zone minimale, sont requis. Pour les machines de taille moyenne à grande, ainsi que pour celles présentant encore plus de complexité, les systèmes de sécurité programmables avec E/S distribuées seront les mieux adaptés.

Relais de surveillance de sécurité (MSR)

Les modules de surveillance de sécurité à relais de type MSR (monitoring safety relay) jouent un rôle clé dans de nombreux systèmes de sécurité. Ces modules sont généralement composés de plusieurs relais à guidage réciproque et d'un circuit complémentaire destiné à assurer l'exécution de la fonction de sécurité.

Les relais à guidage réciproque ont pour fonction d'empêcher les contacts normalement fermés et normalement ouverts d'être fermés simultanément. Certains relais de surveillance de sécurité ont des sorties de sécurité statiques.

Les relais de surveillance de sécurité réalisent diverses vérifications du système de sécurité. A la mise sous tension, ils effectuent un auto-contrôle de leurs composants internes. Lorsque les dispositifs d'entrée sont activés, le relais MSR compare l'état des entrées redondantes. S'il est conforme, le relais MSR vérifie les actionneurs externes connectés à ses sorties. Si le résultat est positif, le relais attend alors un signal de réinitialisation pour activer ses sorties. Par conséquent, un relais MSR sélectionné et configuré correctement peut fournir une détection des défauts système en contrôlant ses dispositifs d'entrée et de sortie connectés. Il peut également fournir un verrouillage du démarrage/redémarrage.

Le choix du relais de sécurité approprié dépend de plusieurs facteurs : le type des dispositifs contrôlés, le type de réinitialisation effectuée, le nombre et le type de sorties, etc.

Types d'entrées fournis au relais de surveillance de sécurité (MSR)

Différents types de dispositifs de protection fournissent différents types d'entrées à un relais de surveillance de sécurité, de sorte qu'un contrôle de compatibilité est important. Vous trouverez ci-après un résumé succinct des types d'entrées possibles et des caractéristiques de détection d'erreurs de croisement nécessaires.

Dispositifs de verrouillage électromécaniques, certains dispositifs de verrouillage sans contact et arrêts d'urgence : contacts mécaniques mono-voie avec un contact normalement fermé, ou à deux voies normalement fermées. Le relais MSR doit pouvoir accepter une ou deux voies et permettre la détection des erreurs de croisement sur les systèmes à deux voies.

Certains dispositifs de verrouillage sans contact et arrêts d'urgence : contacts mécaniques, deux voies, un contact normalement ouvert et un normalement fermé. Le relais MSR doit être capable de traiter des entrées complémentaires.

Dispositifs avec sorties statiques : Les barrières immatérielles, les scrutateurs laser et certains dispositifs de verrouillage de protection sans contact ont deux sorties PNP et exécutent leur propre détection d'erreur de croisement. Le relais MSR doit être capable d'ignorer la procédure de détection des erreurs de croisement du dispositif.

Tapis sensibles à la pression : ces tapis créent un court-circuit entre deux voies. Le relais MSR doit être spécialement conçu ou configurable pour cette application.

Bourrelets sensibles à la pression : certains bourrelets sont conçus de la même façon que les tapis à 4 fils. Certains autres utilisent un dispositif à deux fils qui crée une variation de résistance dans le circuit. Le relais MSR doit être capable de détecter un court-circuit ou une variation de résistance.

Détection de mouvement de moteur : elle mesure la FCEM d'un moteur pendant la décélération. Le relais MSR doit être capable de supporter des tensions élevées, mais aussi de détecter les basses tensions lorsque le moteur décélère.

Mouvement arrêté : le relais MSR doit être capable de détecter les flux d'impulsions provenant de capteurs divers et redondants.

Commande bimanuelle : le relais MSR doit être capable de détecter les entrées complémentaires normalement ouvertes et normalement fermées. Il doit pouvoir assurer également une temporisation de 0,5 s ainsi qu'un séquencement logique.

Les relais de surveillance de sécurité doivent être conçus ou être configurables spécifiquement pour s'interfacer avec chacun de ces types de dispositifs aux caractéristiques électriques différentes. Certains relais MSR sont complètement configurables en différents types. Certains relais MSR ont la possibilité de recevoir différents types d'entrées. Mais une fois qu'un dispositif particulier est sélectionné, le relais ne pourra dialoguer qu'avec lui. Le concepteur doit sélectionner ou configurer un relais MSR compatible avec le dispositif d'entrée.

Impédance d'entrée

L'impédance d'entrée des relais de surveillance de sécurité détermine le nombre de capteurs pouvant être raccordés au relais et la distance jusqu'à laquelle ils peuvent être montés. Par exemple, un relais de sécurité aura une impédance d'entrée maximale autorisée de 500 ohms. Lorsque l'impédance d'entrée sera supérieure à 500 ohms, les sorties ne seront pas activées. L'utilisateur doit donc veiller à ce que l'impédance d'entrée reste inférieure à la valeur maximum spécifiée. La longueur, la section et le type du câblage utilisés affectent l'impédance d'entrée.

Nombre de dispositifs d'entrée

La procédure d'évaluation des risques sera utilisée pour déterminer le nombre de dispositifs d'entrée à raccorder à un relais MSR, ainsi que la fréquence de vérification de ces dispositifs d'entrée. Pour s'assurer que les arrêts d'urgence et les dispositifs de verrouillage de grille sont toujours opérationnels, leur bon fonctionnement doit être contrôlé régulièrement, suivant la fréquence définie lors de l'évaluation des risques. Par exemple, une entrée de relais MSR à deux voies raccordée à une grille de protection à verrouillage de sécurité devant être ouverte à chaque cycle de la machine (c'est-à-dire plusieurs fois par jour) ne justifiera pas nécessairement un contrôle spécifique. La raison en est que l'ouverture de la grille de protection déclenchera l'auto-contrôle par le relais de ses entrées et de ses sorties (selon la configuration) afin de détecter tout éventuel défaut individuel. Plus la grille de protection sera ouverte fréquemment, plus la rigueur de la procédure de contrôle sera élevée.

Les arrêts d'urgence constituent un autre exemple. Étant, par définition, utilisés principalement en cas d'urgence, ils sont susceptibles d'être beaucoup moins sollicités. C'est pourquoi leur bon fonctionnement devra être vérifié suivant un programme de test prévoyant leur actionnement à intervalles réguliers. Ce type de test du système de sécurité est appelé test fonctionnel. Un troisième exemple peut être les portes d'accès pour les réglages de machine. À l'instar des arrêts d'urgence, ces portes peuvent être rarement employées. Là encore, un programme doit être élaboré afin de tester régulièrement le fonctionnement.

L'évaluation des risques permet de déterminer si les capteurs concernés ont besoin d'être contrôlés et à quelle fréquence. Plus le niveau de risque est élevé, plus les exigences seront importantes pour cette procédure de contrôle. Par ailleurs, moins la fréquence des contrôles « automatiques » sera élevée, plus on devra s'imposer des contrôles « manuels » fréquents.

Détection d'erreurs de croisement d'entrée

Dans les systèmes à deux voies, les défauts de courts-circuits entre les voies des dispositifs d'entrée, également appelés erreurs de croisement, doivent être identifiés par le système de sécurité. Cette fonction est réalisée soit par le capteur, soit par le relais de surveillance de sécurité.

Les relais de surveillance de sécurité utilisant des microprocesseurs, par exemple les barrières immatérielles, les scrutateurs laser et les capteurs sans contact évolués, peuvent détecter ces courts-circuits de différentes façons. Une méthode classique de détection de ces erreurs de croisement consiste à effectuer un contrôle par impulsions. La fréquence d'impulsion des signaux d'entrée au relais MSR est très élevée. Les impulsions de la voie 1 sont décalées par rapport à celles de la voie 2. Si un court-circuit se produit, ces impulsions deviennent simultanées, ce qui peut être détecté par le dispositif.

Les relais de surveillance de sécurité électromécanique utilisent une technique de contrôle différentiel différente : ils contrôlent une entrée à enclenchement et une entrée à déclenchement. Un court-circuit entre la voie 1 et la voie 2 actionnera le dispositif de protection contre les surintensités et le système de sécurité arrêtera la machine.

Sorties

Les relais de surveillance de sécurité peuvent avoir un nombre varié de sorties. Le types de ces sorties permet de déterminer le relais MSR à utiliser pour chaque application particulière.

La plupart des relais MSR possèdent au moins 2 sorties de sécurité à fonctionnement instantané. Les sorties de sécurité de ces relais sont caractérisées comme normalement ouvertes. Elles sont par ailleurs considérées comme sorties de sécurité du fait de leur fonctionnalités de redondance et d'auto-contrôle interne. Les sorties temporisées constituent un second type de sortie. Les sorties d'arrêt temporisé sont généralement utilisées pour les arrêts de Catégorie 1, lorsque la machine a besoin d'un certain temps pour exécuter sa fonction d'arrêt avant d'autoriser l'accès à la zone dangereuse. Les relais MSR possèdent également des sorties auxiliaires. Celles-ci sont généralement définies comme normalement fermées.

Puissance de sortie nominale

Les caractéristiques de puissance de sortie nominales indiquent la capacité de commutation de charge d'un dispositif de protection. Habituellement, dans le cas de dispositifs industriels, ces puissances sont définies pour des circuits résistifs ou électromagnétiques (inductifs). Une charge résistive pourra, par exemple, être constituée par un élément chauffant. Les charges électromagnétiques sont généralement constituées par des relais, des contacteurs ou des électroaimants présentant un fort caractère inductif. L'annexe A de la norme CEI 60947-5-1 décrit les caractéristiques des différentes charges.

Code d'identification : Le code d'identification est constitué d'une lettre suivie d'un chiffre, par exemple A300. La lettre se rapporte à l'intensité thermique conventionnelle en boîtier fermé et indique si ce courant est continu ou alternatif. Dans l'exemple, la lettre A indique un courant alternatif de 10 ampères. Le chiffre indique la tension d'isolation assignée. Dans l'exemple, 300 représente 300 V.

Usage : Les catégories d'usage désignent les types de charges que le dispositif peut commuter. Les catégories d'usage selon la norme CEI 60947-5 sont répertoriées dans le tableau suivant.

Usage	Description de la charge
AC-12	Commande de charges résistives et statiques avec isolement par opto-coupleurs
AC-13	Commande de charges statiques avec isolement 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 statiques avec isolement par opto-coupleurs
DC-13	Commande d'électroaimants
DC-14	Commande de charges électromagnétiques pourvues de résistances de limitation dans leur circuit

Intensité thermique, Ith : l'intensité thermique conventionnelle en boîtier fermé correspond à la valeur de courant utilisée pour les essais d'échauffement de l'équipement monté dans un boîtier particulier.

Tension Ue et courant le de fonctionnement assignés : Le courant et la tension de fonctionnement assignés spécifient les capacités de fermeture et d'ouverture des éléments de coupure dans des conditions normales de fonctionnement. Les produits Allen-Bradley Guardmaster sont généralement conçus pour 125 V c.a., 250 V c.a. et 24 V c.c.

VA : les caractéristiques VA (Volt-Ampère) définissent la puissance apparente nominale de commutation, à la fermeture comme à l'ouverture du circuit.

Exemple n° 1 : une classification A150, AC-15 indique que les contacts peuvent fermer un circuit de 7200 VA. Sous 120 V c.a., ces contacts pourront fermer un circuit avec un courant d'appel de 60 A. AC-15 faisant référence à une charge électromagnétique, ces 60 A ne s'appliqueront que pendant une courte durée. Ils correspondent donc au courant d'appel de la charge électromagnétique. La puissance de coupure du circuit n'est que de 720 VA, car l'intensité de la charge inductive en régime établi est de 6 A. Cette valeur constitue l'intensité de service nominale.

Exemple n° 2 : une classification N150, DC-13 indique que les contacts peuvent fermer un circuit de 275 VA. Sous 125 V c.a., ces contacts pourront fermer un circuit de 2,2 A. En courant continu, il n'existe pas de courant d'appel pour les charges électromagnétiques, comme en courant alternatif. La coupure du circuit interviendra également à 275 VA, car l'intensité de la charge électromagnétique en régime établi est de 2,2 A. Cette valeur constitue l'intensité de service nominale.

Redémarrage de la machine

Si, par exemple, une grille de protection à verrouillage de sécurité est ouverte alors que la machine est en fonctionnement, le contacteur d'interverrouillage provoquera son arrêt. Dans la plupart des cas, il sera impératif que la machine ne puisse pas redémarrer directement sitôt la grille refermée. Un moyen classique de réaliser cela consiste à utiliser un système de démarrage à contacteur à verrouillage.

L'appui et le relâchement du bouton de démarrage excite momentanément la bobine de commande du contacteur, laquelle ferme les contacts d'alimentation. Tant que ces contacts d'alimentation seront fermés, la bobine de commande restera alimentée (verrouillée électriquement) par l'intermédiaire des contacts auxiliaires du contacteur qui sont couplés mécaniquement aux contacts d'alimentation. Toute interruption de l'alimentation électrique principale ou du système de commande entraînera la désactivation de la bobine et l'ouverture des contacts d'alimentation principale et des contacts auxiliaires. Le système d'interverrouillage de la grille de protection est relié au circuit de commande du contacteur. Cela implique que pour redémarrer la machine, il faudra refermer la grille puis réactiver le bouton de démarrage normal destiné à réarmer le contacteur et à démarrer la machine.

La nécessité de situations de verrouillage normales est clarifiée par la norme ISO 12100 (extrait) :

« Lorsque la grille est en position fermée, le fonctionnement à caractère dangereux de la machine par rapport auquel elle assure sa protection, peut se dérouler. Mais la fermeture de la grille ne peut pas, en elle-même, l'initier. »

Un grand nombre de machines sont dotées de contacteurs simples ou doubles, ayant un fonctionnement identique à celui décrit précédemment (ou utilisent un système permettant d'obtenir le même résultat). Lorsqu'on installe un dispositif d'interverrouillage de sécurité sur une machine existante, il est nécessaire de déterminer si le système d'alimentation de commande électrique est compatible avec ses caractéristiques. Au besoin, il faudra mettre en place des mesures d'adaptation complémentaires.

Fonctions de réarmement

Les relais de surveillance de sécurité Guardmaster Allen-Bradley sont conçus soit avec un réarmement manuel surveillé, soit avec un réarmement automatique/manuel.

Réarmement manuel surveillé

Le réarmement manuel surveillé nécessite que l'état du circuit de réarmement soit modifié après la fermeture de la grille ou le réarmement de l'arrêt d'urgence. Les contacts auxiliaires normalement fermés à couplage mécanique des commutateurs d'alimentation sont branchés en série avec un bouton-poussoir à impulsion. Lorsque la grille a été ouverte, puis refermée, le relais de sécurité n'autorisera pas le redémarrage de la machine tant qu'il n'y a pas eu de changement d'état de ce bouton de réarmement. Ceci est conforme à l'esprit des exigences de réarmement manuel supplémentaire

définies par la norme (EN) ISO 13849-1. Concrètement, la fonction de réarmement doit garantir que les deux contacteurs sont à l'état OFF et que les deux circuits de verrouillage (et donc les dispositifs de protection) sont fermés. Elle doit également garantir que l'actionneur de réarmement n'a pas été, de quelque façon, contourné ou bloqué (puisqu'un changement de son état est obligatoire). Si ces tests sont positifs, la machine pourra être redémarrée normalement. La norme (EN) ISO 13849-1 cite le changement d'état comme le passage de l'état activé à l'état désactivé ('front descendant').

L'interrupteur de réarmement devra être placé en un point permettant à l'opérateur d'avoir une bonne visibilité sur la source du danger. Ainsi, il pourra vérifier que la zone est totalement dégagée avant la remise en route.

Réarmement automatique/manuel

Certains relais de sécurité sont dotés d'un réarmement automatique/manuel. Le mode de réarmement manuel n'est pas surveillé et le réarmement se produit lorsqu'on appuie sur le bouton de démarrage. Un tel interrupteur de réarmement ne sera pas détecté comme étant en court-circuit ou coincé. Cette approche ne permet donc pas a priori de répondre aux exigences de réarmement manuel supplémentaire définies par la norme (EN) ISO 13849-1, à moins d'avoir recours à des dispositifs complémentaires.

De même, le circuit de réarmement pourra être ponté, permettant un réarmement automatique direct. L'utilisateur doit alors prévoir un autre mécanisme pour empêcher le redémarrage de la machine lors de la fermeture de la grille.

Un dispositif à réarmement automatique ne nécessite aucune action (interrupteur) supplémentaire. Néanmoins, après désactivation du système, il contrôlera systématiquement l'intégrité de celui-ci avant de procéder au réarmement. Un système à réarmement automatique ne doit pas en effet être confondu avec un dispositif dépourvu de toutes fonctionnalités de réarmement. Dans ce dernier cas, le système de sécurité sera directement remis en service après sa désactivation, mais il n'y aura pas de contrôle de son intégrité.

L'interrupteur de réarmement devra être placé en un point permettant à l'opérateur d'avoir une bonne visibilité sur la source du danger. Ainsi, il pourra vérifier que la zone est totalement dégagée avant la remise en route.

Protection à commande directe

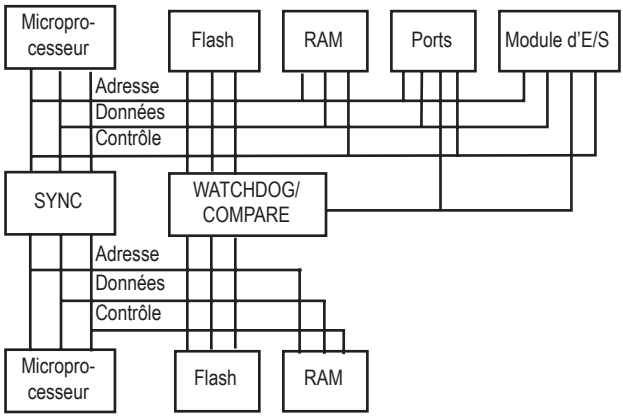
Une protection à commande directe arrête la machine lorsque la grille est ouverte. Elle la redémarre directement dès que la grille est refermée. L'emploi de ces protections à commande directe n'est permis que dans des conditions très restreintes. Elles ne peuvent en effet empêcher les redémarrages intempestifs, ni les défaillances dans la procédure d'arrêt, ce qui peuvent s'avérer extrêmement dangereux. Le système d'interverrouillage doit présenter le plus haut niveau de fiabilité possible (il est le plus souvent recommandé d'utiliser un dispositif de verrouillage de grille). L'emploi de telles

protections à commande directe ne peut être envisagé que sur des machines n'offrant aucune possibilité aux opérateurs d'introduire tout ou partie de leur corps dans la zone dangereuse lorsque la protection est fermée. Le dispositif de protection à commande directe doit alors être la seule voie d'accès possible à la zone dangereuse.

Systèmes de commande logique programmables de sécurité

Le besoin de flexibilité et d'évolutivité dans les applications de sécurité a conduit au développement d'automates ou automates programmables de sécurité. Les automates programmables de sécurité apportent aux utilisateurs le même niveau de flexibilité dans le système de commande des applications de sécurité que celui auquel ils sont habitués avec leurs automates programmables standard. Il existe cependant des différences importantes entre les automates standard et de sécurité. Les automates de sécurité sont disponible sous différentes plates-formes afin de répondre aux exigences d'évolutivité, d'intégration et de fonctionnalité des systèmes de sécurité les plus complexes.

Des microprocesseurs multiples sont utilisés en redondance pour gérer les E/S, la mémoire et les communications de sécurité. Des circuits de surveillance interne (« chiens de garde ») effectuent les diagnostics et leur analyse. Ce type d'architecture est désigné par « 1oo2D » (l'un ou l'autre des deux). L'un ou l'autre des deux microprocesseurs peut en effet prendre en charge la fonction de sécurité. Des diagnostics étendus sont par ailleurs réalisés afin de s'assurer que ces deux microprocesseurs travaillent de façon parfaitement synchronisée.



Architecture 1oo2D

Chaque circuit d'entrée est également contrôlé en interne selon une fréquence très élevée afin de vérifier qu'il fonctionne correctement. Il se peut que vous n'activiez l'arrêt d'urgence qu'une fois par mois mais, dans ce cas, le circuit interne a été testé en permanence.

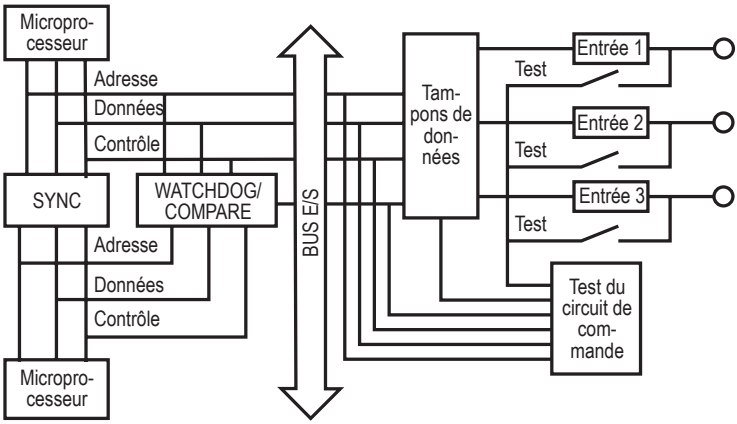


Schéma de principe d'un module d'entrées de sécurité

Les sorties des automates de sécurité peuvent être de type électromécaniques ou statiques de sécurité. Comme les circuits d'entrée, les circuits de sortie sont contrôlés en interne selon une fréquence très élevée afin de garantir qu'ils pourront couper la sortie concernée sans problème lorsque nécessaire. Si l'un des trois circuits est défectueux, sa sortie sera interrompue par les deux autres et le défaut sera signalé par le circuit de surveillance interne. Lorsque des dispositifs de sécurité à contacts mécaniques sont employés (arrêts d'urgence, interrupteurs de grille, etc.), l'utilisateur peut réaliser un test par impulsions pour détecter les erreurs de croisement.

Logiciel

Les automates de sécurité se programment d'une façon très semblable aux automates standard. Tous les diagnostics complémentaires et les recherches de défauts mentionnés plus haut sont réalisés par le système d'exploitation. Le programmeur n'aura donc même pas conscience de ces opérations. La plupart des automates de sécurité possèdent un jeu d'instructions spécial servant à écrire le programme du système de sécurité. Ces instructions tendent à reproduire les fonctions qui seraient réalisées par un système à relais de sécurité équivalent. Par exemple, le fonctionnement de l'instruction d'arrêt d'urgence est très similaire à un relais MSR. 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 les autres instructions logiques, mathématiques, de manipulation de données, etc., sont certifiées par un organisme externe afin de s'assurer que leur fonctionnement est cohérent avec les normes en vigueur.

Les blocs fonctionnels constituent la méthode principale utilisée 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 certifiées pour les applications de sécurité. Ces instructions de sécurité certifiées permettent de programmer des comportements particuliers de l'application.

Il existe des blocs fonctionnels certifiés adaptés à pratiquement tous les dispositifs de sécurité. Une exception à cette règle est cependant constituée par les bourrelets de sécurité utilisant la technologie résistive.

Les automates de sécurité génèrent par ailleurs une « signature » qui permet de suivre les modifications apportées au système. Cette signature englobe généralement une information sur le programme ainsi que sur la configuration des entrées et des sorties et un horodatage. Lorsque le programme est finalisé et validé, l'utilisateur doit enregistrer cette signature avec les résultats de validation afin de pouvoir s'y reporter ultérieurement. Si le programme doit être modifié, une nouvelle validation sera nécessaire et une nouvelle signature devra être enregistrée. Le programme peut également être verrouillé par un mot de passe afin d'empêcher toute modification non autorisée.

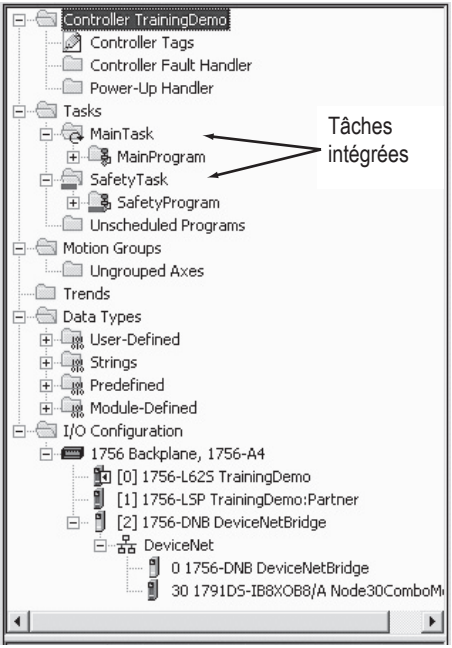
Avec les systèmes à logique programmable, le câblage se trouve simplifié par rapport aux systèmes à relais de surveillance de sécurité. Contrairement aux systèmes câblés qui nécessitent le raccordement à des bornes spécifiques sur les relais de surveillance de sécurité, les dispositifs d'entrée peuvent être connectés à n'importe quelle borne d'entrée de sécurité, de même que les dispositifs de sortie peuvent être connectés à n'importe quelle borne de sortie de sécurité. Ces bornes seront ensuite affectées par le logiciel.

Automates à sécurité intégrée

Les solutions de commande modernes permettent désormais une intégration totale dans une architecture de commande unique faisant cohabiter les fonctions de commande de sécurité et celles de commande standard. La possibilité de réaliser une commande de mouvement, de variation de vitesse, de processus, de traitement par lots ou encore séquentielle à grande vitesse, simultanément à une commande de sécurité de niveau SIL 3 sur un seul et même automate procure des avantages significatifs. L'intégration des commandes standard et de sécurité permet l'utilisation de technologies et d'outils communs. Ceci réduit les coûts de conception, d'installation, de mise en service et de maintenance. La possibilité d'utiliser des accessoires de commande communs, des E/S ou des dispositifs de sécurité distribués sur des réseaux de sécurité, ainsi que des dispositifs d'IHM communs, permet de réduire les coûts d'acquisition et de maintenance, de même que les temps de développement. Toutes ces fonctionnalités augmentent la productivité et la rapidité d'intervention des dépannages. Elles réduisent par ailleurs les coûts de formation grâce à la standardisation.

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

Toutes ces fonctions standard et de sécurité sont isolées les unes des autres. Par exemple, les points de sécurité peuvent être lus directement par le programme standard. Ces points de sécurité peuvent être échangés entre des automates GuardLogix sur EtherNet/IP, ControlNet ou DeviceNet. Les données des points de sécurité peuvent être lues directement par des dispositifs externes, des interfaces homme-machine (IHM), des ordinateurs personnels (PC) ou d'autres automates.



1. Les points et la logique standard se comportent de la même façon qu'avec un automate ControlLogix standard.

2. Les données des points standard, qu'elles soient de type programme ou automate, peuvent être lues par des dispositifs externes, des IHM, des PC, d'autres automates, etc.

3. En tant qu'automate intégré, GuardLogix permet de déplacer (« mapper ») des données de points standard sur des points de sécurité pour les utiliser dans une tâche de sécurité. Les utilisateurs peuvent ainsi vérifier leurs informations d'état depuis le côté standard du GuardLogix. Ces données ne doivent cependant pas être utilisées pour commander directement une sortie de sécurité.

4. Les points de sécurité peuvent être lus directement 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/IP.

7. Les données de points de sécurité, qu'elles soient de type programme ou automate, peuvent être lues par des dispositifs externes, des IHM, des PC, d'autres automates, etc. À noter qu'une fois ces données employées en dehors de la tâche de sécurité, elles sont considérées comme des données standard, non plus comme des données de sécurité.

Réseaux de sécurité

L'utilisation des réseaux de communication en production permet depuis longtemps aux fabricants d'améliorer leur flexibilité, d'augmenter les diagnostics, d'accroître les distances, de réduire les coûts d'installation et de câblage, de faciliter la maintenance et plus généralement d'améliorer la productivité. Ces mêmes objectifs ont également été le moteur du déploiement des réseaux de sécurité industriels. Ces réseaux de sécurité permettent aux fabricants d'implanter des E/S et des dispositifs de sécurité tout autour de leurs machines en les reliant simplement par un unique câble réseau, pour les communications d'E/S de sécurité et standard. Cette approche limite les coûts d'installation tout en améliorant le diagnostic et en permettant une sophistication plus grande des systèmes de sécurité. Ils autorisent également des communications sécurisées entre les contrôleurs logiques ou les automates de sécurité. Ceci permet aux utilisateurs de répartir leurs commandes de sécurité entre plusieurs systèmes intelligents.

Les réseaux de sécurité sont conçus pour détecter les erreurs de transmission et déclencher une fonction appropriée de réaction à un défaut. Les erreurs de communication détectables incluent : l'insertion de message, la perte de message, la corruption de message, le retard de message, la répétition de message et la séquence de message incorrecte.

Dans la plupart des applications, lorsqu'une erreur est détectée, le dispositif passe dans un état désactivé prédéfini, traditionnellement appelé « état de sécurité ». Le module de communication d'entrée ou de sortie de sécurité est chargé de la détection de ces erreurs de communication et du passage à l'état de sécurité le cas échéant.

Les premiers réseaux de sécurité étaient liés à un type de support ou à une configuration d'accès physique spécifiques. Les industriels devaient donc utiliser un matériel dédié (câbles, cartes d'interface réseau, routeurs, passerelles, etc.) qui devenait alors une des composantes de la fonction de sécurité. Ces réseaux étaient limitées puisqu'ils ne prenaient en charge que les communications entre dispositifs de sécurité.
Ceci impliquait pour l'industriel la nécessité d'utiliser plusieurs réseaux différents dans le cadre de sa stratégie de commande de machines (un réseau pour les commandes standard et un autre pour les commandes de sécurité). Ceci augmentait ainsi les coûts d'installation, de formation et de gestion des pièces de rechange.

Les réseaux de sécurité modernes permettent aux dispositifs de commande de sécurité et standard de communiquer par l'intermédiaire d'un câble réseau unique. CIP (Common Industrial Protocol) Safety est un protocole ouvert standard défini par l'ODVA (Open DeviceNet Vendors Association). Il autorise les communications de sécurité entre dispositifs de sécurité sur des réseaux DeviceNet, ControlNet et EtherNet/IP. CIP Safety étant une extension du protocole CIP standard, les dispositifs standard et de sécurité peuvent ainsi coexister sur un même réseau. Les utilisateurs peuvent également établir des passerelles entre différents réseaux contenant des dispositifs de sécurité. Ceci leur permet de répartir ces dispositifs de sécurité de façon à optimiser les temps de réponse en sécurité. Plus simplement, ceci leur facilite la distribution de leurs dispositifs de sécurité. Tant donné que l'exécution du protocole de sécurité est déléguée aux dispositifs terminaux (contrôleurs logiques et automates de sécurité, modules d'E/S de sécurité, composants de sécurité divers), il est possible d'utiliser des câbles, des cartes d'interfaces réseau, des passerelles et des routeurs standard. Tous ces accessoires deviennent en effet externes à la fonction de sécurité et la nécessité d'un matériel réseau spécialisé n'a ainsi plus de raison d'être.

Dispositifs de sortie

Relais de commande et contacteurs de sécurité

Ces relais de commande et ces contacteurs servent à couper l'alimentation électrique de l'actionneur. Ce sont en fait des relais de commande et contacteurs standard auxquels des fonctions spécialisées ont été ajoutées pour les transformer en accessoires de sécurité.

Ils incorporent en pratique des contacts auxiliaires à couplage mécanique destinés à renvoyer une information sur leur état vers le dispositif logique de surveillance. Ce sont ces contacts à couplage mécanique qui permettent d'assurer la fonction de sécurité. Conformément aux normes applicables à ce type de configuration, des contacts normalement fermés et des contacts normalement ouverts ne peuvent pas se trouver en position fermée simultanément. La norme CEI 60947-4-1 définit les exigences relatives à ces contacts à couplage mécanique. Si les contacts normalement ouverts viennent à se souder, les contacts normalement fermés doivent rester ouverts d'au moins 0,5 mm. Réciproquement, si les contacts normalement fermés viennent à se souder, les contacts normalement ouverts doivent rester ouverts.

Les systèmes de sécurité ne doivent pouvoir être démarrés qu'à des emplacements spécifiques. Sur les relais de commande et les contacteurs standard, il est possible de fermer manuellement les contacts normalement ouverts en appuyant sur l'armature. Sur les dispositifs de sécurité, cette armature est protégée contre tout forçage manuel afin de limiter le risque de redémarrage imprévu.

Sur les relais de commande de sécurité, le contact normalement fermé est actionné par la tige de couplage principale. Les contacteurs de sécurité utilisent une embase supplémentaire pour le montage des contacts à couplage mécanique. Si le bloc contact principal vient à se désolidariser de son embase, les contacts à couplage mécanique restent fermés. Les contacts à couplage mécanique sont accouplés de façon permanente au relais de commande ou au contacteur de sécurité. Sur les plus gros contacteurs, l'embase supplémentaire ne permet pas toujours une retransmission précise de la position de la tige de couplage qui est plus longue. Des contacts miroirs sont utilisés et sont situés de chaque côté du contacteur.

Le temps de déclenchement de ces relais de commande ou contacteurs doit être pris en compte pour le calcul des distances de sécurité. Un suppresseur de surtensions est souvent placé sur la bobine pour augmenter la durée de vie des contacts de commande. Pour les bobines c.a., le temps de déclenchement n'est pas affecté. Pour les bobines c.c., ce temps sera augmenté. Ce délai supplémentaire dépendra du mode de suppression choisi.

Les relais de commande et les contacteurs sont prévus pour commuter des charges élevées allant de 0,5 A à plus de 100 A. Le système de sécurité utilise lui des courants faibles. Le signal de retour généré par l'organe logique du système de sécurité pourra aller de quelques milliampères à des dizaines de milliampères, généralement sous 24 V c.c. Les

relais de commande et les contacteurs de sécurité utilisent des contacts jumelés plaqués or pour commuter de façon fiable ces faibles intensités.

Protection contre les surcharges

Une protection des moteurs contre les surcharges est imposée par les normes électriques. Les diagnostics fournis par ce dispositif de protection contre les surcharges contribuent à améliorer non seulement la sécurité de l'équipement, mais aussi celle de l'opérateur. Les technologies disponibles de nos jours permettent la détection de conditions de défaut comme les surcharges, la perte de phase, les défauts de terre, le blocage rotor, les interférences, la sous-charge, les déséquilibres de phase et les surchauffes. La détection et la communication des conditions anormales préalablement au déclenchement permettent d'améliorer la disponibilité de l'outil de production et de protéger les opérateurs ainsi que le personnel de maintenance en cas de situations dangereuses imprévues.

Variateurs et servovariateurs

Des variateurs et servovariateurs de sécurité peuvent être utilisés pour interrompre un mouvement rotatif et réaliser un arrêt de sécurité ou un arrêt d'urgence.

Les variateurs c.a. sont considérés comme étant de sécurité lorsqu'ils possèdent des voies redondantes pour couper l'alimentation du circuit de commande de gâchette. Les voies redondantes sont surveillées par une logique externe ou intégrale selon le type de variateur. Cette approche redondante permet d'utiliser un variateur de sécurité dans un circuit d'arrêt d'urgence sans qu'il soit besoin d'un contacteur dédié.

Les servovariateurs parviennent à ce résultat d'une façon similaire aux variateurs c.a. Ils utilisent également des signaux de sécurité redondants pour leur fonction d'« arrêt sécurisé du couple ».

Systèmes de raccordement

Les systèmes de raccordement fournissent une valeur ajoutée par le biais de la réduction des coûts d'installation et de maintenance qu'ils impliquent pour les systèmes de sécurité. La conception devra donc considérer avec attention le mode de raccordement des dispositifs : voie unique, double voie, double voie avec indication et types de dispositifs multiples.

Lorsqu'il sera nécessaire de monter en série des interrupteurs à deux voies, un boîtier de distribution pourra simplifier l'installation. Grâce à leur classe de protection IP67, ces boîtiers peuvent être montés à distance sur la machine. Lorsqu'un ensemble de dispositifs de types divers doit être utilisé, un boîtier d'E/S ArmorBlock Guard I/O est à recommander. Ses entrées peuvent en effet être configurées logiciellement de façon à accepter différents types de dispositifs.

Chapitre 5 : Calculs de distance de sécurité

Les sources de danger doivent être neutralisées (état de sécurité) avant que l'opérateur puisse pénétrer dans la zone dangereuse. Pour le calcul de la distance de sécurité, il existe deux groupes de normes. Dans ce chapitre ces normes sont groupées comme suit :

ISO EN : (EN ISO 13855)

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

Formules

La distance de sécurité minimale dépend du temps nécessaire pour le traitement de la commande d'arrêt. Elle dépend également du point jusqu'auquel l'opérateur peut accéder à l'intérieur de la zone avant d'être détecté. Les deux principales formules utilisées partout dans le monde sont du même principe et font appel aux mêmes paramètres. Leurs différences résident dans les symboles utilisés pour représenter leurs variables et dans leurs unités de mesure.

Ces deux formules sont les suivantes :

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

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

Dans lesquelles : Ds et S indiquent la distance de sécurité minimale entre la zone dangereuse et le point de détection le plus proche.

Angles d'approche

Pour calculer la distance de sécurité lorsqu'une barrière immatérielle ou un scrutateur de zone sont utilisés, l'angle d'approche par rapport au dispositif de détection doit être pris en considération. Trois types d'approche sont retenus :

Normale – approche perpendiculaire au plan de détection ;

Horizontale – approche parallèle au plan de détection ;

Angulaire – approche de la zone de détection selon un certain angle.

Constante de vitesse

K symbolise la constante de vitesse dans les deux formules. La valeur de cette constante de vitesse dépend de la célérité de mouvement de l'opérateur (la vitesse de déplacement de ses mains, la vitesse et la longueur de ses pas). En se fondant sur des résultats de recherches, on peut raisonnablement retenir une valeur de 1 600 mm/s pour la vitesse de

déplacement des mains d'un opérateur lorsque son corps est stationnaire. Les conditions de l'application réelle sont toutefois à prendre en compte. En règle générale, la vitesse d'approche varie entre 1 600 mm/s et 2 500 mm/s. La constante de vitesse appropriée doit être déterminée par l'évaluation des risques.

Temps d'arrêt

T est le temps nécessaire pour arrêter totalement le système. La durée complète, en secondes, va du moment où le signal d'arrêt est généré jusqu'à celui où la source de danger est totalement neutralisée. Cette durée peut être décomposée selon différentes dimensions (Ts, Tc, Tr et Tbm/Cf. formule US CAN) pour faciliter l'analyse. Ts est le temps d'arrêt le plus défavorable de la machine/l'équipement. Tc est le temps d'arrêt le plus défavorable du système de commande. Tr est le temps de réponse du dispositif de protection, y compris son interface. Tbm est la durée d'arrêt supplémentaire, au delà des seuils prédéfinis par l'utilisateur, autorisée au niveau du contrôle de freinage avant détection d'une erreur de temps d'arrêt. Tbm est notamment utilisé pour les presses mécaniques rotatives. Ts + Tc + Tr sont généralement mesurés par un dispositif de contrôle du temps d'arrêt lorsque ces valeurs ne sont pas prédéfinies.

Facteurs de profondeur de pénétration

Les facteurs de profondeur de pénétration sont représentés par les symboles C et Dpf. Il s'agit de la distance d'avancement maximale en direction de la source de danger avant détection par le dispositif de protection. Les facteurs de profondeur de pénétration varieront selon le type de dispositif et de l'application. Vérifier la norme pertinente pour déterminer le meilleur facteur de profondeur de pénétration. Dans le cas d'une approche normale par rapport à une barrière immatérielle ou un scrutateur de zone dont la sensibilité de détection sera inférieure à 64 mm, les normes ANSI et canadiennes utilisent :

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

Dans le cas d'une approche normale par rapport à une barrière immatérielle ou un scrutateur de zone, dont la sensibilité de détection sera inférieure à 40 mm, les normes ISO et EN utilisent :

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

Ces deux formules ont un point d'intersection correspondant à une taille d'objet de 19,3 mm. Pour la détection d'objets inférieurs à 19 mm, l'approche US CAN est plus restrictive. En effet, elle impose de placer la barrière immatérielle ou le scrutateur de zone plus loin de la source de danger. Pour la détection d'objets supérieurs à 19,3 mm, c'est la norme ISO EN qui est la plus restrictive. Les constructeurs de machines fabriquant pour le marché mondial devront retenir le résultat le plus défavorable de l'application de ces deux équations.

Applications avec accès à travers le champ de détection

Pour la détection des plus grands objets, les normes US CAN et ISO EN diffèrent légèrement en ce qui concerne le facteur de profondeur de pénétration et la sensibilité de détection. La valeur ISO EN est de 850 mm alors que la valeur US CAN est de 900 mm. Les deux normes diffèrent également au niveau de la sensibilité de détection des objets.

Applications avec accès par dessus le champ de détection

Les deux normes s'accordent sur une hauteur de position minimum du faisceau de détection le plus bas de 300 mm. Elles diffèrent cependant sur la hauteur de position minimum du faisceau de détection le plus haut. La norme ISO EN stipule 900 mm, alors que la norme US CAN impose 1 200 mm. Ces valeurs de position du faisceau supérieur apparaissent néanmoins discutables. Si l'on considère qu'il s'agit d'une application avec accès à travers le champ de détection, la hauteur du faisceau de détection le plus haut devra être en effet bien supérieure pour tenir compte du cas d'un opérateur se trouvant debout. Cependant, s'il s'agit d'une application dans laquelle l'opérateur peut passer par dessus le plan de détection, les critères définis pour ce type d'accès peuvent être retenus.

Faisceaux unique ou multiples

Les faisceaux unique ou multiples sont définis plus particulièrement par les normes ISO EN. Le tableau ci-dessous indique les hauteurs « pratiques » de faisceaux multiples par rapport au sol. Le facteur de profondeur de pénétration est de 850 mm dans la plupart des cas et 1 200 mm dans le cas de l'utilisation d'un faisceau unique. Quant à elle, l'approche US CAN intègre cela au niveau de ses critères d'accès à travers le champ de détection. Les tentatives d'accès par dessus, par dessous ou sur le côté d'un dispositif à faisceaux simples ou multiples devront toujours être prises en compte par ailleurs.

Nombre de faisceaux	Hauteur par rapport au sol – mm (in)	C – mm (in)
1	750 (29.5)	1200 (47.2)
2	400 (5.7), 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)

Calculs de la distance de sécurité

Dans le cas d'une approche normale par rapport à une barrière immatérielle, les modes de calcul de la distance de sécurité selon les normes ISO EN et US CAN sont très voisins. Il existe cependant quelques différences. Dans le cas d'une approche normale par rapport à une barrière immatérielle verticale dont la sensibilité de détection est au maximum de 40 mm, la démarche proposée par l'ISO EN nécessite normalement deux étapes. Il faut d'abord calculer S en utilisant 2 000 comme constante de vitesse.

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

La valeur minimale que peut prendre S est 100 mm.

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

La norme US CAN utilise quant à elle une démarche en une seule étape : Ds = 1 600 x T * Dpf

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

Approches angulaires

Dans la plupart des installations, les barrières immatérielles et les scrutateurs sont montés verticalement (approche normale) ou horizontalement (approche parallèle). Ces montages ne sont pas considérés comme angulaires tant qu'ils sont dans une tolérance de ±5° par rapport à leur axe normal. Lorsque cet angle devient supérieur à ±5°, des risques potentiels supplémentaires liés aux approches prévisibles (par exemple, le raccourcissement de la distance de détection) doivent être pris en considération. En général, les angles supérieurs à 30° par rapport au plan de référence (le sol par exemple) doivent être associés à une approche normale et ceux inférieurs à cette valeur, à une approche parallèle.

Tapis de sécurité

Avec les tapis de sécurité, la distance de sécurité doit prendre en considération la vitesse de déplacement et la foulée des opérateurs. Considérant que l'opérateur se déplace en marchant et que le tapis de sécurité est fixé au sol, Le premier pas de l'opérateur sur le tapis correspond à un facteur de pénétration de 1200 mm (48 in). Si l'opérateur doit monter sur une plateforme, le facteur de pénétration peut être réduit d'un coefficient de 40 % de la hauteur de la marche. Il est important de fixer soigneusement le(s) tapis afin d'éviter tout déplacement.

Exemple

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

Dpf = 3,4 (14 – 6,875) = 1 in (25,4 mm)

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

C = 8 (14-14) = 0

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 devra être placée par rapport à la source de danger sera de 508 mm (20 in), dans l'optique d'une utilisation de la machine n'importe où dans le monde.

Chapitre 6 : Systèmes de commande de sécurité

Introduction

Qu'est-ce qu'un système de commande de sécurité (souvent désigné par l'acronyme anglais SRCS) ? Il s'agit de la partie du système de commande d'une machine ayant pour objet de prévenir l'apparition de conditions dangereuses. Il peut s'agir d'un système spécifique externe ou il peut être intégré au système normal de commande de la machine.

Son degré de complexité peut aller d'un système simple, par exemple un interrupteur de verrouillage sur une grille de protection et un interrupteur d'arrêt d'urgence montés en série avec la bobine de commande d'un contacteur de puissance, à un système composite intégrant à la fois des dispositifs simples et des dispositifs complexes communicant entre eux logiciellement ou matériellement.

Les systèmes de commande de sécurité sont conçus pour exécuter des fonctions de sécurité. Le système doit continuer à fonctionner correctement dans toutes les situations prévisibles. Qu'est-ce qu'une fonction de sécurité ; comment concevons-nous un système pour la réaliser ; et quand nous avons fait cela, comment pouvons-nous la représenter ?

Fonction de sécurité

Une fonction de sécurité est mise en œuvre par les composants de sécurité du système de commande de la machine. Elle a pour but de placer ou de maintenir l'équipement protégé à l'état de sécurité par rapport à un danger ou un ensemble de dangers. Une défaillance de la fonction de sécurité peut entraîner l'augmentation immédiate du risque d'utilisation de l'équipement, c'est-à-dire d'une situation dangereuse.

On parle de « situation dangereuse » lorsqu'une personne pourrait être exposée à un danger. Une situation dangereuse n'implique pas nécessairement que la personne soit blessée. La personne exposée peut en effet être capable de reconnaître le danger et d'éviter les blessures. La personne exposée peut cependant ne pas être consciente du danger ou le danger peut être provoqué par un démarrage imprévu. La tâche principale du concepteur du système de sécurité est donc de prévenir les situations dangereuses et d'empêcher les démarrages imprévus.

La fonction de sécurité peut souvent être déterminée par des contraintes multi-critères. Par exemple, la fonction de sécurité liée à une grille de protection à verrouillage de sécurité est caractérisée par trois critères :

1. les dangers isolés par le dispositif de protection ne peuvent pas fonctionner avant que la protection soit fermée ;

2. l'ouverture du dispositif de protection doit entraîner l'arrêt du danger s'il est actif au moment de l'ouverture ; et

3. la fermeture du dispositif de protection ne doit pas redémarrer le danger protégé par le dispositif de protection.

Lors de la définition d'une fonction de sécurité destinée à une application spécifique, le mot « danger » devra être remplacé par la description du danger spécifique. La source du danger ne doit pas être confondue avec ses conséquences. L'écrasement, le sectionnement et les brûlures sont les conséquences d'un danger. Une source de danger est, par exemple, un moteur, un vérin, un couteau, une torche, une pompe, un faisceau laser, un robot, un effecteur de bras robotisé, une électrovanne ou tout autre type d'actionneur, ou encore un danger mécanique lié à la gravité.

On trouve souvent la formule « lors de ou préalablement à une sollicitation de la fonction de sécurité » dans la littérature relative aux systèmes de sécurité. Qu'est-ce donc qu'une sollicitation de la fonction de sécurité ? Il peut s'agir, par exemple, de l'ouverture d'un dispositif de protection à verrouillage, de l'interruption d'une barrière immatérielle, d'un déplacement sur un tapis de sécurité ou de l'actionnement d'un bouton d'arrêt d'urgence. L'attente de l'opérateur est que la source du danger soit désactivée ou qu'elle le reste si elle est déjà arrêtée.

La fonction de sécurité est exécutée par les divers composants de sécurité du système de commande de la machine. Elle n'est pas exécutée par un dispositif unique, par exemple uniquement la grille de protection. Le dispositif d'interverrouillage de cette grille a pour objet envoyer un signal de commande à un dispositif logique qui, à son tour, va désactiver l'actionneur. La fonction de sécurité commence donc par l'émission d'une commande et se termine par son exécution.

Le système de sécurité doit être conçu avec un niveau d'intégrité adapté aux risques présentés par la machine. Plus ces risques sont importants, plus les niveaux d'intégrité devront être élevés pour garantir l'efficacité de la fonction de sécurité. Les systèmes de sécurité des machines peuvent être classifiés selon le niveau de performance correspondant à leur capacité à exécuter leurs fonctions de sécurité ou, en d'autres termes, suivant leur niveau d'intégrité de sécurité fonctionnelle.

Sécurité fonctionnelle des systèmes de commande

Qu'est-ce que la sécurité fonctionnelle ?

La sécurité fonctionnelle est la partie du système de sécurité global qui dépend du bon fonctionnement du procédé ou de l'équipement en réponse à ses entrées. La norme CEI TR 61508-0 fournit l'exemple suivant pour mieux comprendre la signification de la sécurité fonctionnelle. « L'utilisation d'un dispositif de protection thermique sous forme de capteur thermique logé dans les bobinages d'un moteur électrique pour couper son alimentation en cas de surchauffe est un exemple de sécurité fonctionnelle. Mais fournir une isolation spécialisée pour résister à des températures élevées n'est pas un exemple de sécurité fonctionnelle (bien que ce soit quand même un exemple de mesure de sécurité destiné à protéger le moteur contre le même danger). »

À titre d'exemple complémentaire, comparons une barrière de protection matérielle à une grille de protection à verrouillage de sécurité. La protection matérielle n'est pas considérée comme une « sécurité fonctionnelle » bien qu'elle puisse protéger contre l'accès au même danger que la grille de protection à verrouillage de sécurité. La grille de

protection à verrouillage de sécurité est par contre typiquement un dispositif de sécurité fonctionnelle. Lorsque la grille est ouverte, son mécanisme d'interverrouillage envoie un signal « d'entrée » au système chargé de maintenir la condition de sécurité. De même, un équipement de protection individuelle (EPI) sera utilisé comme mesure de protection pour améliorer la sécurité du personnel. Mais cet EPI ne sera cependant pas considéré comme un dispositif de sécurité fonctionnelle.

Le terme de sécurité fonctionnelle a été introduit par la norme CEI 61508:1998. Depuis, le terme n'a parfois été associé qu'aux systèmes de sécurité programmables. C'est une erreur. La sécurité fonctionnelle peut s'appliquer à de nombreux dispositifs entrant dans la composition de systèmes de sécurité. Des dispositifs comme des barrières immatérielles de sécurité, des relais de sécurité, des automates de sécurité, des contacteurs de sécurité et des variateurs de sécurité peuvent être interconnectés pour constituer un système de sécurité qui accomplira une fonction de sécurité particulière. C'est le principe même de la sécurité fonctionnelle.

Par conséquent, un système de commande électrique à sécurité fonctionnelle est parfaitement apte à maîtriser les dangers créés par les parties en mouvement des machines.

Deux types de paramètres sont à considérer pour la mise en œuvre d'un système de sécurité fonctionnelle :

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

L'évaluation des risques joue un rôle clé pour la définition de ces paramètres ou exigences de sécurité fonctionnelle. L'analyse des tâches et des dangers conduit à l'élaboration des exigences fonctionnelles de sécurité (c'est-à-dire, la fonction de sécurité). La quantification des risques permet de mettre en évidence les exigences d'intégrité de la sécurité (c'est-à-dire, le niveau d'intégrité de la sécurité ou le niveau de performance).

Les quatre principales normes de sécurité fonctionnelle des machines en vigueur sont les suivantes :

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

   Cette norme regroupe les réquisitions et les prescriptions applicables à la conception des systèmes et sous-systèmes électroniques et programmables complexes. Cette norme a un caractère générique. Elle n'est donc pas limitée au secteur des machines.

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

Cette norme est la version spécifique aux machines de la précédente norme CEI/EN 61508. Elle définit les exigences applicables à la conception des systèmes de commande électriques relatifs à la sécurité des machines, ainsi qu'à la conception des sous-systèmes et dispositifs de moindre complexité. Elle stipule que les sous-systèmes complexes ou programmables devront être conformes à la norme CEI/EN 61508

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

   Cette norme est destinée à fournir une transition directe avec les Catégories définies par l'ancienne norme EN 954-1.

4. CEI 61511 « Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur de l'industrie des procédés ».

   Cette norme est la transposition de la norme CEI/EN 61508 au secteur des procédés.

Les normes de sécurité fonctionnelle représentent un pas en avant significatif. Elles permettent d'aller au-delà des exigences relatives à la fiabilité de la commande et au système des Catégories de la précédente version de la norme ISO 13849-1:1999 (EN 954-1:1996).

Les catégories n'ont pas complètement disparu ; elles demeurent en vigueur dans l'actuelle norme (EN) ISO 13849-1.

CEI/EN 62061 et (EN) ISO 13849-1

Les normes CEI/EN 62061 et (EN) ISO 13849-1 concernent toutes deux les systèmes de commande électriques relatifs à la sécurité. Il est possible qu'elles soient à terme regroupées en une seule norme utilisant une terminologie commune. Toutes deux permettent de parvenir au même résultat, mais elles font appel à des méthodes différentes. Leur finalité est de fournir aux utilisateurs une possibilité de choix en fonction de leur situation particulière. Ces utilisateurs peuvent donc décider d'utiliser l'une ou l'autre. Elles sont, de plus, harmonisés sous la Directive Machines européenne.
Ces deux normes proposent des niveaux de sécurité comparables, qu'ils soient référencés « SIL » ou « PL ». Leurs différences méthodologiques leur permettent de s'adapter aux spécificités des utilisateurs auxquels elles sont destinées.
La méthodologie utilisée par la norme CEI/EN 62061 autorise la mise en œuvre de fonctionnalités de sécurité complexes. Elles peuvent être déployées dans le cadre d'architectures système qui n'étaient pas envisagées jusqu'alors. L'objectif de la norme (EN) ISO 13849-1 est d'offrir une solution plus directe et moins complexe pour des fonctionnalités de sécurité plus conventionnelles, déployées dans le cadre d'architectures systèmes classiques.

L'élément qui différencie le plus ces deux normes est leur champ d'application respectif. La norme CEI/EN 62061 est mieux adaptée aux systèmes électriques. De son côté,

la norme (EN) ISO 13849-1 s'applique aussi bien aux systèmes pneumatiques, hydrauliques et mécaniques, qu'aux systèmes électriques.

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 de permettre aux utilisateurs des deux normes de s'y retrouver.

Il précise la relation entre les deux normes et explique comment établir la correspondance entre les niveaux de performance PL (Performance Level) de la norme (EN) ISO 13849-1 et les niveaux d'intégrité de sécurité SIL (Safety Integrity Level) de la norme CEI/EN 62061, tant au niveau des systèmes que des sous-systèmes.

Afin de démontrer que les deux normes aboutissent aux mêmes résultats, le rapport donne un exemple de système de sécurité calculé selon la méthodologie de chacune d'entre elles. Ce rapport clarifie également plusieurs points qui avaient conduit à des interprétations différentes. L'un de ces points les plus critiques est certainement la question de l'exclusion de défauts.

En général, lorsqu'un niveau de performance PLe est requis pour la mise en œuvre d'une fonction de sécurité par un système de commande de sécurité, il n'est pas normal de jouer uniquement sur les exclusions de défauts pour obtenir ce niveau de performance. Cela dépendra de la technologie utilisée et de l'environnement de travail prévu. Il est donc essentiel que les concepteurs attachent une importance accrue à la définition des exclusions de défauts lorsque les exigences de niveau de performance PL augmentent.

En général, l'utilisation des exclusions de défaut ne convient pas pour les aspects mécaniques des détecteurs de position électromécaniques en vue d'atteindre un niveau PLe dans la conception d'un système de commande de sécurité. Les exclusions de défaut susceptibles d'être attachées à des conditions de défaut mécanique particulières (par exemple, l'usure, la corrosion, les ruptures) sont définies dans le tableau A.4 de la norme ISO 13849-2.

Par exemple, un système de verrouillage de porte devant garantir un niveau de performance PLe devra avoir un facteur de tolérance aux pannes minimum de 1 (par exemple, en utilisant deux détecteurs de position mécaniques conventionnels). Il n'est en effet normalement pas admissible d'exclure des défauts tels que des ruptures d'actionneurs de contacts à ce niveau de performance. Cependant, il peut être envisagé d'exclure des défauts, comme un court-circuit dans le câblage d'un panneau de commande conçu conformément aux normes applicables.

SIL et CEI/EN 62061

La norme CEI/EN 62061 définit de façon combinée l'ampleur du risque à réduire et la capacité du système de commande à réduire ce risque, en termes de niveaux d'intégrité de sécurité SIL (Safety Integrity Level). Il existe 3 niveaux SIL applicables au secteur des machines. Le niveau le plus faible est SIL 1, le plus élevé est SIL 3.

Tant donné que la classification SIL est également utilisée dans d'autres secteurs industriels comme la pétrochimie, la production d'énergie et le transport ferroviaire, la norme CEI/EN 62061 trouve toute son utilité lorsque des machines sont utilisées dans ces secteurs. Des risques plus importants encore peuvent exister dans d'autres secteurs comme les industries des procédés. C'est pour cette raison que la norme CEI 61508, ainsi que la norme CEI 61511 spécifique au secteur des procédés, incluent un niveau SIL 4.

Un niveau SIL est applicable à une fonction de sécurité. Les sous-systèmes composant le système chargé d'assurer cette fonction de sécurité doivent avoir des caractéristiques SIL compatibles. On parlera parfois dans ce cas du niveau SIL maximum des sous-systèmes ou SIL CL (SIL Claim Limit). Une étude complète et approfondie de la norme CEI/EN 62061 est nécessaire avant de pouvoir l'appliquer correctement.

PL et (EN) ISO 13849-1

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

Comparaison des niveaux PL et SIL

Ce tableau présente les équivalences approximatives entre les classifications PL et SIL lorsqu'elles s'appliquent à des structures de circuit de sécurité classiques.

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

Correspondance approximative entre les niveaux PL et SIL

IMPORTANT : le tableau précédent est fourni à titre informatif uniquement. Il NE DOIT PAS être utilisé comme base pour effectuer des conversions. La totalité des exigences de chacune de ces normes doit être prises en considération. Les tableaux de l'annexe K fournissent des informations plus détaillées.

Chapitre 7 : Conception du système selon la norme (EN) ISO 13849

Une étude complète et approfondie de la norme (EN) ISO 13849-1 est nécessaire avant de pouvoir l'appliquer correctement. Ce qui suit ne constitue qu'un aperçu sommaire.

Cette norme définit des règles pour la conception et l'intégration de composants de sécurité dans un système de commande, notamment au niveau de certains aspects logiciels. La norme concerne le système de sécurité dans son ensemble, mais elle peut également être appliquée aux composants de ce système.

Logiciel SISTEMA de calcul du niveau PL

SISTEMA est un outil logiciel destiné à l'implémentation de la norme (EN) ISO 13849-1. Son utilisation simplifie très largement les aspects quantification et calcul de la mise en œuvre de cette norme.

SISTEMA signifie « Safety Integrity Software Tool for the Evaluation of Machine Applications » et fait l'objet d'évolutions et mises à jour régulières par l'IFA. Il nécessite la saisie de divers types de données relatives à la sécurité fonctionnelle, décrites plus loin dans ce chapitre. Ces données peuvent être entrées manuellement ou automatiquement par le biais d'une bibliothèque de données SISTEMA propre à un fabricant (SISTEMA Data Library).

La bibliothèque de données SISTEMA de Rockwell Automation est disponible au téléchargement, ainsi qu'un lien vers le site de téléchargement de SISTEMA, à l'adresse : *www.rockwellautomation.com, sous Solutions & Services > Safety Solutions.*

Présentation de la norme (EN) ISO 13849-1

La présentation générale suivante vise à fournir un aperçu des dispositions de base de la norme (EN) ISO 13849-1. Elle fait aussi mention de sa révision publiée début 2106. Il est essentiel d'étudier la norme proprement dite en détail.
Cette norme a un champ d'application très vaste car elle s'applique à toutes les technologies, notamment : électrique, hydraulique, pneumatique et mécanique. Bien que la norme ISO 13849-1 puisse être utilisée pour des systèmes complexes, elle renvoie également le lecteur à la norme CEI 61508 pour les composants logiciels intégrés complexes.

La norme ISO 13849-1 définit des niveaux de performances [PL a, b, c, d ou e]. Le concept original de Catégories est conservé mais des exigences supplémentaires sont à satisfaire avant de pouvoir revendiquer un niveau PL pour un système.

L'ensemble des paramètres peut être listé de façon simplifiée comme suit :

- L'architecture du système. Ceci recouvre principalement ce qui était précédemment défini par les Catégories.

- Les données de fiabilité requises pour les composants du système.
- Le taux de couverture des tests de diagnostic DC (Diagnostic Coverage) du système. Cela représente l'efficacité d'une surveillance des défauts au niveau du système.
- La protection contre les défaillances de cause commune.
- La protection contre les défauts systématiques
- Le cas échéant, les exigences particulières au niveau logiciel

Nous reviendrons plus en détail sur ces facteurs ultérieurement. Mais avant cela, il est important de bien comprendre les intentions et les principes de base de la norme dans son ensemble. Il est clair à ce stade qu'il y a des considérations supplémentaires à assimiler. Mais les détails prendront plus de sens une fois bien compris les objectifs et la raison d'être de la norme.

Premièrement, pourquoi une norme est-elle nécessaire ? Il est évident que les technologies applicables aux systèmes de sécurité des machines ont progressé et se sont modifiées considérablement au cours des dix dernières années. Jusqu'à un temps relativement récent, les systèmes de sécurité étaient basés sur l'utilisation d'équipements « simples » présentant des modes de défaillance très faciles à prévoir. Désormais, les dispositifs électroniques et électroniques programmables sans cesse plus complexes se généralisent dans les systèmes de sécurité. Ceci a eu un effet favorable sur les coûts, la flexibilité et la compatibilité. Mais cela s'est traduit également par le fait que les normes en vigueur n'étaient plus adaptées. Pour savoir si un système de sécurité est suffisant, il faut en savoir plus sur ce système. C'est pourquoi les normes de sécurité fonctionnelle exigent plus d'informations. Alors que les systèmes de sécurité utilisent de plus en plus une approche de type « boîte noire » en intégrant des sous-systèmes préqualifiés, leur conformité aux normes devient cruciale. Ces normes doivent donc être capables d'interroger pertinemment la technologie. Pour y parvenir, elles doivent pouvoir intégrer tous les facteurs fondamentaux concernant la fiabilité, la détection des défauts ainsi que l'intégrité architecturale et systémique. C'est l'objectif de la norme (EN) ISO 13849-1.

Pour parcourir de façon logique l'ensemble de cette norme, les motivations de deux types d'utilisateurs fondamentalement différents doivent être pris en compte : les concepteurs de sous-systèmes de sécurité et les concepteurs de systèmes de sécurité proprement-dits. Dans les faits, le concepteur du sous-système (typiquement, un fabricant de composants de sécurité) sera soumis à un niveau de rigueur supérieur. Il devra en effet fournir toutes les informations nécessaires pour garantir au concepteur de système que son sous-système présente une intégrité adaptée au système que celui-ci envisage. Cela nécessitera concrètement un certain nombre d'essais, d'analyses et de calculs. Les résultats devront être présentés sous la forme requise par la norme.

Le concepteur du système (typiquement, un concepteur ou un intégrateur de machines) utilisera les données du sous-système pour effectuer des calculs relativement simples dans le cadre de la détermination du niveau de performance (PL) global du système.

Détermination de la fonction de sécurité

Nous devons donc définir ce que doit être la fonction de sécurité. La fonction de sécurité doit clairement être adaptée à la tâche requise. Comment la norme nous aide-t-elle à le vérifier ?
Il est important de bien comprendre que la fonction à réaliser ne peut être déterminée que par les caractéristiques spécifiques à l'application réelle. Ceci peut être considéré comme la phase de définition du concept de sécurité. Elle ne pourra pas être totalement couverte par la norme car celle-ci ne peut pas connaître toutes les caractéristiques des applications particulières. Ceci s'applique souvent également au constructeur de machines. Il fabrique en effet les machines, mais il ne connaît pas forcément les conditions exactes dans lesquelles elles seront utilisées.

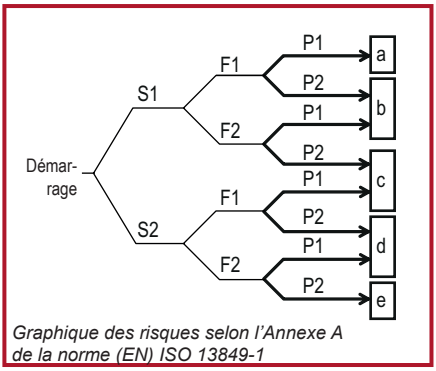
La norme apporte cependant une aide en proposant une liste regroupant un grand nombre de fonctions de sécurité couramment utilisées (par exemple, la fonction d'arrêt de sécurité déclenchée par un dispositif de protection, d'inhibition et de démarrage/redémarrage) et en indiquant certaines des exigences généralement associées à ces fonctions. Étude de la norme (EN) ISO 12100 : « Principes généraux de conception et appréciation du risque » est recommandée à ce stade. La norme ISO TR 22100-2 fournit des recommandations utiles sur la relation entre le processus d'évaluation des risques d'une machine conformément à la norme ISO 12100 et le processus d'attribution de niveau PL de la norme (EN) ISO 13849-1. Il existe également un grand nombre de normes adaptées spécifiquement à certains types de machines et qui fournissent des exigences fonctionnelles de sécurité dédiées pour ces machines. Dans les normes européenne (EN), elles sont désignées par « normes de type C ». Certaines d'entre elles ont des équivalents directs dans les normes ISO. La norme ISO TR 22100-1 fournit des informations supplémentaires sur la relation entre les normes ISO 12100 et C.

Il est clair que l'étape de définition du concept de sécurité dépend du type de machine, mais aussi des caractéristiques de l'application et de l'environnement dans lequel elle est déployée. Le constructeur de machine devra anticiper au maximum ces facteurs pour définir son concept de sécurité. Les conditions d'utilisation normales (c'est-à-dire, prévues) devront en conséquence être indiquées dans le manuel utilisateur. L'utilisateur de la machine devra pour sa part s'assurer qu'elles sont compatibles avec ses conditions d'utilisation réelles.

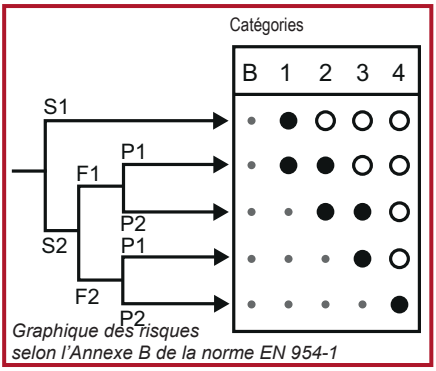
Le niveau PLr sert à déterminer le niveau de performance requis pour la fonction de sécurité et cet aspect est déterminé pendant l'évaluation du risque. Pour déterminer ce niveau PLr, la norme propose un graphe des risques permettant d'intégrer les facteurs de gravité des blessures, de fréquence d'exposition et de possibilité d'évitement propres à l'application.

Le résultat obtenu sera le niveau PLr. Les utilisateurs de l'ancienne norme EN 954-1 reconnaîtront cette approche. Mais ils noteront qu'au sein de la norme (EN) ISO 13849-1, la ligne S1 est désormais subdivisée, contrairement à l'ancien graphique des risques. La version de 2015 offre la possibilité de réduire le niveau PLr d'un cran dans certaines circonstances selon la probabilité prévisible de survenance.

Conception du système selon la norme (EN) ISO 13849



Graphique des risques selon l'Annexe A de la norme (EN) ISO 13849-1



Graphique des risques selon l'Annexe B de la norme EN 954-1

Désormais, nous avons une description de la fonctionnalité de sécurité et du niveau de performance nécessaire PLr pour les composants de sécurité du système de commande (parfois désignés par l'acronyme anglais SRP/CS) qui seront chargés de mettre en œuvre cette fonction. Nous devons maintenant concevoir le système et vérifier qu'il est conforme au niveau PLr.

Un facteur décisif du choix de la norme de référence à utiliser ((EN) ISO 13849-1 ou EN/CEI 62061) sera la complexité de la fonction de sécurité. Dans la majorité des cas, pour les machines, la fonction de sécurité sera relativement simple et la norme (EN) ISO 13849-1 sera l'option la mieux adaptée. Les données de fiabilité, le taux de couverture des tests de diagnostic (DC), l'architecture système (Catégorie), les défaillances de cause commune et, éventuellement, les contraintes logicielles seront prises en compte pour l'évaluation du niveau de performance PL.

Ce qui suit n'est qu'une description simplifiée destinée uniquement à fournir un aperçu de la démarche. Il est important d'avoir bien à l'esprit qu'absolument toutes les dispositions incluses dans le texte de la norme doivent être intégrées. Il existe cependant une aide pour cela. Le logiciel SISTEMA est là pour apporter une assistance au niveau documentaire et à celui des calculs. Il est capable également de produire un dossier technique.

SISTEMA est disponible dans une multitude de langues, notamment l'allemand et l'anglais. L'IFA, développeur de SISTEMA, est un organisme de recherche et d'essais basé en Allemagne et qui fait autorité. Il est particulièrement impliqué dans la résolution des problèmes scientifiques et techniques liés à la sécurité dans le cadre des politiques d'assurance obligatoire et de prévention des accidents en Allemagne. Il collabore avec des organismes dédiés à l'hygiène et à la sécurité au travail dans plus de 20 pays.

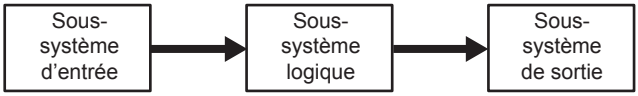
Les experts de l'IFA, en liaison avec leurs collègues du BG, ont largement participé à la rédaction des normes (EN) ISO 13849-1 et CEI/EN 62061.

La « bibliothèque » de données de composants de sécurité Rockwell Automation conçue pour SISTEMA est disponible sur : *www.rockwellautomation.com, sous Solutions & Services > Safety Solutions.*

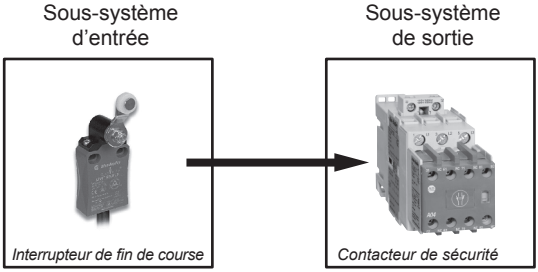
Quel que soit le mode de calcul du niveau PL, il est important de partir de bonnes bases. Nous devons aborder notre système de la même façon que la norme. Commençons donc par cela.

Structure du système

Tout système peut être décomposé selon ses composants de base ou « sous-systèmes ». Chaque sous-système possède sa propre fonction discrète. La plupart des systèmes peuvent être décomposés en trois fonctions de base : entrée, traitement logique et actionnement (certains systèmes simples n'utilisent pas de traitement logique).



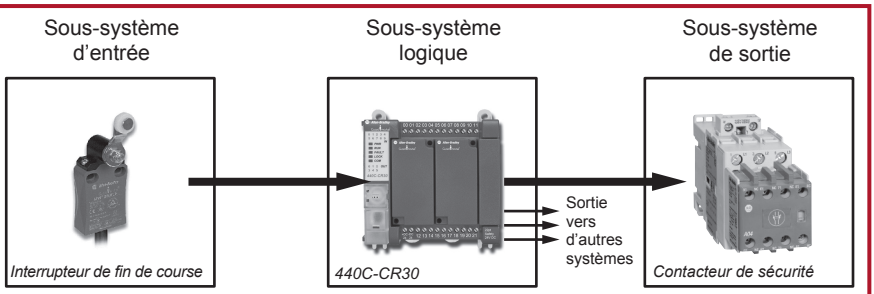
Les groupes de composants qui assurent ces fonctions constituent les sous-systèmes.



Interrupteur de sécurité et contacteur de sécurité

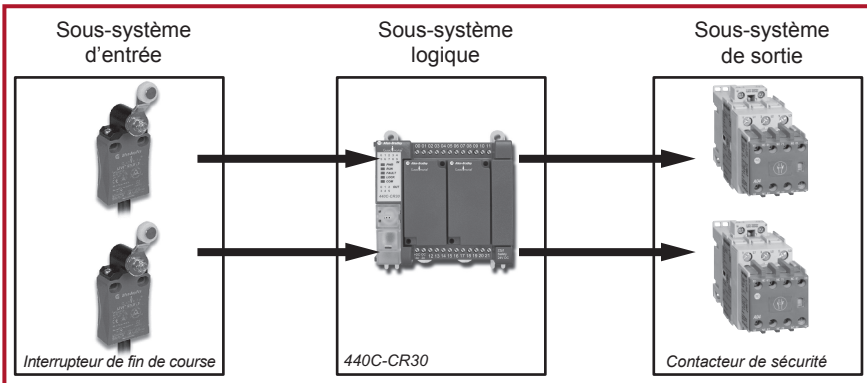
Un exemple de système électrique simple mono-voie est présenté ci-dessus. Il n'est constitué que d'un sous-système d'entrée et d'un sous-système de sortie.

Conception du système selon la norme (EN) ISO 13849



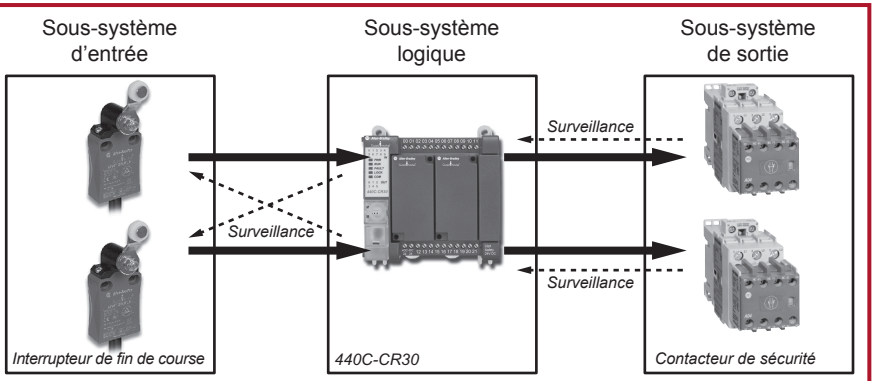
Interrupteur de sécurité, automate de sécurité et contacteur de sécurité

Le système ci-dessus est un peu plus complexe car il fait appel à un traitement logique. L'automate de sécurité pourra lui-même avoir une tolérance interne aux défauts (par exemple, grâce à l'utilisation d'une deuxième voie). Mais le système global sera toujours limité à une seule voie du fait des sous-systèmes à interrupteur de fin de course unique et à contacteur de sécurité unique. Un système mono-voie subira une défaillance en cas de défaillance d'un de ses sous-systèmes mono-voie. Il n'intègre aucune « tolérance aux pannes ».



Système de sécurité à deux voies

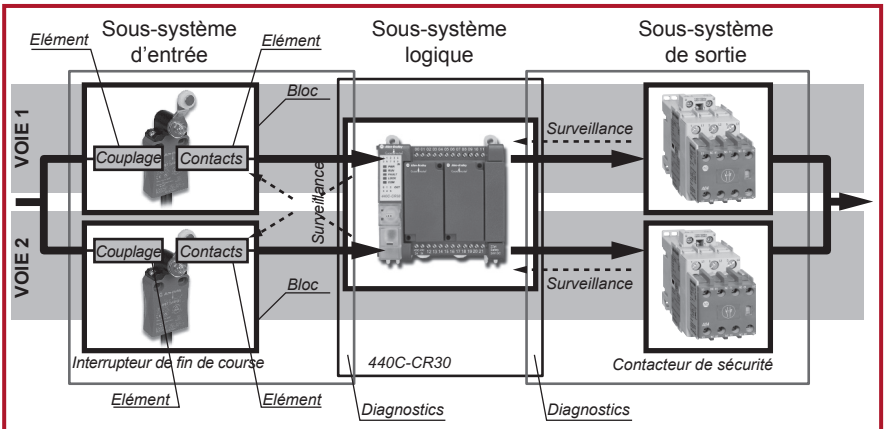
Un système à double voie (également appelé système redondant ou « tolérant aux pannes ») est présenté ci-dessus. Chaque sous-système possède deux voies et peut tolérer un défaut unique tout en fournissant la fonction de sécurité. Cette fonction de sécurité doit connaître deux défaillances, une sur chaque voie, avant que le sous-système et donc le système subisse une défaillance. Il est évident qu'un système à deux voies aura moins de chance de tomber en panne et de provoquer une situation dangereuse qu'un système mono-voie. Mais il est possible de le rendre encore plus fiable (pour ce qui est de sa fonction de sécurité) si nous lui incluons des fonctionnalités de diagnostic afin de détecter les défauts potentiels. Naturellement, une fois un défaut détecté, il sera nécessaire également d'y réagir et de placer le système à l'état de sécurité. Le schéma suivant montre l'ajout de fonctionnalités de diagnostic au système par l'intermédiaire de techniques de surveillance interne.



Système de sécurité à deux voies avec diagnostics

Un système comprend généralement (mais pas nécessairement toujours) deux voies sur tous ses sous-systèmes. Nous constatons sur l'exemple que chaque sous-système possède deux « sous-voies ». La norme parle de « blocs » pour désigner cette configuration. Un sous-système à deux voies possède au minimum deux blocs et un sous-système à une voie au minimum un bloc. Il peut se produire que certains systèmes utilisent une combinaison de blocs à une et deux voies.

Si nous voulons analyser de façon plus approfondie le système en exemple, nous devons nous intéresser particulièrement aux composants de ces blocs. Le logiciel SISTEMA utilise le terme d'« éléments » pour les désigner.



Décomposition d'un système de sécurité à deux voies avec diagnostics

Dans ce nouveau schéma, le sous-système des interrupteurs de fin de course est présenté décomposé selon ses éléments. Le sous-système de contacteur de sortie est subdivisé au niveau blocs. Le sous-système logique n'est pas subdivisé car il est déjà qualifié et validé par le fabricant selon un niveau PL donné. Les fonctions de surveillance relatives aux interrupteurs de fin de course aussi bien qu'aux contacteurs sont exécutées par l'automate. En conséquence, les cadres délimitant les sous-systèmes d'interrupteurs de fin de course et de contacteur sont représentés en léger chevauchement sur le cadre délimitant le sous-système logique.

Ce principe de décomposition élémentaire du système est retenu dans la méthodologie proposée par la norme (EN) ISO 13849-1 ainsi que dans le principe de structuration du système de base utilisé par SISTEMA. Cependant, il est important de noter qu'il existe quelques différences infimes entre les deux. La norme n'est pas restrictive quant à la méthodologie. Cependant, dans sa méthode simplifiée d'estimation du niveau PL, la première étape consiste normalement à décomposer le système complet en voies et en blocs sur chacune de ces voies. Avec SISTEMA, il est généralement plus pratique de subdiviser le système en sous-systèmes, puis chaque sous-système en blocs. La norme ne se réfère pas explicitement au concept de sous-système. Son utilisation par SISTEMA permet cependant d'obtenir une approche plus compréhensible et plus intuitive. Il n'y a bien sûr aucun effet sur le résultat final. SISTEMA et la norme utilisent des principes et des formules de calcul identiques. Il est également intéressant de noter que l'approche par sous-systèmes est également utilisée par la norme EN/CEI 62061.

Le système que nous avons utilisé comme exemple n'est autre que l'un des cinq types d'architecture système de base mentionnés par la norme. Toute personne familiarisée avec le système des Catégories identifiera cet exemple comme typique de la Catégorie 3 ou 4.

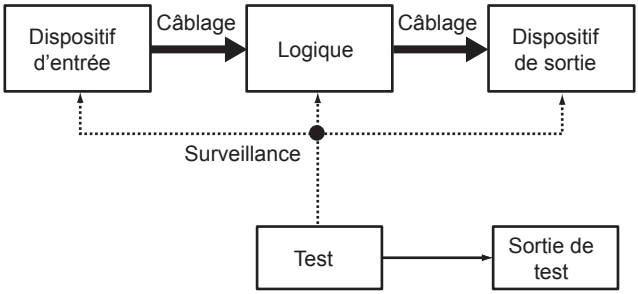
La norme utilise les cinq Catégories originales de l'ancienne norme EN 954. Elle les appelle Catégories d'architecture désignée. Les exigences propres à ces catégories sont presque (mais pas tout à fait) identiques à celles de la norme EN 954-1. Les catégories d'architecture désignée sont représentées dans les figures suivantes. Il est important de noter qu'elles peuvent s'appliquer à un système complet aussi bien qu'à un sous-système. Les schémas ne doivent pas nécessairement être perçus uniquement comme la représentation d'une structure physique, mais plutôt comme la représentation graphique des exigences conceptuelles.

Architecture désignée de Catégorie B

La Catégorie d'architecture désignée 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 mis en défaut en cas d'apparition d'une seule défaillance.
Voir la norme (EN) ISO 13849-1 pour l'ensemble des exigences applicables.

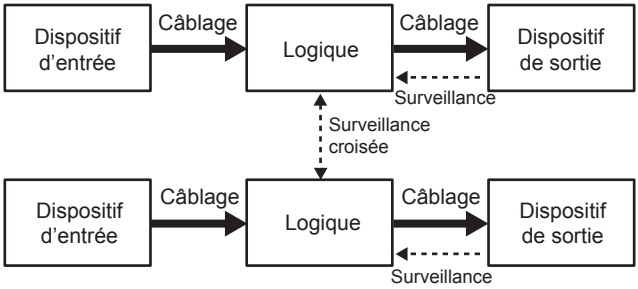
Architecture désignée de Catégorie 1

L'architecture désignée de catégorie 1 présente la même structure que celle de catégorie B. Elle peut également être mis en défaut en cas d'apparition d'une seule défaillance. Mais, étant donné qu'elle doit aussi 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 les exigences complètes.



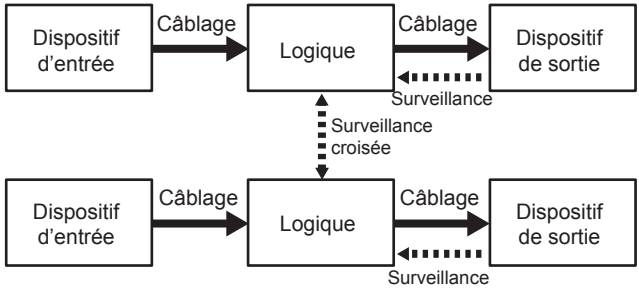
Architecture désignée de Catégorie 2

La Catégorie d'architecture désignée 2 doit utiliser des principes de sécurité de base (voir l'annexe de la norme (EN) ISO 13849-2). Une fonction de diagnostics de surveillance par l'intermédiaire de tests fonctionnels du système ou du sous-système, doit également être prévue. Ces tests doivent être effectués au démarrage, puis périodiquement selon une fréquence correspondant à au moins cent tests pour chaque sollicitation de la fonction de sécurité. La version 2015 remaniée ouvre la porte d'une exigence substitutive pour le passage de la fonction de sécurité à un état de sécurité avant le délai de sécurité de procédé. Une défaillance du système ou du sous-système reste possible si un seul défaut se produit entre les tests fonctionnels, mais cela est généralement moins probable que pour la Catégorie 1. Notez que pour la Catégorie 2 utilisée pour le niveau PLd il doit y avoir deux dispositifs de sortie de signal car, en cas de détection d'un défaut, la sortie de test doit déclencher un état de sécurité. Voir la norme (EN) ISO 13849-1 pour l'ensemble des exigences applicables.



Architecture désignée de Catégorie 3

La Catégorie d'architecture désignée 3 doit utiliser des principes de sécurité de base (voir les annexes de la norme (EN) ISO 13849-2). Elle est soumise également à la contrainte que le système ou le sous-système ne soit pas mis en défaut en cas d'apparition d'une seule défaillance. Cela signifie que le système devra présenter une tolérance à une défaillance unique pour sa fonction de sécurité. La façon la plus classique de répondre à cette exigence est d'utiliser une architecture à deux voies, comme illustré ci-dessus. De plus, il est également demandé que, chaque fois que c'est possible, cette défaillance unique soit détectée. Cette exigence est identique à celle imposée originellement pour la Catégorie 3 par la norme EN 954-1. Dans ce contexte, l'interprétation de l'expression « chaque fois que c'est possible » s'était avérée parfois problématique. Elle signifiait en effet que la Catégorie 3 pouvait accepter aussi bien un système redondant mais sans détection de défauts (souvent appelé de façon imagée mais juste « redondance aveugle ») qu'un système redondant dans lequel tous les défauts isolés sont détectés. Cette question a été réglée par la norme (EN) ISO 13849-1. Celle-ci impose en effet d'apprécier la qualité de couverture des tests de diagnostic (DC). Nous pouvons constater que plus la fiabilité [$MTTF_D$] du système sera élevée, plus ce taux DC sera faible. Toutefois, dans tous les scénarios, le taux DC doit être au minimum de 60 % pour l'architecture de Catégorie 3.



Architecture désignée de Catégorie 4

La Catégorie d'architecture désignée 4 doit utiliser des principes de sécurité de base (voir les annexes de la norme (EN) ISO 13849-2). Elle est soumise à un ensemble de contraintes

semblables à celles applicables à la Catégorie 3. Mais elle impose un niveau de surveillance plus élevé, c'est-à-dire un taux de couverture des tests de diagnostic supérieur. Ceci est indiqué par les pointillés en gras qui représentent les fonctions de surveillance. Sur le fond, la différence entre les Catégories 3 et 4 est la suivante : pour la Catégorie 3 la plupart des défauts doivent être détectés, alors que pour la Catégorie 4 tous les défauts dangereux individuels et toutes les combinaisons dangereuses de défauts doivent l'être systématiquement. Dans la pratique, cela passe généralement par un haut niveau de diagnostic afin de garantir la détection de tous les défauts pertinents avant une possible accumulation. Le taux de couverture des tests de diagnostic doit, dans ce cas, être au moins de 99 %.

Données de fiabilité

La norme (EN) ISO 13849-1 utilise des données de fiabilité quantifiées pour le calcul du niveau PL que devra assurer la partie sécurité d'un système de commande. La première interrogation que cela soulève est : « où pouvons-nous obtenir ces données » ? Il est toujours possible d'utiliser des données provenant de tables de fiabilité éprouvées. Mais la norme indique clairement que la source à privilégier est le fabricant. Dans cet esprit, Rockwell Automation met à disposition les informations pertinentes concernant ses produits sous forme d'une bibliothèque de données pour SISTEMA.
Avant de poursuivre, nous devons examiner les types de données nécessaires et également comprendre comment elles peuvent être produites.

Le type de données idéalement requis par la norme (et par SISTEMA) pour déterminer le niveau de performance PL est la probabilité de défaillance dangereuse par heure PFH. Il s'agit des mêmes données que celles employées dans la norme CEI 61508 et représentées par l'abréviation PFH_D employée dans la norme CEI/EN 62061.

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

Le tableau ci-dessus montre le rapport entre la valeur PFH_D et les niveaux PL et SIL. Pour certains sous-systèmes, la probabilité de défaillance dangereuse PFH_D est disponible directement auprès du fabricant. Cela facilite grandement les choses pour le calcul. Le fabricant devra généralement avoir effectué des calculs et/ou des tests relativement complexes sur ses sous-systèmes afin d'être en mesure de fournir cette information. Lorsque cette donnée n'est pas disponible, la norme (EN) ISO ISO13849-1 propose une alternative simplifiée. Elle repose sur la durée moyenne de fonctionnement avant défaillance dangereuse ($MTTF_D$) d'un système mono-voie. Le niveau PL (et donc la valeur PFH_D) d'un système ou sous-système peut ensuite être calculé en utilisant

la méthodologie et les formules de la norme. Ceci sera même réalisé plus facilement encore à l'aide de SISTEMA.

REMARQUE : il est important de retenir que, pour un système à deux voies (avec ou sans diagnostics), il n'est pas permis d'utiliser le rapport 1/PFH_D pour déterminer la valeur $MTTF_D$ exigée par la norme (EN) ISO 13849-1. Cette norme ne fait référence qu'à la valeur $MTTF_D$ d'un système mono-voie. Cette valeur sera différente de la valeur $MTTF_D$ combinée 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.

$MTTF_D$ d'un système mono-voie

Cette valeur représente le temps moyen avant l'apparition d'un défaut pouvant entraîner la défaillance de la fonction de sécurité. Elle est exprimée en années. Il s'agit de la valeur moyenne des $MTTF_D$ des « blocs » de chaque voie et s'applique à un système aussi bien qu'à un sous-système. La norme fournit la formule suivante pour le calcul de la moyenne des $MTTF_D$ de chaque élément utilisé dans un système ou un sous-système mono-voie.

A ce niveau, la valeur ajoutée de SISTEMA apparaît évidente. Les utilisateurs économisent le temps passé à la consultation des tables et le calcul des formules puisque ces tâches sont effectuées par le logiciel. Les résultats finaux peuvent être imprimés sous forme d'un rapport en 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 deux voies, celles-ci sont identiques. En conséquence, le résultat de la formule peut s'appliquer à l'une ou l'autre voie.

Si les voies du système ou du sous-système sont différentes, la norme fournit une autre formule pour traiter ce cas.

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

Elle revient en fait à faire la moyenne des deux moyennes. A des fins de simplification, il est également permis d'utiliser uniquement la valeur de voie la plus défavorable.

La norme classe les $MTTF_D$ selon trois niveaux, comme indiqué ci-dessous :

Évaluation de la valeur $MTTF_D$ de chaque voie	**Plage de la valeur $MTTF_D$ de chaque voie**
Faible	3 ans <= $MTTF_D$ < 10 ans
Moyen	10 ans <= $MTTF_D$ < 30 ans
Élevé	30 ans <= $MTTF_D$ < 100 ans

Niveaux de valeur $MTTF_D$

Il est à noter que la norme (EN) ISO 13849-1 limite la valeur $MTTF_D$ pratique d'un sous-système mono-voie à 100 ans maximum, même si les valeurs réelles déterminées par le calcul peuvent s'avérer parfois bien supérieures.

Comme nous le verrons plus loin, la plage de valeur $MTTF_D$ moyenne ainsi obtenue sera ensuite combinée avec la Catégorie d'architecture désignée et le taux de couverture des tests de diagnostic (DC) afin d'obtenir une estimation provisoire du niveau PL. Le terme « provisoire » est utilisé ici parce que d'autres exigences, notamment l'intégrité systématique et les mesures contre les causes de défaillance communes, devront encore être satisfaites lorsque cela est nécessaire.

Méthodes de détermination des données

Il est maintenant nécessaire d'examiner un peu plus en détail comment les fabricants déterminent leurs données sous la forme de valeur PFH_D ou $MTTF_D$. La compréhension de ce processus est essentielle pour pouvoir utiliser à bon escient ces données constructeur. Les composants peuvent être regroupés en trois types fondamentaux :

- Mécaniques (électromécaniques, mécaniques proprement-dits, pneumatiques, hydrauliques, etc.)
- Électroniques (utilisant notamment des semi-conducteurs)
- Logiciels

Il existe des différences fondamentales entre les mécanismes de défaillance commune de ces différents types de technologies. Sur le fond, on peut les résumer de la façon suivante :

Technologie mécanique :

La défaillance sera proportionnelle à la fois à la fiabilité intrinsèque et au taux d'utilisation. Plus le taux d'utilisation sera élevé, plus les composants auront une chance de se trouver altérés et de tomber en panne. Il convient de noter que ce facteur ne constitue pas la seule cause de défaillance, mais à moins de limiter le temps et les cycles de fonctionnement, il sera prédominant. Il va de soit qu'un contacteur ayant un cycle de commutation d'une fois toutes les dix secondes garantira un fonctionnement fiable bien moins longtemps que le même contacteur fonctionnant une seule fois par jour.

Les dispositifs de type matériel incorporent généralement des composants conçus individuellement pour une utilisation spécifique. Ces composants ont été formés, moulés,

coulés, usinés, etc. Ils ont ensuite été combinés entre eux au moyen d'assemblages, de ressorts, d'aimants, de bobines électriques, etc. afin de constituer un mécanisme. Etant donné que ces composants de base ne disposent généralement pas d'historique d'utilisation dans d'autres applications, il ne sera pas possible d'obtenir des données de fiabilité préexistantes les concernant. L'estimation de la valeur PFH_D ou $MTTF_D$ pour le mécanisme est normalement basée sur des tests. Les deux normes EN/CEI 62061 et (EN) ISO 13849-1 préconisent un procédé de test appelé test $B10_D$.

Dans le test $B10_D$, un certain nombre d'échantillons du dispositif (généralement au moins dix) sont testés dans des conditions représentatives. Le nombre moyen de cycles de fonctionnement obtenus avant que 10 % de ces échantillons présentent une défaillance entraînant une situation dangereuse est désigné comme valeur B10d. Dans la pratique, il est fréquent que tous les échantillons tombant en panne passent en fait dans un état de sécurité. Mais dans ce cas, la norme stipule que la valeur B10d (danger) peut être considérée comme égale à deux fois la valeur B10.

Technologie électronique :

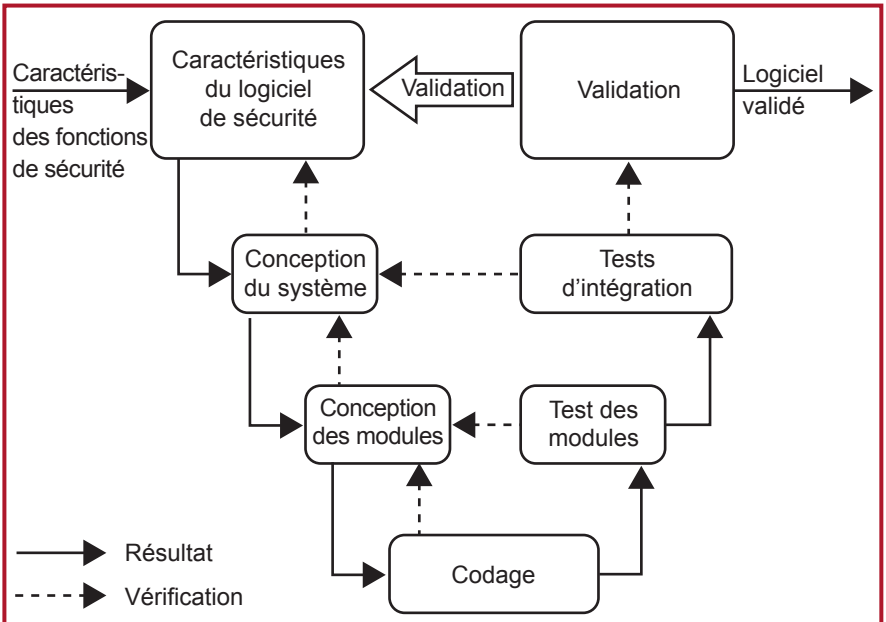
Il n'existe aucune détérioration physique due à la présence de pièces en mouvement. En supposant un environnement de fonctionnement conforme aux caractéristiques électriques et thermiques spécifiées, la cause de défaillance principale d'un circuit électronique sera liée à la fiabilité intrinsèque de ses composants (ou, plus exactement, à leur manque de fiabilité). De nombreuses raisons peuvent être à l'origine de la défaillance de composants individuels : imperfections introduites pendant la fabrication, surtensions excessives, problèmes de liaison mécanique, etc. En général, les défaillances de composants électroniques sont imputables à une charge, à un délai et à la température, mais sont difficiles à prévoir par analyse et elles apparaissent comme étant de nature aléatoire. En conséquence, le test d'un dispositif électronique en laboratoire ne révélera pas nécessairement de profils types de défaillance à long terme.

Pour déterminer la fiabilité de ces dispositifs électroniques, il faudra donc généralement avoir recours à l'analyse et au calcul. Il est possible de trouver des données pertinentes pour les composants spécifiques dans des tableaux de données de fiabilité. Il est également possible de déterminer les modes de défaillance dangereux d'un composant par l'analyse. Il est admis et courant d'établir une moyenne pondérée entre les modes de défaillance de sécurité (50 %) et dangereux (50 %) du composant. Cela produit généralement un résultat de type plutôt « conservateur ».

La norme CEI 61508 fournit des formules pouvant être utilisées pour le calcul de la probabilité globale de défaillance dangereuse PFH ou PFD du dispositif (c'est-à-dire, du sous-système). Ces formules sont très complexes et prennent en compte (lorsqu'applicable) la fiabilité du composant, les risques de défaillance de cause commune (coefficient bêta), le taux de couverture des tests de diagnostic (DC), l'intervalle entre les tests fonctionnels et l'intervalle entre les tests de validité. La bonne nouvelle est que ces calculs complexes seront normalement réalisés par le fabricant du dispositif ! Les deux normes EN/CEI 62061 et (EN) ISO 13849-1 acceptent qu'un sous-système soient calculé selon les formules de la norme CEI 61508. La valeur PFH_D résultante est utilisable directement selon l'annexe K de la norme (EN) ISO 13849-1 ou dans l'outil de calcul SISTEMA.

Technologie logicielle :

Les défaillances logicielles sont par nature intrinsèquement systémiques. Toute défaillance sera imputable au mode de conception, d'écriture ou de compilation du logiciel. Par conséquent les défaillances ne pourront être causées que par le système dans lequel elles se produisent, et non par son utilisation. Pour maîtriser ces défaillances, il faut donc maîtriser le système. Les deux normes CEI 61508 et (EN) ISO 13849-1 définissent des exigences et des méthodologies pour cela. Il n'est pas nécessaire d'entrer dans le détail ici. On retiendra simplement qu'elles utilisent un modèle en V classique. Le logiciel intégré est un point non négligeable pour le concepteur du dispositif. L'approche traditionnelle consiste à développer le logiciel intégré conformément aux méthodes formelles définies dans la partie 3 de la norme CEI 61508. Concernant le programme d'application, c'est-à-dire le logiciel permettant à l'utilisateur de dialoguer avec le système, la majorité des dispositifs de sécurité programmables sont fournis avec des blocs fonctionnels ou sous-programmes « certifiés ». Cela simplifie les tâches de validation du programme d'application. Car il ne faut pas oublier qu'une fois ce programme d'application terminé, il devra toujours être validé. La façon dont les blocs sont reliés entre eux et paramétrés doit être contrôlée et validée par rapport à la tâche prévue. Les deux normes (EN) ISO 13849-1 et CEI/EN 62061 fournissent des recommandations pour cette procédure.



Modèle en V pour le développement du logiciel

Taux de couverture des tests de diagnostic

Nous avons déjà abordé ce point lorsque nous avons traité des Catégories d'architecture désignée 2, 3 et 4. Ces Catégories requièrent en effet certains tests de diagnostic afin de vérifier que la fonction de sécurité est toujours active. L'expression « taux de couverture des tests de diagnostic » (traditionnellement désigné par DC) est utilisée pour caractériser l'efficacité de ces tests. Il est important de réaliser que le taux DC n'est pas basé uniquement sur le nombre de composants pouvant présenter une défaillance dangereuse. Il prend en compte le taux de défaillance dangereuse total. Le symbole λ est utilisé pour désigner ce « taux de défaillance ». DC exprime la relation entre les taux d'apparition des deux types suivants de défaillance dangereuse :

Les **défaillances dangereuses détectées [λdd]**, c'est-à-dire les défauts susceptibles de provoquer ou de conduire à une perte de la fonction de sécurité, mais qui sont détectés. Après cette détection, une fonction de réaction au défaut entraînera le passage du dispositif ou du système à l'état de sécurité.

La **défaillance dangereuse [λd]**, c'est-à-dire l'ensemble des défauts pouvant potentiellement provoquer ou conduire à une perte de la fonction de sécurité. Elle inclut donc les défauts détectés et ceux qui ne le sont pas. Évidemment, les défauts réellement dangereux sont ceux qui ne sont pas détectés (désignés par λdu].

La valeur DC est fournie par la formule :
DC = λdd/λd (exprimé en pourcentage).

La définition du taux de couverture des tests de diagnostic DC est commune aux normes (EN) ISO 13849-1 et EN/CEI 62061. Cependant, son mode de calcul diffère. La seconde norme propose un calcul basé sur l'analyse du mode de défaillance, mais permet aussi d'employer la méthode simplifiée sous forme de tables de référence telles que celles fournies par la norme (EN) ISO 13849-1. Diverses techniques de diagnostic courantes y sont listées avec, en regard, le taux DC qu'elles sont supposées permettre d'obtenir. Dans certains cas, une analyse rationnelle reste cependant nécessaire. Pour certaines de ces techniques en effet, le taux de couverture des tests de diagnostic DC obtenu sera fonction de la fréquence à laquelle le test est effectué. Cette approche a été parfois critiquée comme étant trop imprécise. Dans la pratique, l'estimation du taux DC sera influencée par un grand nombre de variables. Quelle que soit la technique utilisée, le résultat ne pourra donc en général pas prétendre à un autre qualificatif qu'approximatif.

Il est aussi important de savoir que les tables de référence de la norme (EN) ISO 13849-1 sont le produit de recherches complètes réalisées par l'IFA à partir des résultats fournis par des techniques de diagnostic éprouvées sur des applications réelles. Dans un esprit de simplification, la norme répartit les valeurs DC selon quatre niveaux d'efficacité de base :

< 60 % = aucun
60 % à <90 % = faible
90 % à <99 % = moyen
≥99 % = élevé

Cette approche par niveaux d'efficacité plutôt qu'en valeurs de pourcentage spécifiques peut également être considérée comme plus réaliste en termes de précision. L'outil SISTEMA utilise les mêmes tables de référence que la norme. Avec le développement de l'utilisation de composants électroniques complexes dans les dispositifs de sécurité, le facteur DC devient de plus en plus important. Il est à penser que les évolutions futures des normes apporteront des approfondissements sur ce point. En attendant, une analyse technique rationnelle et un peu de bon sens devraient être suffisants pour faire le choix optimal du niveau d'efficacité DC.

Défaillance de cause commune

Dans la plupart des systèmes ou sous-systèmes à deux voies (c'est-à-dire, ne tolérant qu'un seul défaut), le principe du diagnostic est basé sur le postulat qu'il ne se produira pas de défaillances dangereuses sur les deux voies en même temps. L'expression « en même temps » peut être formulée de façon plus exacte ainsi : « dans l'intervalle entre les tests de diagnostic ». Si cet intervalle entre les tests de diagnostic est raisonnablement court (par exemple, inférieur à huit heures), il est raisonnable de considérer que deux défauts distincts et non liés auront peu de chance de se produire dans ce laps de temps. Cependant, la norme précise clairement qu'il faut bien s'assurer que les possibilités d'apparition du défaut soient distinctes et non liées. Par exemple, si la défaillance d'un composant peut entraîner de façon prévisible la défaillance d'autres composants, la résultante de ces différents défauts combinés sera considérée comme un défaut unique.

Il est également possible qu'un évènement entraînant la défaillance d'un composant particulier soit susceptible de provoquer la défaillance d'autres composants. C'est ce qu'on appelle une « défaillance de cause commune » (habituellement désignée par l'acronyme CCF). La propension d'apparition d'une défaillance CCF est habituellement symbolisée par le coefficient bêta (β). Il est très important que les concepteurs de sous-systèmes et de systèmes soient sensibilisés aux possibilités d'apparition de défaillances CCF. Il existe de nombreux types de défaillances CCF et, par conséquent, de nombreuses façons de les éviter. La norme (EN) ISO 13849-1 propose une alternative raisonnable entre les extrêmes que constituent une trop grande complexité et une trop grande simplification. De la même façon que la norme EN/CEI 62061 qui adopte, quant à elle, une approche essentiellement qualitative. Elle propose une liste de mesures reconnues comme efficaces dans la prévention des défaillances CCF.

N°	Mesure contre les défaillances de cause commune	Note
1	Séparation/isolement	15
2	Diversification	20
3	Conception/application/expérience	20
4	Évaluation/analyse	5
5	Compétence/formation	5
6	Environnement	35

Système d'évaluation des défaillances de cause commune

Un nombre approprié de ces mesures devra être mis en œuvre dans la conception du système ou du sous-système. On pourra rétorquer légitimement que le seul recours à cette liste n'est certainement pas suffisant pour prévenir tout risque d'apparition de défaillances CCF. Néanmoins, si l'esprit de cette liste est bien compris, il apparaîtra clairement que son premier objectif est d'inciter le concepteur à analyser les risques d'apparition de défaillances CCF et à mettre en œuvre les mesures de prévention appropriées en fonction de la technologie et des caractéristiques de l'application prévue. L'utilisation de la liste force à prendre en compte un certain nombre de techniques fondamentales permettant d'obtenir une efficacité maximum. La diversité des modes de défaillance et des compétences de conception seront ainsi mises en évidence. L'outil SISTEMA de l'IFA se base également sur les tables de référence de recherche CCF de la norme et les présente sous une forme très pratique à utiliser.

Défauts systématiques

Nous avons déjà évoqué la question de la quantification des données de fiabilité de sécurité dans le cadre de la $MTTF_D$ et de la probabilité de défaillance dangereuse. Cependant, cette question a d'autres ramifications. Lorsque nous avons utilisé ces termes, nous faisions référence qu'aux défauts aléatoires par nature. En effet, la norme CEI/EN 62061 parle spécifiquement de probabilité de défaillance matérielle aléatoire (ou PFH_D. Mais il existe un type de défauts, génériquement appelés « défauts systématiques », qui peuvent découler d'erreurs commises au niveau de la conception ou du processus de fabrication. Un exemple classique en est fourni par les erreurs de programmation logicielle. Dans son Annexe G, la norme définit des mesures destinées à éviter ces erreurs (et donc les défaillances induites). Ces mesures incluent des dispositions telles que l'utilisation de matériaux et de techniques de fabrication adaptés, des revues de conception, l'analyse et la modélisation sur ordinateur. Il existe également des évènements prévisibles et des caractéristiques susceptibles d'apparaître dans l'environnement d'utilisation qui pourront provoquer des défaillances si leurs effets potentiels ne sont pas sous contrôle. L'Annexe G propose également des mesures à ce niveau. Par exemple, il est facile de prévoir qu'il pourra se produire des pertes occasionnelles d'alimentation. En conséquence, la mise hors tension des composants devra entraîner la mise en sécurité du système. Ces mesures peuvent sembler relever du simple bon sens, et c'est le cas. Elles n'en sont pas moins essentielles. Toutes les autres réquisitions de la norme deviennent sans objet si la surveillance et la prévention des défaillances systématiques ne sont pas considérées avec l'importance qu'elles méritent. Cela nécessite parfois également des mesures de même type que celles utilisées pour le contrôle des défaillances matérielles aléatoires (afin de garantir le niveau de PFH_D souhaité), comme les tests de diagnostic automatiques et l'utilisation de matériels redondants.

Exclusion de défauts

L'un des outils fondamentaux pour l'analyse des systèmes de sécurité est l'analyse des défaillances. Le concepteur et l'utilisateur doivent comprendre comment le système de sécurité va fonctionner en présence de défauts. De nombreuses techniques existent pour réaliser cette analyse. Citons par exemple, l'analyse de l'arbre des défaillances, des modes de défaillance, de leurs effets et de leur criticité, l'analyse de l'arborescence des évènements et la revue des charge et des résistances.

Au cours de cette analyse, il sera possible de découvrir certains défauts ne pouvant pas être détectés par les tests de diagnostic automatiques (à moins d'impliquer des coûts économiques disproportionnés). De plus, la probabilité d'apparition de ces défauts pourra être rendue extrêmement faible grâce à des méthodes de limitation au niveau de la conception, de la construction et des tests. Dans ces conditions, certains défauts pourront être exclus du champ de surveillance. L'exclusion de défaut consiste à négliger délibérément un défaut dont la probabilité d'apparition dans le système de commande de sécurité (SRCS) sera négligeable.

La norme (EN) ISO 13849-1 autorise l'exclusion de défauts sur la base de l'improbabilité technique de leur apparition, de l'expérience technique généralement reconnue et des exigences techniques relatives à l'application. La norme (EN) ISO 13849-2 fournit quant à elle des exemples et des justifications d'exclusion de certains défauts dans des systèmes électriques, pneumatiques, hydrauliques et mécaniques. Les exclusions de défauts doivent être déclarées et justifiées de façon détaillée dans la documentation technique.

Il sera dans certains cas impossible d'évaluer un système de commande de sécurité sans supposer que certains défauts puissent être exclus. Pour plus d'informations sur l'exclusion de défauts, se reporter à la norme ISO 13849-2.

Plus le niveau de risque devient important, plus la justification de l'exclusion de défauts devient rigoureuse. En général, lorsqu'un niveau PLe est requis pour la mise en œuvre d'une fonction de sécurité par un système de commande de sécurité, il n'est pas normal de s'appuyer uniquement sur les exclusions de défauts pour obtenir ce niveau de performance. Cela dépendra de la technologie utilisée et de l'environnement de travail prévu. Il est donc essentiel que les concepteurs attachent une importance accrue à la définition des exclusions de défauts lorsque les exigences de niveau de performance PL augmentent.

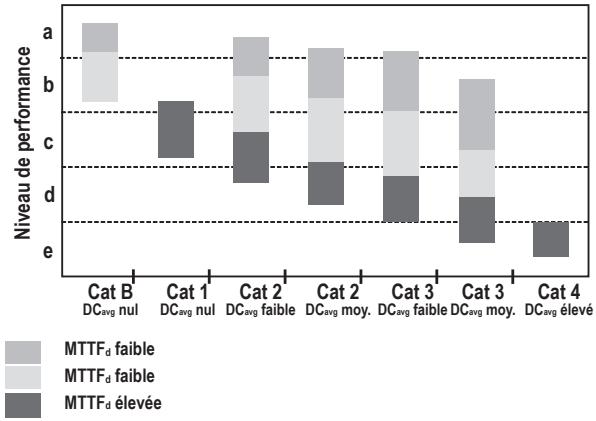
Niveau de performance (PL)

Le niveau de performance est une valeur discrète qui définit la capacité des composants de sécurité du système de commande à exécuter une fonction de sécurité.

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

- La $MTTF_D$ (durée moyenne de fonctionnement avant défaillance dangereuse de chaque voie)
- Le taux DC (couverture des tests de diagnostic).
- L'Architecture (la Catégorie)

Le schéma suivant présente une méthode graphique pour déterminer le niveau PL en combinant ces facteurs. Le tableau à l'annexe K présente les résultats de différents modèles de Markov ayant servi de base à ce schéma. On se référera à ce tableau lorsqu'une estimation plus précise est nécessaire.



Détermination graphique du niveau de performance PL

D'autres conditions sont également à satisfaire pour atteindre le niveau PL requis. Elles comprennent les dispositions relatives aux défaillances de cause commune, aux défaillances systématiques, aux conditions ambiantes et au temps de mission. Si la valeur PFH_D du système ou du sous-système est connue, les tableaux à l'annexe K peuvent servir à dériver le niveau PL.

Conception et combinaison de sous-systèmes

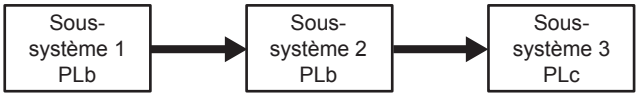
Les sous-systèmes conformes au niveau PL sont combinables en un système au moyen du tableau comme illustré.

PLlow	**N**low	**PL**
a	> 3	non autorisé
	≤3	a
b	> 2	a
	≤2	b
c	> 2	b
	≤2	c
d	> 3	c
	≤3	d
e	> 3	d
	≤3	e

Calcul du niveau de performance PL dans le cas de sous-systèmes associés en série

L'utilisation de ce tableau issu de la norme n'est pas obligatoire. Il vise simplement à fournir une méthode alternative très simple de scénario le plus défavorable si les valeurs PFHd ne sont pas connues. Le niveau PL du système peut être calculé par d'autres méthodes, y compris avec l'outil SISTEMA. Le principe du tableau est simple à comprendre. Premièrement, la valeur du système est celle de son sous-système le plus faible. Deuxièmement, plus il y a de sous-systèmes, plus la possibilité de pannes est grande.

Dans le système présenté ci-dessous en exemple, les niveaux de performances les plus faibles sont ceux des sous-systèmes 1 et 2. Tous deux sont en effet de niveau PLb. En conséquence, en suivant la ligne b (au niveau de la colonne PLlow), puis la ligne « inférieur ou égal à 2 » (au niveau de la colonne Nlow) sur le tableau, nous trouvons que le niveau PL global du système est b (dans la colonne PL). Si les trois sous-systèmes étaient de niveau PLb, le niveau PL global obtenu serait PLa.



Combinaison de sous-systèmes en série dans un système de niveau PLb

Validation

La validation des fonctions de sécurité inclut et va au-delà de la vérification des niveaux de performance atteints. L'objectif est de s'assurer que la fonction de sécurité mise en œuvre prend en fait en compte les exigences de sécurité globales des machines. La validation joue un rôle très important dans les processus de développement et de mise en service du système de sécurité. La norme ISO/EN 13849-2:2012 définit les règles de cette validation. Elle fait appel à un plan de validation et propose pour réaliser ces validations des techniques de test et d'analyse, comme l'analyse de l'arbre des défaillances ou l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC). La plupart de ces exigences s'appliquent généralement au fabricant du sous-système plutôt qu'à son utilisateur.

Mise en service de la machine

Lors de la phase de mise en service du système ou de la machine, la validation des fonctions de sécurité doit être exécutée dans tous les modes de fonctionnement. Elle doit inclure toutes les situations normales ainsi que les situations anormales prévisibles. Les différentes combinaisons d'entrées et de séquences de fonctionnement doivent également être prises en compte. Cette procédure est importante. Il est en effet nécessaire de toujours vérifier l'adéquation du système aux conditions de fonctionnement et d'environnement réelles. Certaines de ces conditions en effet peuvent s'avérer différentes de celles qui avaient prévues lors de la conception.

Chapitre 8 : Conception du système selon la norme CEI/EN 62061

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

L'évaluation des risques débouche sur une stratégie de réduction des risques. Celle-ci permet à son tour d'identifier les fonctions de commande de sécurité nécessaires. Ces fonctions doivent être décrites en intégrant les éléments suivants :

- les spécifications des exigences fonctionnelles ;
- les spécifications des exigences d'intégrité de sécurité.

Les exigences fonctionnelles regroupent un certain nombres de points comme la fréquence de fonctionnement, le temps de réponse nécessaire, les modes de fonctionnement, les cycles de travail, les conditions d'utilisation et les fonctions de réaction aux défauts. Les exigences d'intégrité de sécurité sont classées selon différents niveaux appelés niveaux d'intégrité de sécurité SIL (Safety Integrity Level). En fonction de la complexité du système, tout ou partie des éléments du tableau ci-dessous devront être pris en compte pour déterminer si la configuration du système est conforme à la classification SIL nécessaire.

Éléments à prendre en compte pour la classification SIL	**Symbole**
Probabilité de défaillance dangereuse par heure	PFH_D
Tolérance aux pannes matérielles	HFT
Proportion de défaillances non dangereuses	SFF
Intervalle entre tests de validité	T_1
Intervalle entre tests de diagnostic	T_2
Sensibilité aux défaillances de cause commune	β
Taux de couverture des tests de diagnostic	DC

Éléments à prendre en compte pour la détermination du niveau SIL

Sous-systèmes

Le terme « sous-système » a une signification particulière dans la norme CEI/EN 62061. C'est le premier niveau de la décomposition d'un système en sous-parties qui, si elles viennent à se mettre en défaut, entraîneront la défaillance de la fonction de sécurité. Par conséquent, si deux interrupteurs redondants sont utilisés dans un système, ces interrupteurs ne constituent pas individuellement un sous-système. C'est l'ensemble de ces deux interrupteurs et les éventuelles fonction de diagnostic associées qui constitue le sous-système.

Probabilité de défaillance dangereuse par heure (PFH_D)

La norme CEI/EN 62061 utilise les mêmes méthodes de base que celles présentées dans le chapitre relatif à la norme (EN) ISO 13849-1 pour déterminer le taux de défaillance au niveau des composants. Des dispositions et des méthodes identiques s'appliquent aux composants « mécaniques » et électroniques. Dans la norme CEI/EN 62061 il n'est cependant pas fait référence à une valeur $MTTF_D$ exprimée en années. Le taux de défaillance horaire (λ) sera calculé soit directement, soit au moyen, ou à partir, de la valeur B10 selon la formule suivante :

λ = 0.1 x C/B10 (dans laquelle C = nombre de cycles de fonctionnement par heure)

Il existe une différence de méthodologie significative entre les deux normes pour la détermination de la valeur PFH_D totale d'un sous-système ou d'un système. Une analyse des composants doit ici être réalisée afin de déterminer la probabilité de défaillance des sous-systèmes. Des formules simplifiées sont fournies pour le calcul des architectures courantes de sous-système (décrites plus loin). Lorsque ces formules ne sont pas adaptées, il sera nécessaire d'utiliser des méthodes de calcul plus complexes, comme les modèles de Markov. Les probabilités de défaillance dangereuse (PFH_D) de chaque sous-système seront alors additionnées pour déterminer la valeur PFH_D totale du système. Le tableau 3 dans la norme peut alors servir à déterminer le niveau d'intégrité de sécurité SIL adapté à cette valeur PFH_D.

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

Probabilité de défaillance dangereuse par rapport aux niveaux SIL

Les données de PFH_D d'un sous-système sont généralement fournies par le fabricant du matériel. Des données pour les systèmes et composants de sécurité de Rockwell Automation sont disponibles sur le site Internet suivant :

www.rockwellautomation.com, sous Solutions & Services > Safety Solutions.

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

Pour les dispositifs électromécaniques peu complexes, le mécanisme d'apparition de panne est généralement lié au nombre et à la fréquence des opérations plutôt qu'au temps simplement. Par conséquent, pour ces composants, les données sont obtenues à partir de tests types (par exemple, le test B10 décrit dans le chapitre sur la norme (EN) ISO 13849-1). Des informations relatives à l'application, comme le nombre de cycles de fonctionnement attendus par an, seront alors nécessaires pour convertir la valeur B10d, ou les données similaires, en valeur PFH_D.

REMARQUE : la relation suivante est généralement vérifiée (sous réserve de l'application éventuelle d'un facteur de conversion des années en heures) :

$PFH_D = 1/MTTF_D$

Toutefois, il est important de retenir que, pour un système à deux voies (avec ou sans diagnostics), il n'est pas permis d'utiliser le rapport $1/PFH_D$ pour déterminer la valeur $MTTF_D$ exigée par la norme (EN) ISO 13849-1. Cette norme ne fait référence qu'à la valeur $MTTF_D$ d'un système mono-voie. Cette valeur sera différente de la valeur $MTTF_D$ combinée des deux voies d'un sous-système à deux voies, y compris l'incidence du taux de couverture des tests de diagnostic.

Contraintes architecturales

La particularité essentielle de la norme CEI/EN 62061 est la division du système de sécurité en sous-systèmes. Le niveau d'intégrité de sécurité du matériel revendiqué par un sous-système est non seulement limité par la valeur PFH_D, mais aussi par sa tolérance aux défauts matériels et sa proportion de défaillances non dangereuse (SFF). La tolérance aux défauts matériels définit la capacité du système à exécuter sa fonction en présence de défauts. Une tolérance aux défauts égale à zéro signifie que la fonction ne sera plus exécutée dès lors qu'un seul défaut se produira. Une tolérance aux défauts de un autorisera le sous-système à exécuter sa fonction en présence d'un défaut unique. La proportion de défaillances non dangereuses (SFF) représente la fraction du nombre de défauts total n'entraînant pas de défaillance dangereuse. La combinaison de ces deux éléments constitue ce qu'on appelle la contrainte architecturale. Elle détermine le niveau SIL maximum réalisable ou SIL CL. Le tableau suivant présente cette relation entre la contrainte architecturale et le niveau SIL CL. Un sous-système (et donc son système) doit respecter à la fois les exigences de PFH_D et les contraintes architecturales, de même que toutes les autres dispositions applicables de la norme.

Proportion de défaillances non dangereuses (SFF)	Tolérance aux pannes matérielles		
	0	1	2
< 60 %	Non autorisé sauf exception particulière	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL3
≥ 99 %	SIL3	SIL3	SIL3

Contraintes architecturales et niveaux SIL

Par exemple, une architecture de sous-système possédant une tolérance à un seul défaut et une proportion de défaillances non dangereuses de 75 % sera limitée à un niveau maximal SIL 2, quelle que soit sa probabilité de défaillance dangereuse. Lorsque des sous-systèmes sont combinés, le niveau SIL global du système SRCS résultant sera limité à un niveau inférieur ou égal au niveau SIL CL le plus bas de tous les sous-systèmes participant à la fonction de commande de sécurité.

Réalisation du système

Pour calculer la probabilité de défaillance dangereuse, chaque fonction de sécurité doit être décomposée en blocs fonctionnels qui seront ensuite utilisés comme base des sous-systèmes. La conception traditionnelle d'un système destiné à l'exécution d'une fonction de sécurité consiste en un dispositif de détection connecté à un dispositif logique lui-même connecté à un actionneur. Ceci constitue une disposition en série de ces sous-systèmes. Comme nous l'avons vu précédemment, si nous pouvons déterminer la probabilité de défaillance dangereuse de chaque sous-système et connaître son niveau SIL CL, il sera alors facile de calculer la probabilité de défaillance du système en additionnant les probabilités de défaillance de chacun de ses sous-systèmes. Ce principe est illustré ci-dessous.

SOUS-SYSTÈME 1 Détection de position	SOUS-SYSTÈME 2 Résolution de programme	SOUS-SYSTÈME 3 Actionneurs de sortie
Exigences fonctionnelles et d'intégrité de la norme CEI/EN 62061	Exigences fonctionnelles et d'intégrité de la norme CEI/EN 62061	Exigences fonctionnelles et d'intégrité de la norme CEI/EN 62061
Contraintes architecturales SIL CL 2	Contraintes architecturales SIL CL 2	Contraintes architecturales SIL CL 2
$PFH_D = 1 \times 10^{-7}$	$PFH_D = 1 \times 10^{-7}$	$PFH_D = 1 \times 10^{-7}$
$= PFH_D^1$ $= 1 \times 10^{-7}$ $= 3 \times 10^{-7}$, c.-à-d., convenant pour SIL 2	$+ PFH_D^2$ $+ 1 \times 10^{-7}$	$+ PFH_D^3$ $+ 1 \times 10^{-7}$

Si, par exemple, nous souhaitons obtenir un niveau SIL 2, chaque sous-système doit avoir un niveau d'intégrité maximum SIL CL d'au moins SIL 2. La somme des probabilités de défaillance dangereuse (PFH_D) du système ne doit par ailleurs pas dépasser la limite indiquée dans le précédent tableau « Probabilité de défaillance dangereuse par rapport aux niveaux SIL ».

Conception de sous-système selon la norme CEI/EN 62061

Lorsque le concepteur du système utilise des composants déjà « prêt à l'emploi » dans des sous-systèmes conformes à la norme CEI/EN 62061, les choses deviennent beaucoup plus simples car les exigences propres à la conception des sous-systèmes ne s'appliqueront pas dans ce cas. Ces exigences sont, en général, déjà intégrées par le fabricant du dispositif (sous-système). C'est un avantage car elles sont bien plus complexes que celles requises pour la conception du système proprement-dit.

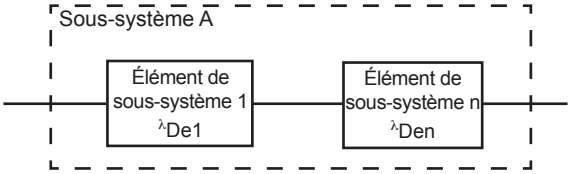
La norme CEI/EN 62061 impose que les sous-systèmes complexes comme les automates de sécurité soient conformes à la norme CEI 61508 ou aux autres normes applicables. Cela implique que les dispositifs utilisant des composants électroniques programmables complexes bénéficieront de toute la rigueur de la norme CEI 61508.

Or, son application est parfois très stricte et exigeante. Par exemple, l'évaluation de la probabilité de défaillance dangereuse PFH_D d'un sous-système complexe peut s'avérer un processus très complexe faisant appel à des techniques comme les modèles de Markov, les schémas fonctionnels de fiabilité ou l'analyse de l'arbre des défaillances.

La norme CEI/EN 62061 définit des règles applicables à la conception des sous-systèmes de moindre complexité. Sont habituellement concernés des composants électriques relativement simples, comme les interrupteurs d'interverrouillage et les relais de surveillance de sécurité électromécaniques. Les exigences ne sont pas aussi « pointues » que celles de la norme CEI 61508. Mais leur application peut cependant s'avérer très délicate.

La norme CEI/EN 62061 retient quatre architectures logiques de sous-système et propose des formules de calcul correspondantes. Celles-ci peuvent servir à évaluer la probabilité de défaillance dangereuse (PFH_D) d'un sous-système de faible complexité. Ces architectures sont purement des représentations logiques. Elles ne doivent pas être considérées comme des architectures physiques. Ces quatre architectures sont résumées dans les schémas suivants.

Pour les architectures de sous-système de base représentées ci-dessous, les probabilités de défaillance dangereuse s'ajoutent simplement les unes aux autres.

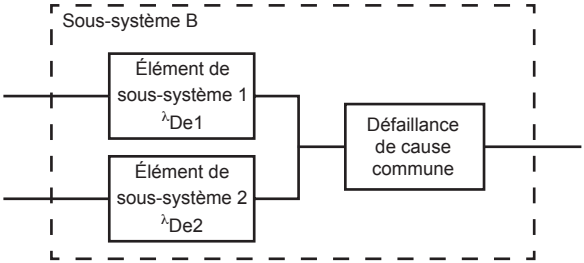


Architecture de sous-système logique de type A

$\lambda DssA = \lambda De1 + \ldots + \lambda Den$
$PFHDssA = \lambda DssA$

λ (lambda) sert à indiquer le taux de défaillance. L'unité de mesure de ce taux de défaillance est le nombre de défaillances par heure. λD indique le taux de défaillances dangereuses. λ_{DssA} désigne quant à lui le taux de défaillance dangereuse du sous-système A ; c'est la somme des taux de défaillance des éléments individuels, e1, e2, e3, à en inclus. La probabilité de défaillance dangereuse est multipliée par 1 heure pour créer la probabilité de défaillance par heure.

Le schéma suivant présente un système à tolérance de défaut unique sans fonction de diagnostic. Lorsque l'architecture n'a ainsi qu'une tolérance de défaut unique, il existe un risque potentiel de défaillance de cause commune à prendre en considération. Les effets des défaillances de cause commune sont brièvement décrits plus loin dans ce chapitre.



Architecture de sous-système logique de type B

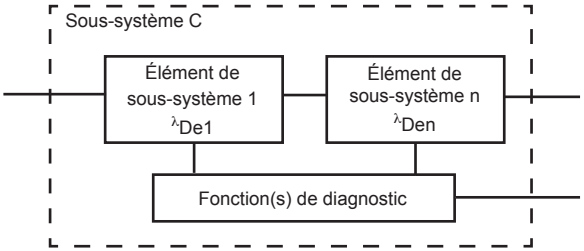
$DssB = (1-\beta)^2 \times \lambda De1 \times \lambda De2 \times T1 + \beta \times (\lambda De1 + \lambda De2)/2$
PFHDssB = λDssB

La formule propre à cette architecture intègre l'agencement en parallèle des éléments du sous-système et agrège les deux éléments suivants provenant du précédent tableau « Éléments à prendre en compte pour la détermination du niveau SIL ».

β – la sensibilité aux défaillances de cause commune (bêta) ;

T1 – l'intervalle entre les tests de validité ou la durée vie (la plus petite valeur des deux). Les tests de sécurité sont conçus pour détecter les défauts et les détériorations de fonctionnement du sous-système de sécurité afin de permettre sa restauration éventuelle. En pratique, cela signifiera généralement son remplacement (cela correspond au concept de « temps de mission » de la norme (EN) ISO 13849-1).

Le schéma suivant est la représentation fonctionnelle d'un système à tolérance zéro défaut avec fonction de diagnostic. La couverture de diagnostic est utilisée pour réduire la probabilité de pannes matérielles dangereuses. Les tests de diagnostic sont réalisé automatiquement. La définition du taux de couverture des tests de diagnostic est la même que dans la norme (EN) ISO 13849-1. Il s'agit du rapport entre le taux de défaillances dangereuses détectées et le taux de défaillances dangereuses global.

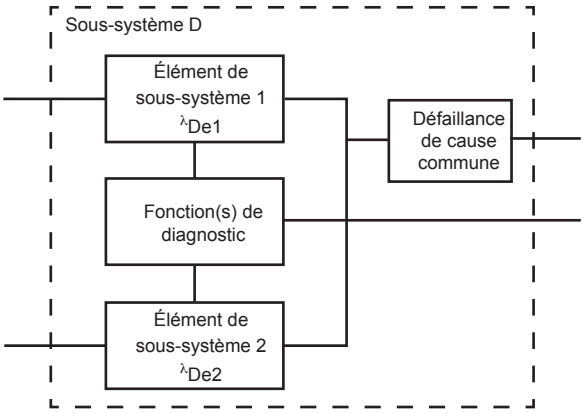


Architecture de sous-système logique de type C

$\lambda_{DssC} = \lambda_{De1} (1\text{-}DC_1) + \ldots + \lambda_{Den} (1\text{-}DC_n)$
PFHDssC = λDssC

Ces formules incluent le taux de couverture des tests de diagnostic (DC) pour chacun des éléments du sous-système. Les taux de défaillances de chaque sous-système sont diminués de la valeur du taux de couverture des tests de diagnostic correspondante.

Ci-dessous est présenté le quatrième exemple d'architecture de sous-système. Ce sous-système a une tolérance de défaut unique et inclut une fonction de diagnostic. Le risque potentiel de défaillance de cause commune doit également être pris en considération avec les système à tolérance de défaut unique.



Architecture de sous-système logique de type D

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

λDssD = (1 – β)2 {[λDe1 x λDe2 x (DC1+ DC2)] x T2/2 + [λDe1 x λDe2 x (2- DC1 – DC2)] x T1/2 } + β x (λDe1 + λDe2)/2
PFHDssD = λDssD

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

$A_{DssD} = (1 - \beta)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1\text{-}DC)] \times T_1 \} + \beta \times \lambda_{De}$
PFHDssD = λDssD

On remarquera que les deux formules utilisent un paramètre supplémentaire, l'intervalle de diagnostic T2. Il s'agit simplement d'un contrôle périodique de la fonction. Il est moins complet que le test de validité.

À titre d'exemple, nous prendrons les valeurs suivantes et nous considérerons que les éléments du sous-système sont identiques :

β = 0,05
λDe = 1 x 10^{-6} défaillances/heure
T1 = 87 600 heures (10 ans)
T2 = 2 heures
DC = 90 %

PFHDssD = 5,790E-8 défaillances dangereuses par heure. On se trouve donc dans la plage correspondant au niveau SIL 3

Effet de l'intervalle entre les tests de validité

La norme CEI/EN 62061 indique qu'un intervalle entre tests de validité PTI (Proof Test Interval) de 20 ans est souhaitable (mais non obligatoire). Voyons l'effet de cet intervalle entre les tests de validité sur le système. Si nous recalculons la formule avec T1 = 20 ans, nous obtenons une valeur PFHDssD = 6.58E-8. Ce résultat se trouve toujours dans la plage requise pour le niveau SIL 3. Pour son calcul du taux de défaillance dangereuse global, le concepteur gardera à l'esprit que ce sous-système particulier doit être combiné à d'autres sous-systèmes.

Effet de l'analyse de défaillance de cause commune

Examinons maintenant l'effet des défaillances de cause commune sur le système. Supposons que nous prenions des mesures supplémentaires et que notre valeur β (bêta) passe à 1 % (0,01), alors que l'intervalle entre tests de validité reste à 20 ans. Le taux de défaillance dangereuse passera alors à 2,71E-8. Autrement dit, le sous-système sera mieux adapté à une utilisation dans un système SIL 3.

Défaillance de cause commune (CCF)

Une défaillance de cause commune est causée par un ensemble de défauts à caractère dangereux ayant une cause identique. Les informations relatives aux défaillance de cause commune sont généralement nécessaires uniquement au concepteur du sous-système, habituellement son fabricant. Elles sont utilisées dans la formule précédemment fournie pour l'estimation de la valeur PFH_D d'un sous-système. Elles ne sont généralement pas nécessaire au niveau de la conception du système.

L'Annexe F de la norme CEI/EN 62061 propose une approche simple pour estimer la valeur CCF. Le tableau suivant présente un résumé de la méthode d'évaluation utilisée.

N°	Mesure contre les défaillances de cause commune	Note
1	Séparation/isolement	25
2	Diversification	38
3	Conception/application/ expérience	2
4	Évaluation/analyse	18
5	Compétence/formation	4
6	Environnement	18

Grille d'évaluation des mesures contre les défaillances de cause commune

Des points sont attribués pour chaque mesure spécifique mise en œuvre contre les pannes d'origine commune. Ces points sont totalisés pour déterminer le coefficient de défaillance de cause commune, tel que présenté dans le tableau suivant. Ce coefficient bêta est utilisé pour la modélisation des sous-système afin d'« ajuster » le taux de défaillance.

Note globale	Facteur de défaillance de cause commune (R)
< 35	10 % (0,1)
35 – 65	5 % (0,05)
65 – 85	2 % (0,02)
85 – 100	1 % (0,01)

Coefficient bêta de défaillance de cause commune

Taux de couverture des tests de diagnostic (DC)

Des tests de diagnostic automatiques sont utilisés pour réduire la probabilité de défaillances matérielles dangereuses. L'idéal serait de pouvoir détecter toutes les défaillances matérielles dangereuses. Mais en pratique, la valeur maximale est fixée à 99 % (c'est-à-dire 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 totale.

$$DC = \frac{\text{Probabilité de défaillances dangereuses détectées, } \lambda_{DD}}{\text{Probabilité de défaillances dangereuses totale, } \lambda_{Dtotal}}$$

La valeur DC sera toujours comprise entre zéro et 99 %.

Tolérance aux pannes matérielles

La tolérance aux défauts matériels représente le nombre de défauts qu'un sous-système peut supporter avant de provoquer une défaillance dangereuse. Par exemple, une tolérance aux défauts matériels de 1 signifie que 2 défauts pourront entraîner la perte de la fonction de commande de sécurité (mais pas un défaut seul).

Gestion de la sécurité fonctionnelle

La norme fixe des règles de contrôle des activités techniques et de gestion afférentes à l'exploitation d'un système de commande de sécurité électrique.

Intervalle entre tests de validité

L'intervalle entre tests de validité représente la durée au bout de laquelle il sera nécessaire de recontrôler entièrement le sous-système ou de le remplacer afin de garantir qu'il soit toujours à l'état « comme neuf ». En pratique, dans le secteur des machines, ceci est obtenu par remplacement. L'intervalle entre tests de validité est donc généralement assimilé à la durée de vie. La norme (EN) ISO 13849-1 parle, elle, de Temps de mission.

Un test de validité vise à détecter les défauts et les détériorations d'un système de commande de sécurité. Il doit permettre la restauration de ce système dans un état aussi proche que possible de son état neuf. Le test de validité doit détecter l'ensemble de tous les défauts dangereux, y compris la fonction de diagnostic (s'il y en a une). Les voies séparées doivent être testées séparément.

A l'inverse des tests de diagnostic qui sont automatiques, les tests de validité sont généralement réalisés manuellement et hors ligne. Du fait de leur caractère automatique, les tests de diagnostic sont effectués fréquemment, alors que les tests de validité sont réalisés ponctuellement. Par exemple, le câblage d'un dispositif d'interverrouillage monté sur une grille de protection pourra être contrôlé automatiquement pour y détecter d'éventuels courts-circuits et coupures de circuits au moyen d'un test de diagnostic (par exemple, par impulsions).

L'intervalle entre tests de validité doit être spécifié par le fabricant. Parfois, le fabricant fournit différents intervalles entre tests de validité. Il est plus fréquent de seulement remplacer le sous-système par un neuf qui réalise effectivement un test de validité.

Proportion de défaillances non dangereuses (SFF)

La proportion de défaillances non dangereuses est similaire au taux de couverture des tests de diagnostic, mais elle prend de plus en compte la propension inhérente

au système à se mettre en sécurité en cas d'apparition de défaut. Par exemple, lorsqu'un fusible grille, il y a apparition d'un défaut. Mais il est très probable que ce défaut ne se traduira que par une coupure du circuit. Dans la plupart des cas, il s'agira donc d'une « défaillance non dangereuse ». La valeur SFF exprime le rapport : (somme des défaillances « non dangereuses » plus nombre de défaillances dangereuses détectées) sur (somme des défaillances « non dangereuses » plus nombre de défaillances dangereuses détectées et non détectées). Il est important de retenir que les seuls types de défaillances à prendre en considération sont ceux qui ont un effet sur la fonction de sécurité.

La valeur SFF est normalement indiquée par le fabricant si elle est pertinente.

La proportion de défaillances non dangereuses (SFF) peut être calculée à l'aide de l'équation suivante :

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

dans laquelle :

$\sum_S$ = taux de défaillance de sécurité,
$\sum \lambda_S + \sum \lambda_D$ = taux de toutes les défaillances,
λ_{DD} = taux de défaillances dangereuses détectées,
λ_D = taux de toutes les défaillances dangereuses.

Défaillance systématique

La norme définit des règles pour maintenir sous contrôle et éviter les défaillances systématiques. Les défaillances systématiques diffèrent des défaillances matérielles aléatoires. Celles-ci sont des pannes pouvant survenir à n'importe quel moment et résultant généralement d'une forme de dégradation des composants matériels. Les types de défaillance systématique les plus courants sont les erreurs de conception du logiciel, les erreurs de conception du matériel, les erreurs de spécification de paramètres et de procédure de fonctionnement. Voici quelques exemples de mesures à prendre pour éviter ces défaillances systématiques :

- sélection, combinaison, disposition, assemblage et installation appropriés des composants ;
- utilisation de bonnes pratiques d'ingénierie ;
- respect des caractéristiques et des instructions de montage du fabricant ;
- respect de la compatibilité entre les composants ;
- prise en compte des conditions d'environnement :
- utilisation de matériaux adaptés.

Chapitre 9 : Systèmes de commande de sécurité, considérations supplémentaires

Présentation

Ce chapitre aborde les aspects et les principes généraux de type structurels à prendre en considération lors de la conception d'un système de commande de sécurité.

Catégories de systèmes de commande

Les « Catégories » de systèmes de commande ont été introduites par l'ancienne norme EN 954-1:1996 (ISO 13849-1:1999). Toutefois, elles sont encore utilisées pour décrire la structure des systèmes de commande de sécurité et elles demeurent une partie intégrante de la norme (EN) ISO13849-1 en tant qu'architectures désignées. La description et les exigences de ces Catégories sont abordées précédemment dans cette publication dans la section « Présentation de la norme (EN) ISO 13849-1 ». Cette section vise à fournir un guide simplifié mais pratique sur la mise en œuvre des structures de Catégories.

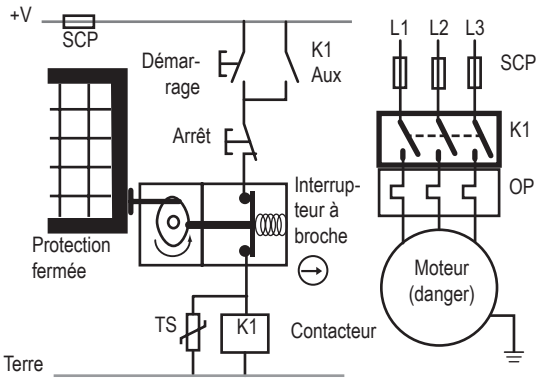
Catégorie B

La Catégorie B doit constituer le socle sur lequel toutes les autres Catégories s'appuient. Elle n'inclut pas de dispositions ou de structure spécifiques pour la sécurité au-delà des principes de sécurité de base stipulés dans les annexes A à D de la norme (EN) ISO 13849-2. Ils représentent les bonnes pratiques générales en matière de conception et de sélection des matériaux.

Catégorie 1

La Catégorie 1 requiert l'utilisation de composants et de principes de sécurité éprouvés.

Le scénario présenté ici est un système type visant à respecter les exigences de la Catégorie 1. Le dispositif de verrouillage et le contacteur jouent des rôles clés pour dissiper l'énergie du moteur lorsqu'un accès à la zone dangereuse est nécessaire. Le dispositif d'interverrouillage à broche est conforme à la norme CEI 60947-5-1 relative aux contacts à ouverture directe. Ceci est symbolisé sur le schéma par la flèche dans un cercle. Avec les composants éprouvés, la probabilité d'une dissipation de l'énergie est supérieure pour la Catégorie 1 que pour la Catégorie B. L'utilisation de composants éprouvés vise à réduire au minimum la possibilité d'une perte de la fonction de sécurité, mais il convient de noter qu'un défaut unique peut aboutir à la perte de cette fonction.

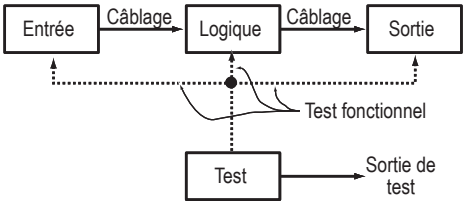


Système de sécurité simple de Catégorie 1

La Catégorie 1 vise à prévenir la défaillance au moyen d'une conception simple qui utilise des composants à haute fiabilité. Lorsque ce type de prévention ne permet pas une réduction suffisante des risques, une détection des défauts doit être mise en place. Les Catégories 2, 3 et 4 permettent cette détection des défaillances et des défauts, avec des niveaux d'exigence croissants dans la réduction des risques.

Catégorie 2

En plus de respecter les critères de la Catégorie B et d'utiliser des principes de sécurité éprouvés, un système de sécurité de Catégorie 2 doit utiliser un dispositif de test. Ces tests doivent permettre de détecter tous défauts sur la partie sécurité du système de commande. Lorsqu'aucun défaut n'est détecté, le système peut fonctionner normalement. Si des défauts sont détectés, une fonction de réaction à ceux-ci doit garantir que la machine demeure dans un état de sécurité.



Le dispositif de test peut faire partie intégrante du système de sécurité ou être un équipement séparé.

Les tests doivent être effectués :

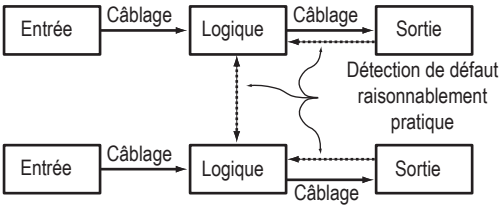
- à la mise sous tension initiale de la machine ;
- avant le démarrage de la source de danger ;
- périodiquement si cela est jugé nécessaire par l'évaluation des risques.

Remarque : la norme (EN) ISO 138491-1 suppose un test au rapport 100:1 exigé pour la fonction de sécurité ou un test à la demande de la fonction de sécurité avec la capacité de détecter un défaut et arrêter la machine en un temps plus court que ce qu'il faut pour atteindre le danger.

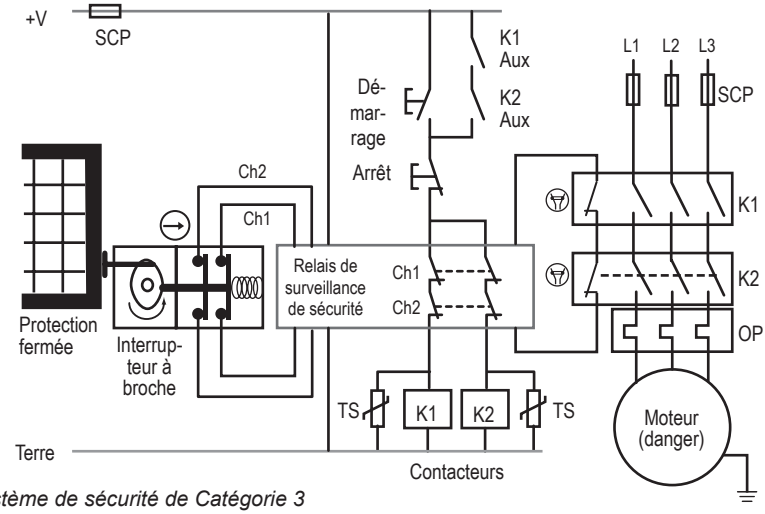
En substance, un sous-système ou système de sécurité doit être déclenché afin de tester l'état parfaitement opérationnel de la fonction de sécurité. Autrement dit, elle peut être difficile ou impossible à mettre en œuvre avec des technologies ayant des caractéristiques mécaniques. Une approche de Catégorie 2 est généralement plus pertinente pour les technologies électroniques. Pour le niveau PLd, une sortie de test doit être capable de déclencher un état de sécurité dès lors qu'un défaut est détecté.

Catégorie 3

En plus de respecter les critères de la Catégorie B et d'utiliser des procédés de sécurité éprouvés, un système de sécurité de Catégorie 3 nécessite que la fonction de sécurité puisse être exécutée même en présence d'un défaut unique. Ce défaut doit être détecté au moment ou avant la sollicitation suivante de la fonction de sécurité, lorsque cela est raisonnablement simple à réaliser.
Certains défauts, tels que les erreurs de croisement, qui ne provoquent pas une perte immédiate de la fonction de sécurité, peuvent ne pas être détectés. Autrement dit, pour la Catégorie 3, une accumulation de défauts non détectés peut aboutir à la perte de la fonction de sécurité.



Le schéma ci-joint permet de comprendre le principe d'un système de Catégorie 3. Un système redondant combiné à un dispositif de surveillance croisée et à la surveillance des sorties sera utilisé pour garantir le bon fonctionnement de la fonction de sécurité.



Système de sécurité de Catégorie 3

Le schéma présente un système de Catégorie 3. L'interrupteur de sécurité à broche comporte des jeux de contacts redondants. Le relais MSR possède lui-même en interne des circuits redondants qui se surveillent réciproquement. Un jeu de contacteurs redondants coupe l'alimentation du moteur. Les contacteurs sont surveillés par le relais MSR via les contacts à couplage mécanique.

La détection des défauts doit être prise en considération pour chaque partie du système de sécurité. Quels sont les modes de défaillance d'un interrupteur à broche double voie ? Quels sont les modes de défaillance du relais MSR ? Quels sont les modes de défaillance des contacteurs K1 et K2 ? Quels sont les modes de défaillance du câblage ?

Pour les circuits de Catégorie 3, il est fréquent d'utiliser des interrupteurs de sécurité à broche uniques avec des jeux de contacts électriques redondants. Autrement dit, la possibilité d'un défaut d'un composant unique au sein de la chaîne de commande doit être exclue. Si ce défaut ne peut pas être exclu, un défaut unique peut provoquer la perte de la fonction de sécurité. Il est très important que toute exclusion de défaut soit pleinement justifiée.

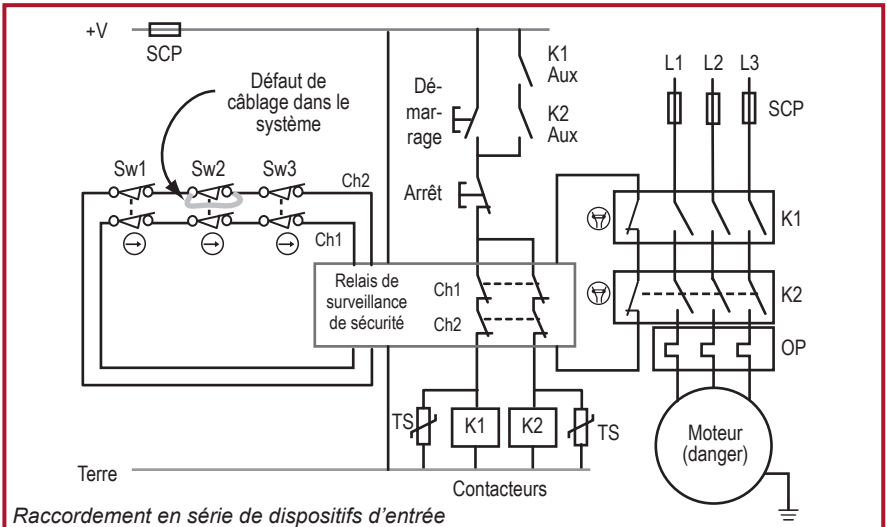
Le relais de surveillance de sécurité (MSR) fournit une fonction de diagnostic de défaut pour l'interrupteur de sécurité à broche et les contacteurs. Le relais MSR peut aussi faciliter d'autres fonctionnalités, telles qu'une réinitialisation manuelle. Concernant leur architecture interne, les relais de surveillance de sécurité ont généralement le niveau PLe ou SIL 3.

Les deux contacteurs doivent disposer d'une protection contre les surcharges et les courts-circuits. La probabilité d'une défaillance de contacteur avec des contacts soudés est faible, mais pas impossible. La défaillance d'un contacteur pourra aussi être due au maintien de ses contacts de commutation d'alimentation en position fermée en raison d'une armature bloquée. Si l'un des contacteurs génère une défaillance dangereuse, le second pourra continuer de fonctionner et coupera l'alimentation du moteur. Ce relais MSR détectera le contacteur défaillant lors du

démarrage du cycle suivant de la machine. Lorsque la grille sera refermée et que le bouton de démarrage sera enfoncé, les contacts à couplage mécanique du contacteur défaillant resteront ouverts et le relais MSR ne pourra pas fermer ses contacts de sécurité, ce qui révélera le défaut.

Pannes non détectées

Avec une structure de système de Catégorie 3, il peut toujours exister des défauts ne pouvant pas être détectés. Néanmoins, ils ne devront pas, en tant que tels, entraîner la perte de la fonction de sécurité. Lorsque des défauts sont détectés, nous devons d'autre part savoir si, dans certaines circonstances, ils pourraient être masqués ou acquittés de façon involontaire par l'action d'autres dispositifs au sein du système.



Raccordement en série de dispositifs d'entrée

Le schéma ci-dessus présente une pratique courante de raccordement de dispositifs multiples à un relais de surveillance de sécurité. Chaque dispositif contient deux contacts à ouverture (normalement fermés). Cette approche permet de réduire le coût du câblage puisque ces capteurs sont montés en série. Mais, supposons qu'un court-circuit se produise sur l'un des contacts (Sw2 sur le schéma). Ce défaut peut-il être détecté ?

Si l'interrupteur Sw1 (ou Sw3) est ouvert, les circuits des deux voies Ch1 et Ch2 seront ouverts et le relais MSR coupera l'alimentation de la source de danger. Si alors Sw3 est ouvert puis refermé, le défaut sur ses contacts ne sera pas détecté car il n'y aura pas de changement d'état du relais MSR. Les deux voies Ch1 et Ch2 resteront donc ouvertes. Si alors Sw1 (ou Sw3) est fermé, la source de danger pourra être réactivée par une simple pression sur le bouton de démarrage. Dans ces circonstances, le défaut n'aura pas entraîné la perte de la fonction de sécurité mais il n'aura pas été détecté. Il restera présent dans le système et l'apparition d'un défaut ultérieur (un court-circuit sur le deuxième contact de Sw2) pourrait entraîner cette fois la perte de la fonction de sécurité.

Si Sw2 a été uniquement ouvert et fermé, sans activation des autres interrupteurs, la voie Ch1 s'ouvre et la voie Ch2 reste fermée. Le relais MSR met la source de danger hors tension du fait de l'ouverture de Ch1. Lorsque Sw2 se ferme. le moteur ne pourra pas être redémarré en appuyant sur le bouton de démarrage. Ceci s'explique par le fait que Ch2 ne s'est pas ouverte. Le défaut est ainsi détecté. Cependant, si pour une quelconque raison, Sw1 (ou Sw3) vient alors à s'ouvrir et se refermer, les circuits des deux voies Ch1 et Ch2 seront ouverts puis refermés. Cette séquence simulera un acquittement du défaut et entraînera un réarmement involontaire du relais MSR.

Cela pose la question de quel taux de couverture des tests de diagnostic (DC) peut être atteint pour les interrupteurs individuels dans cette structure lors de l'utilisation de la norme (EN) ISO 13849-1 ou CEI 62061. Jusqu'à la publication de la norme ISO TR 24119 (novembre 2015 : Sécurité des machines – Évaluation des défauts masqués dans les connexions en séries des protecteurs avec dispositif de verrouillage ayant des contacts libres), il n'y avait pas de guide définitif spécifique à ce sujet, mais il était fréquent de supposer un taux DC de 60 %, à la condition que les interrupteurs soient testés individuellement à des périodes appropriées pour détecter les défauts. S'il était prévisible qu'un ou plusieurs interrupteurs ne seraient jamais testés individuellement, alors leur taux DC devrait être fixé comme étant zéro. La norme ISO TR 24119 fournit des recommandations détaillées pour la détermination du taux DC des dispositifs de protection à verrouillage au moyen de contacts sans potentiel raccordés en série. Le tableau suivant fournit une vue d'ensemble de base. Il est essentiel d'étudier complètement le document afin de déterminer le taux DC effectif maximum admissible pour toute architecture et application particulière.

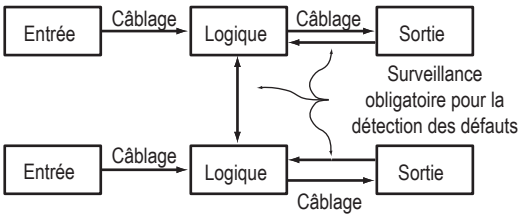
Nombre de protections mobiles employées fréquemment[1]	Nombre de protections mobiles supplémentaires	Probabilité de masquage	Taux de couverture des tests de diagnostic	Niveau PL maximum atteignable
0	2 à 4	Faible	Moyen	PL d
	5 à 30	Moyen	Faible	PL d
	> 30	Élevé	Aucun	PL c
1	1	Faible	Moyen	PL d
	2 à 4	Moyen	Faible	PL d
	≥ 5	Élevé	Aucun	PL c
> 1	--	Élevé	Aucun	PL c

[1] Fréquence de commutation supérieure à une fois par heure

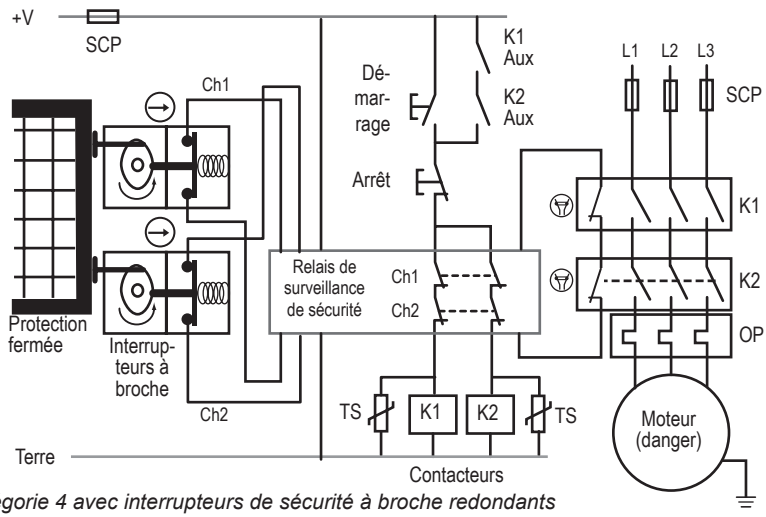
Le branchement en série des contacts électromécaniques est limité au niveau maximum PLd et, dans certains cas, au niveau maximum PLc. À noter que, dans tous les cas, si la survenance d'un masquage de défaut est prévisible (par ex., ouverture simultanée de multiples dispositifs de protection mobiles dans le cadre du fonctionnement ou du service normal), le taux DC est limité à aucun.
Il est intéressant de noter que ces caractéristiques spécifiques aux structures de Catégorie 3 ont toujours nécessité une attention particulière. Mais, avec les normes de sécurité fonctionnelle, elles deviennent véritablement sensibles.

Catégorie 4

Comme la Catégorie 3, la Catégorie 4 exige que le système soit conforme aux réquisitions de la Catégorie B, qu'il respecte les principes de sécurité éprouvés et soit capable d'exécuter la fonction de sécurité en présence d'un défaut unique. A l'inverse de la Catégorie 3 dans laquelle une telle accumulation de défauts peut entraîner la perte de la fonction de sécurité, la Catégorie 4 impose que la fonction de sécurité puisse être exécutée même en présence de plusieurs défauts. Dans la pratique, cela passe généralement par un haut niveau de diagnostic afin de garantir la détection de tous les défauts pertinents avant une possible accumulation. En prenant en compte l'accumulation théorique des défauts, 2 défauts peuvent suffire, même si la prise en considération de 3 défauts peut être nécessaire pour certaines conceptions.

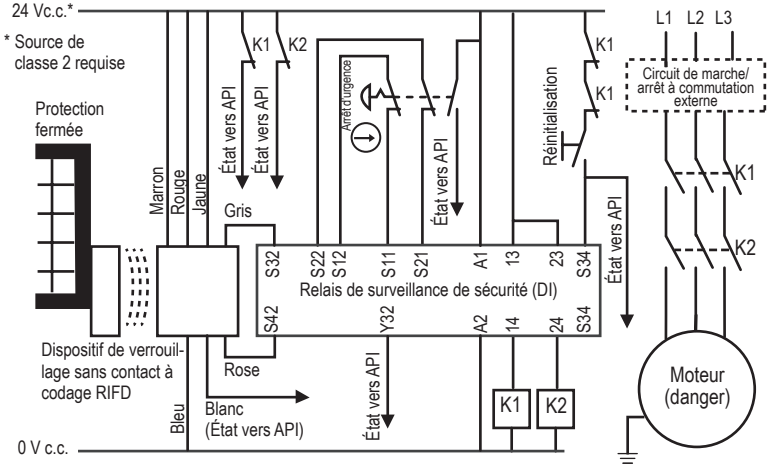


Le schéma de principe de la Catégorie 4 est présenté ici. La surveillance des deux dispositifs de sortie et la surveillance croisée sont nécessaires. La Catégorie 4 a un taux de couverture des tests de diagnostic supérieur à la Catégorie 3.



Catégorie 4 avec interrupteurs de sécurité à broche redondants

Jusqu'à relativement récemment, les interrupteurs de sécurité à broche uniques avec deux voies électriques ont été utilisés pour les circuits de la Catégorie 4. Pour employer un seul interrupteur à broche dans un circuit à deux voies, il est nécessaire d'exclure les possibles points de défaillance uniques sur la broche mécanique d'activation et le couplage de l'interrupteur. Cependant, le rapport technique conjoint ISO TR 23849 a clarifié le fait que ce type d'exclusion de défaut ne doit pas être employé sur les systèmes PLe ou SIL 3. Si le concepteur du système de sécurité préfère les dispositifs de verrouillage à broche, deux interrupteurs distincts peuvent être employés pour être conforme à la Catégorie 4.



Catégorie 4 avec dispositif de verrouillage sans contact électronique à déclenchement RFID

La technologie contemporaine adopte une approche différente pour la mise en place d'une architecture de Catégorie 4 (et le niveau PLe/SIL 3). L'utilisation de composants électroniques complexes a permis l'intégration rentable de la tolérance aux pannes et un haut niveau de taux de couverture des tests de diagnostic dans un seul dispositif. Le dispositif de verrouillage présenté est non seulement conforme à la Catégorie 4, mais il fournit aussi un niveau extrêmement élevé de résistance à la modification indésirable (neutralisation) au moyen du codage RFID. Il peut aussi être branché en série avec d'autres dispositifs similaires sans abaisser la catégorie ou le taux de couverture des tests de diagnostic.

Niveau de performance (PL) pour la classification des composants et des systèmes

Les architectures désignées (Catégories) de la norme (EN) ISO 13849 sont utilisables pour la classification de niveau de performances (PL) des composants de sécurité et des systèmes. Ceci crée une certaine confusion qu'il sera possible de clarifier à travers l'étude des composants et de leurs possibilités. L'étude des exemples précédents montre qu'un composant tel qu'un interrupteur de sécurité de Catégorie 1 est utilisable tel quel sur un système de Catégorie 1.
Il pourra également être incorporé dans un système de Catégorie 3 ou 4 s'il est monté en double et qu'une fonction de diagnostic est assurée par un relais de surveillance de sécurité.

Certains composants, comme les relais de surveillance et les automates de sécurité programmables, ont leur propre système de diagnostic interne et effectuent un autocontrôle afin de garantir leur bon fonctionnement. Ils peuvent donc être classés directement parmi les composants de sécurité compatibles avec les Catégories 2, 3 et 4 sans besoin de mesures supplémentaires.

Considérations relatives aux défauts et à leur exclusion

L'analyse de sécurité implique l'analyse approfondie des défauts potentiels. Une anticipation très précise du comportement du système de sécurité en cas d'apparition de ces défauts sera également nécessaire. Les normes ISO 13849-1 et ISO 13849-2 fournissent des détails sur les critères et les exclusions de défauts.

Si un défaut produit la défaillance en série d'autres composants, ce défaut d'origine et tous les autres défauts consécutifs seront considérés comme un défaut unique.

Si plusieurs défauts résultent d'une même cause, ces différents défauts seront considérés comme un seul et même défaut. C'est ce qu'on appelle une défaillance de cause commune.

L'apparition de plusieurs défauts indépendants simultanément est considérée comme très improbable. Elle ne sera pas prise en considération dans cette analyse.

Exclusions de défauts

Les normes (EN) ISO 13849-1 et CEI 62061 autorisent les exclusions de défauts lors de la détermination d'une classification de systèmes de sécurité s'il peut être démontré que la survenance d'un défaut est extrêmement improbable. Lorsque des exclusions de défauts sont ainsi réalisées, il est important qu'elles soient rigoureusement justifiées et qu'elles soient valables pour toute la durée de vie du système de sécurité. Plus le niveau de risque géré par le système de sécurité est élevé, plus la justification requise pour l'exclusion d'un défaut devra être stricte. Ceci a toujours provoqué une certaine confusion sur les types de défauts pouvant être exclus ou non. Comme nous l'avons déjà vu dans ce chapitre, les récentes versions des normes et leurs documents d'application ont apporté des clarifications sur certains aspects de ce problème.

En général, lorsqu'un niveau PLe ou SIL 3 est requis pour la mise en œuvre d'une fonction de sécurité par un système de sécurité, la norme ISO TR 23849 explique qu'il n'est pas normal de jouer uniquement sur les exclusions de défauts pour obtenir ce niveau de performance. Cela dépendra de la technologie utilisée et de l'environnement de travail prévu. Il est donc essentiel que le concepteur attache une importance accrue à la définition des exclusions de défauts lorsque les exigences de niveau PL ou SIL augmentent. Par exemple, une exclusion de défauts ne pourra pas être utilisée sur le côté mécanique des détecteurs de position électromécaniques et des interrupteurs manuels (par exemple, un dispositif d'arrêt d'urgence) afin d'obtenir une classification PLe ou SIL 3 du système. Les exclusions de défaut susceptibles d'être attachées à des conditions de défaut mécanique particulières (par exemple, l'usure, la corrosion, les ruptures) sont définies dans le tableau A.4 de la norme ISO 13849-2. Par exemple, un système d'interverrouillage de grille devant garantir un niveau PLe ou SIL 3 devra avoir un facteur de tolérance aux défauts minimum de 1 (par exemple, en utilisant deux détecteurs de position mécaniques conventionnels). Il n'est en effet normalement pas admissible d'exclure des défauts tels que des ruptures d'actionneurs de contacts à ce niveau de performance. Cependant, il peut être envisagé d'exclure des défauts, comme un court-circuit dans le câblage d'un panneau de commande conçu conformément aux normes applicables.

Catégories d'arrêt selon les normes CEI/EN 60204-1 et NFPA 79

Lorsqu'on parle de système de commande de sécurité, le terme « Catégorie » a des significations différentes, ce qui crée une confusion regrettable. Jusqu'à présent, nous avons principalement parlé des catégories de sécurité telles qu'elles ont été définies par la norme EN 954-1. Elles correspondent à une classification des performances d'un système de sécurité par rapport à certaines conditions de défaut.

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 : impose la coupure immédiate de l'alimentation sur les actionneurs. Ce type d'arrêt est parfois qualifié de non contrôlé. Dans certains cas en effet, le mouvement pourra prendre un temps notable avant de cesser, par exemple dans le cas d'un moteur tournant en roue libre avant de s'arrêter définitivement.

La Catégorie d'arrêt 1 : impose le maintien de l'alimentation jusqu'à l'arrêt complet du moteur afin de pouvoir le freiner électriquement, puis la coupure de cette alimentation ensuite. Remarque : voir la norme CEI 60204-1 pour des informations sur les Catégories d'arrêt 1a et 1b.

La Catégorie d'arrêt 2 : correspond à un arrêt contrôlé avec maintien de l'alimentation sur les actionneurs de la machine. Une procédure d'arrêt de production normale est considérée comme un arrêt de Catégorie 2..

Il est à noter que seules les catégories d'arrêt 0 ou 1 peuvent être utilisée en cas d'arrêt d'urgence. Le choix entre ces deux catégories doit être déterminé par l'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 aurait nécessité une sortie temporisée sur le relais de coupure d'alimentation terminal. Une grille à verrouillage de sécurité est souvent associée à un dispositif d'arrêt de Catégorie 1. Ceci permet de maintenir cette grille en position fermée tant que la machine n'est pas rendue à l'état de sécurité (c'est-à-dire, totalement arrêtée).

L'arrêt d'une machine sans se préoccuper du type d'automate programmable utilisé peut affecter le redémarrage et entraîner une détérioration grave des outils et de la machine. Un automate standard (non classé de sécurité) ne peut pas en effet être utilisé pour une fonction d'arrêt de sécurité. Par conséquent, d'autres solutions doivent être envisagées. Les deux solutions ci-après sont envisageables pour la Catégorie d'arrêt 1 :

1. Relais de sécurité à commande de neutralisation temporisée

Un relais de sécurité avec des sorties à action instantanée et temporisée est utilisé. Les sorties à action instantanée sont raccordées aux entrées du dispositif programmable (par exemple, automate ou « activation » variateur) et les sorties temporisées sont raccordées à un contacteur principal. Lorsque l'interrupteur de sécurité est actionné, les sorties instantanées du relais de sécurité changent d'état, indiquant au système programmable qu'il peut procéder à l'arrêt selon la séquence normale. Après l'écoulement d'un délai court

mais suffisant pour l'exécution de ce processus, la sortie temporisée du relais de sécurité change d'état et coupe le contacteur principal.

Remarque : le calcul du temps d'arrêt complet devra prendre en compte la temporisation des sorties du relais de sécurité. Ceci est particulièrement important pour la détermination du positionnement des dispositifs en fonction de la distance de sécurité.

2. Automates programmables de sécurité

La logique et les fonctions de temporisation peuvent être mises en œuvre facilement à l'aide d'un automate de sécurité tel que GuardLogix.

Exigences relatives aux systèmes de commande de sécurité aux États-Unis

Fiabilité de commande

Le plus haut niveau de réduction des risques selon les normes applicables aux robots, aux États-Unis comme au Canada, est obtenu par des systèmes de commande de sécurité respectant des critères de fiabilité de commande. Les systèmes de commande de sécurité garantissant la fiabilité de commande sont des architectures double voie avec surveillance. La fonction d'arrêt du robot ne doit pas être empêchée par la défaillance d'un seul composant, y compris de la fonction de surveillance elle-même.

Cette fonction de surveillance doit générer une commande d'arrêt lors de la détection d'un défaut. Une alarme doit être émise si une source de danger persiste après la cessation du mouvement. Le système de sécurité doit demeurer à l'état de sécurité tant que le défaut n'est pas corrigé. Il est préférable que le défaut soit détecté lors de son apparition. Si cela n'est pas possible à obtenir, ce défaut devra être détecté lors de la sollicitation suivante du système de sécurité. Les défaillances de cause commune doivent être prises en considération s'il existe une probabilité significative qu'elles se produisent.

Au Canada, il existe deux exigences supplémentaires par rapport aux États-Unis. Premièrement, les systèmes de commande de sécurité doivent être indépendants des systèmes de commande programmables standard. Deuxièmement, le système de sécurité ne doit pas pouvoir être facilement désactivé ou contourné sans que cela soit détecté.

Commentaires sur la fiabilité de commande

L'aspect le plus important de ce concept de fiabilité de commande est la tolérance à un seul défaut et la surveillance (détection de défaut). Les textes 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 ».

Il en découle trois considérations très importantes concernant les défauts : (1) les défauts ne sont pas tous détectés, (2) l'ajout du terme « composant » soulève des questions sur le câblage et (3) le câblage fait partie intégrante du système de sécurité. Les erreurs de câblage peuvent entraîner la perte de la fonction de sécurité.

L'objectif de la fiabilité de commande est clairement de permettre l'exécution de la fonction de sécurité même en présence d'un défaut. Si ce défaut est détecté, le système de sécurité doit exécuter une mesure de sécurité, avertir de la présence du défaut et empêcher le fonctionnement de la machine jusqu'à ce que le défaut soit rectifié. Si le défaut n'est pas détecté, la fonction de sécurité doit quand même pouvoir être exécutée en cas de sollicitation.

Chapitre 10 : Exemples d'application

Présentation – Fonctions de sécurité préconfigurées pour les machines

Les fonctions de sécurité des machines, qu'il s'agisse d'un arrêt d'urgence, d'une protection ou d'une détection de présence, requièrent différents éléments, notamment un détecteur ou un dispositif d'entrée, un organe logique et un dispositif de sortie. Ensemble, ces éléments fournissent un niveau de protection calculé en tant que niveau de performance comme stipulé dans la norme (EN) ISO 13849-1.

Dans ce chapitre, nous avons sélectionné une des nombreuses fonctions de sécurité préconfigurées pour les machines par Rockwell Automation. Ces documents sur les fonctions de sécurité fournissent chacun des recommandations concernant une fonction de sécurité spécifique, sur la base des exigences fonctionnelles, de la sélection des équipements et des exigences de niveau de performance. Ces recommandations incluent l'installation et le câblage, la configuration, le plan de vérification et de validation, ou encore le calcul du niveau de performance.

Les fonctions de sécurité préconfigurées sont gratuites et téléchargeables à partir du site Internet de Rockwell Automation.

www.rockwellautomation.com, sous Solutions & Services > Safety Solutions.

La fonction de sécurité préconfigurée suivante est basée sur l'interrupteur de sécurité de surveillance de porte avec un relais de sécurité configurable. Les produits suivants sont utilisés : L'interrupteur de sécurité sans contact et à codage RFID SensaGuard, qui est connecté à un relais de sécurité configurable Guardmaster 440C-CR30. Les dispositifs de sortie employés sont des contacteurs de sécurité 100S-C.
La classification de sécurité suivante est obtenue par cette fonction de sécurité préconfigurée : CAT. 4, PLe selon (EN) ISO 13849-1.

Le numéro de publication du document original est le suivant : SAFETY-AT133C-EN-P

Description de la sécurité fonctionnelle

Les personnels sont protégés des mouvements dangereux par une cloison fixe. L'accès éventuellement nécessaire à la zone dangereuse s'effectue à travers une porte pivotante. La porte est surveillée par un interrupteur de sécurité sans contact SensaGuard, lequel est connecté aux entrées du relais de sécurité configurable 440C-CR30. Le relais 440C-CR30 commande deux contacteurs de sécurité 100S-C branchés en série

et contrôlant l'alimentation électrique du moteur exécutant les mouvements dangereux. Chaque fois que cette porte surveillée est ouverte, le système de sécurité coupe l'alimentation du moteur. Le moteur et le mouvement dangereux qu'il commande sont arrêtés (Catégorie d'arrêt 0). Le redémarrage du moteur est impossible tant que la porte surveillée est ouverte. Lorsque la porte est fermée, le moteur peut être redémarré en appuyant sur et en relâchant le bouton de réinitialisation pour réinitialiser le relais 440C-CR30, puis en déclenchant le démarrage externe afin de rétablir l'alimentation du moteur commandée par les contacteurs 100S-C.

L'interrupteur SensaGuard surveille l'état (ouvert ou fermé) de la porte. L'interrupteur SensaGuard surveille aussi la présence de défauts sur ses deux sorties OSSD. Le relais 440C-CR30 surveille la présence de défauts sur les entrées de l'interrupteur SensaGuard et aussi l'état des signaux de réinitialisation et de retour des contacteurs 100S-C. Le relais surveille aussi la présence de défauts sur ses propres sorties. Ces sorties commandent les contacteurs 100S-C. Le relais 440C-CR30 désactive ses sorties et coupe l'alimentation électrique du moteur lorsqu'un défaut est détecté. Il n'est pas réinitialisé tant que ce défaut n'est pas corrigé.

Nomenclature

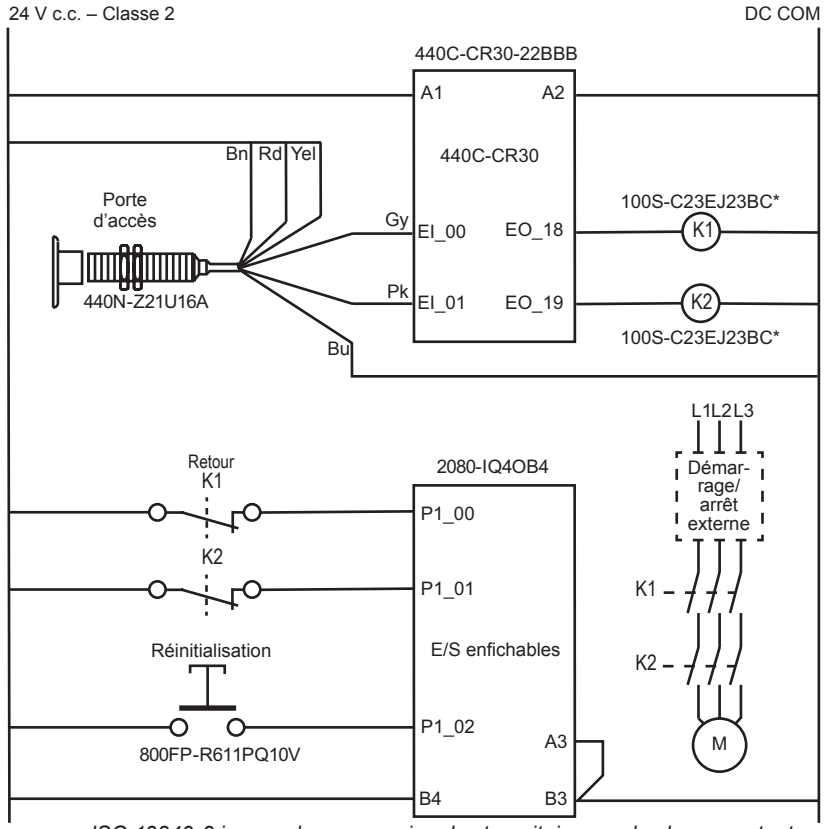
Cette application utilise les produits suivants.

Référence	Description	Quantité
440N-Z21S16B	Interrupteur SensaGuard, en plastique 18 mm, 2 x PNP, 0,2 A max., sortie de sécurité, câble 10 m	1
800FP-R611	800F à réarmement, plastique rond (type 4/4X/13, IP66), bleu, R, pack standard	1
2080-IQ4OB4	Module mixte d'entrées/sorties TOR 4 voies	1
1761-CBL-PM02	Câble ; relais de sécurité configurable 440C-CR30 vers ordinateur personnel, câble d'imprimante	1
440C-CR30-22BBB	Relais de sécurité à configuration logicielle Guardmaster 440C-CR30, PLe SIL 3, 22 E/S de sécurité, port série intégré, port de programmation USB, 2 ports enfichables, 24,0 V c.c.	1
100S-C23EJ23BC	Contacteur de sécurité MCS 100S-C, 23 A, 24 V c.c. (avec bobine électrique), contact jumelé	2

Aperçu du système

L'interrupteur de sécurité SensaGuard permet de confirmer que la porte protégée est dans une condition de sécurité fermée. Le mouvement dangereux est arrêté ou inhibé chaque fois que cette porte n'est pas fermée. Outre la surveillance de l'état de la porte protégée, l'interrupteur SensaGuard surveille la présence de conditions de défauts au niveau de ses sorties. Le relais de sécurité configurable 440C-CR30 détecte aussi les défauts de discontinuité, de voie unique ou de court-circuit à 0 V au niveau des entrées de l'interrupteur SensaGuard.

Le relais de sécurité configurable 440C-CR30 surveille les sorties testées par impulsions qui commandent les bobines de contacteur de sécurité pour toutes les conditions de défaut. L'état de sécurité approprié des contacteurs de sécurité K1 et K2 est confirmé par le relais de sécurité configurable 440C-CR30 chargé de surveiller les signaux de retour au niveau de SMF2 lors du démarrage.



**La norme ISO 13849-2 impose la suppression des transitoires sur la charge en tant que principe de sécurité de base.*
La bobine électronique « EJ » fournit une suppression appropriée.

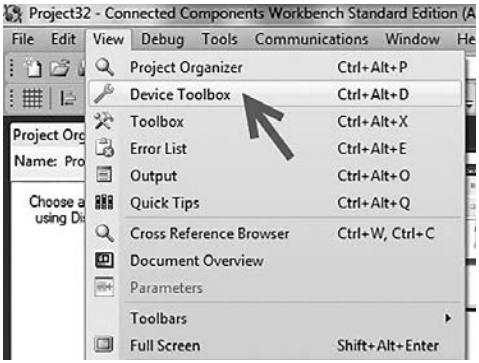
Configuration

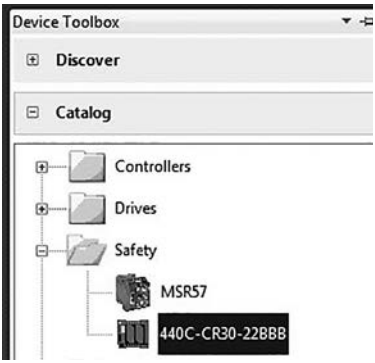
Le relais 440C-CR30 est configuré au moyen du logiciel Connected Components Workbench™, version 6.01 ou ultérieure. Ce document n'a pas pour objet de fournir la description détaillée de chacune de ces étapes. La connaissance du logiciel Connected Components Workbench est présumée.

Configuration du relais 440C-CR30

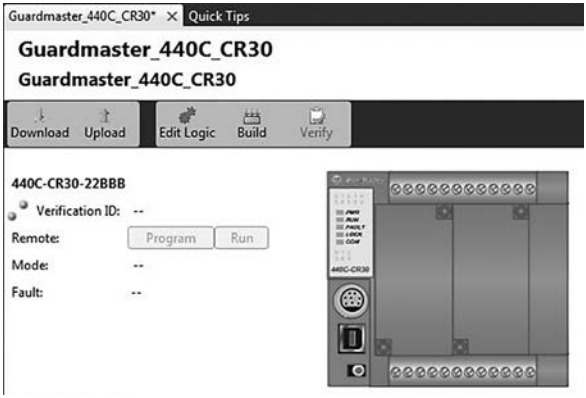
Suivez cette procédure pour configurer le relais Guardmaster 440C-CR30 dans Connected Components Workbench.

1. Dans le logiciel Connected Components Workbench, sélectionnez View, puis Device Toolbox. Dans la boîte de dialogue Device Toolbox, sélectionnez 440C-CR30-22BBB.

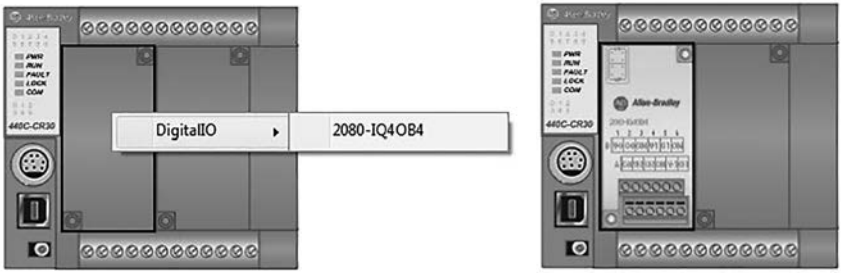




2. Dans le volet Project Organizer, cliquez deux fois sur Guardmaster_400C_CR30*.

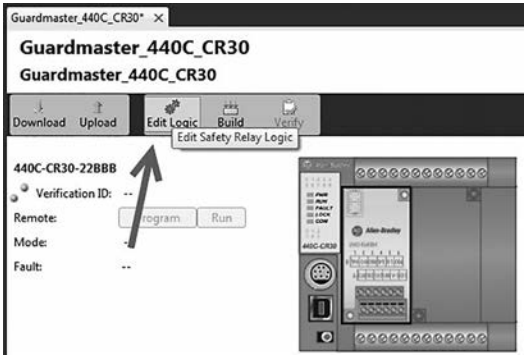


3. Pour ajouter le module d'E/S enfichable nécessaire dans ce circuit, cliquez avec le bouton droit de la souris sur l'espace de module enfichable gauche et sélectionnez le module 2080-IQ4OB4.

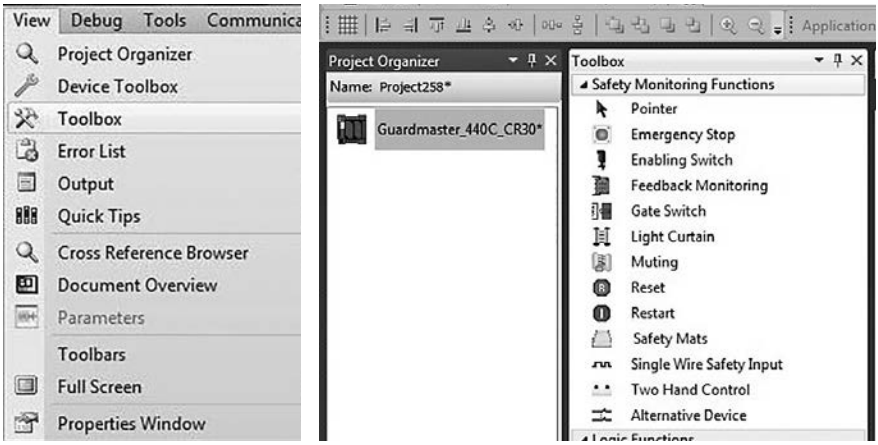


CONSEIL : le module d'E/S est indiqué en gris standard car il ne s'agit pas d'un module d'E/S de sécurité. Cette sélection est autorisée dans cette application, car elle ne sert pas à connecter des signaux de sécurité. Les entrées telles que les retours et le bouton de réinitialisation ne sont pas considérées comme des signaux de sécurité au sens strict. L'utilisation d'E/S standard pour ces signaux non liés à la sécurité peut réserver le nombre limité d'entrées et de sorties de sécurité pour les véritables signaux de sécurité.

4. Cliquez sur le bouton Edit Logic pour ouvrir l'espace de travail Connected Components Workbench. Un espace de travail vide apparaît.



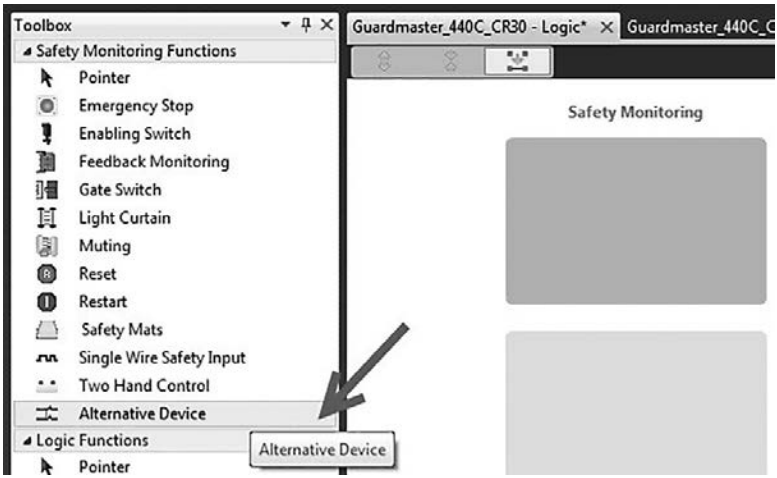
5. Dans le menu déroulant View, sélectionnez Toolbox. La boîte à outils apparaît.



Configuration des entrées

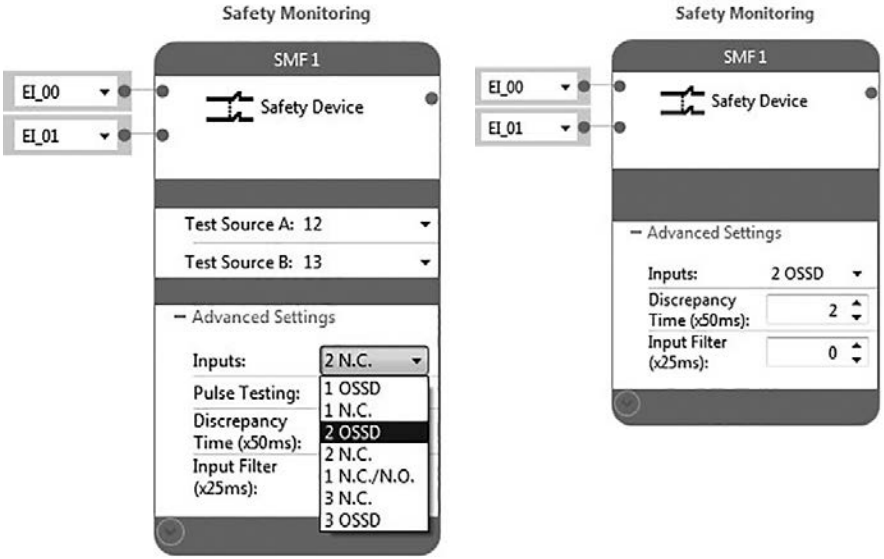
La boîte à outils (Toolbox) ne répertorie pas de fonction de surveillance de sécurité SensaGuard. Procédez comme suit pour en configurer une.

1. Sélectionnez Alternative Device. Faites glisser le dispositif sur le bloc vert dans la colonne Safety Monitoring et relâchez.

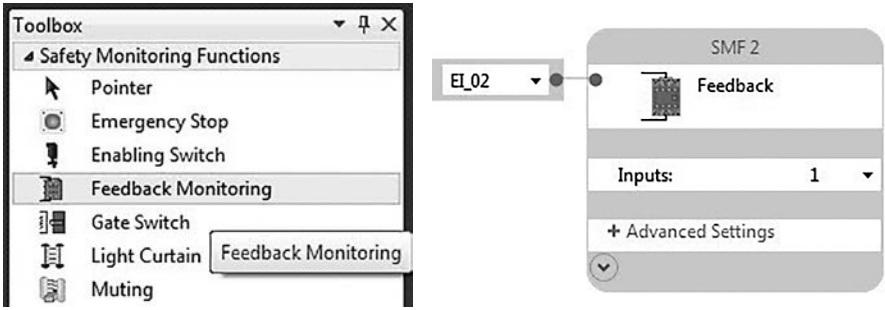


Le logiciel Connected Components Workbench affecte automatiquement les deux premières entrées disponibles, EI_00 and EI_01, au dispositif. Laissez-les attribuées. Le logiciel Connected Components Workbench affecte automatiquement le nom de fonction SMF 1 à ce bloc. Par défaut, le logiciel considère qu'il s'agit d'un dispositif électromécanique et affecte des sources de test (Test Sources). L'interrupteur SensaGuard comporte deux sorties OSSD et n'a pas besoin de sources de test.

2. Pour configurer correctement le bloc, ouvrez Advanced Settings et sélectionnez 2 OSSD dans le menu déroulant Inputs. Le bloc résultant apparaît comme illustré.

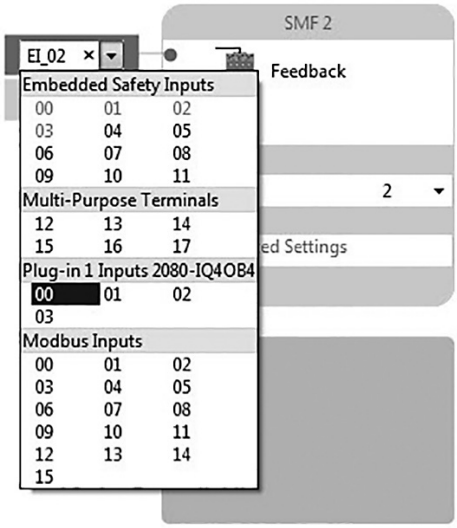


3. Cliquez sur, faites glisser et relâchez une fonction Feedback Monitoring sous Safety Monitoring Functions vers le bloc Safety Monitoring sous le bloc SensaGuard au niveau de l'espace de travail.

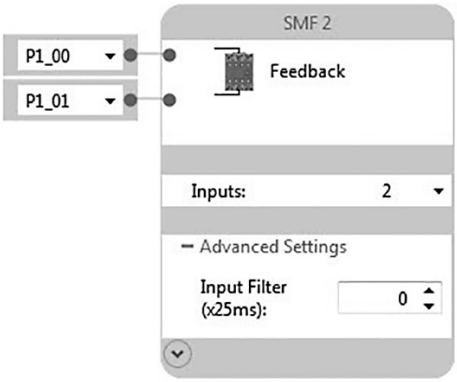


Veuillez noter que Connected Components Workbench l'affecte à EI_02, qui est la borne d'entrée de sécurité disponible suivante. Le logiciel suppose qu'il s'agit d'une entrée unique et affecte automatiquement le nom de fonction SMF 2 à ce bloc.

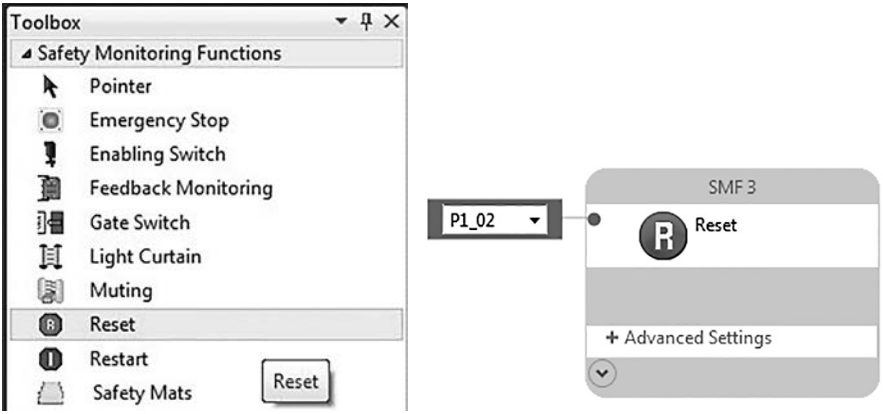
4. Comme le circuit requiert deux entrées, à savoir une pour chaque contacteur, changez le nombre d'entrée en 2, une pour le contact N.F. de chaque contacteur 100S.



5. Affectez les entrées aux bornes enfichables PI_00 et PI_01. Cela évite d'utiliser inutilement les entrées de sécurité pour les signaux de retour.



6. Cliquez sur, faites glisser et relâchez une fonction Reset sous Safety Monitoring Functions vers le bloc Safety Monitoring sous le bloc Feedback Monitoring au niveau de l'espace de travail.

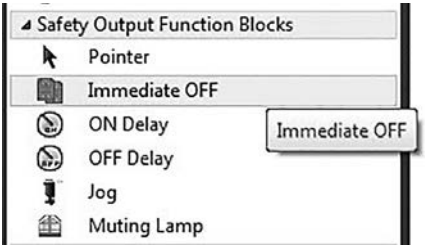


Le logiciel Connected Components Workbench affecte automatiquement le nom de fonction SMF 3 à ce bloc. Réaffectez l'entrée Reset à la borne enfichable PI_02.

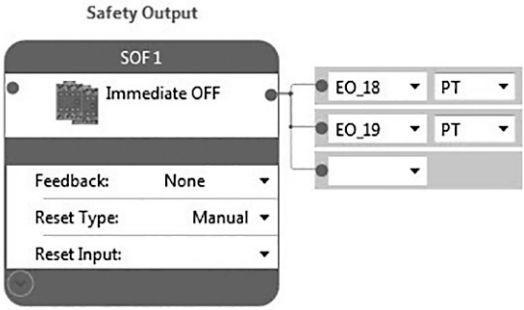
Configuration des sorties

Procédez comme suit pour configurer les sorties.

1. Cliquez sur et faites glisser Immediate OFF à partir de la section Safety Output Function Blocks de la boîte à outils.

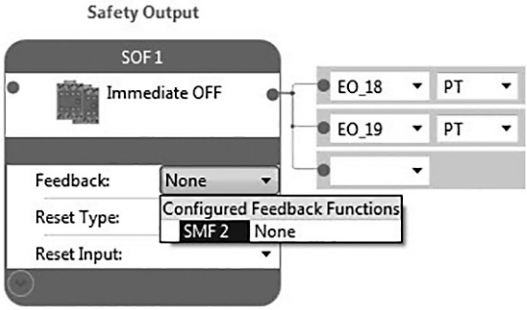


2. Relâchez sur le bloc supérieur de la colonne Safety Output dans l'espace de travail.

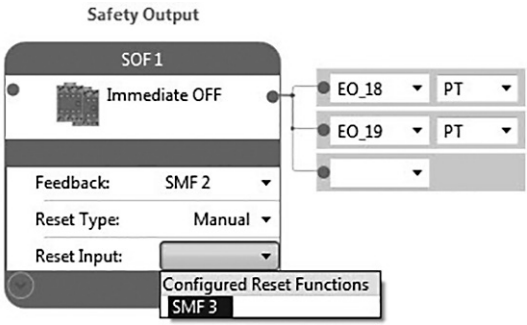


Connected Components Workbench affecte automatiquement les bornes de sortie EO_18 et EO_19. Pulse Testing est la valeur par défaut pour ces bornes. L'option Reset Type a par défaut la valeur Manual. Laissez ces paramètres à leurs valeurs par défaut.

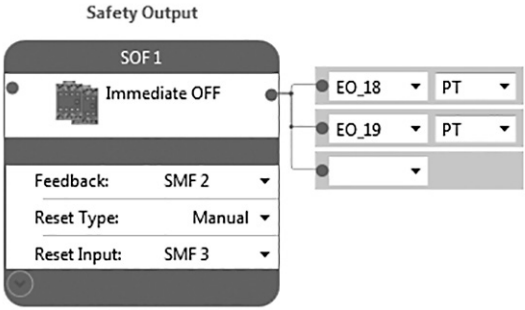
3. Sélectionnez SMF 2 dans le menu déroulant Feedback.



4. Sélectionnez SMF 3 dans le menu déroulant Reset Input.



La configuration des sorties de sécurité est terminée.

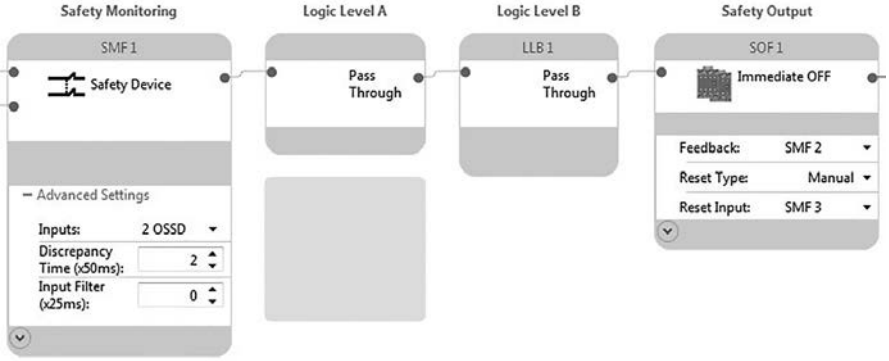


Configuration de la logique

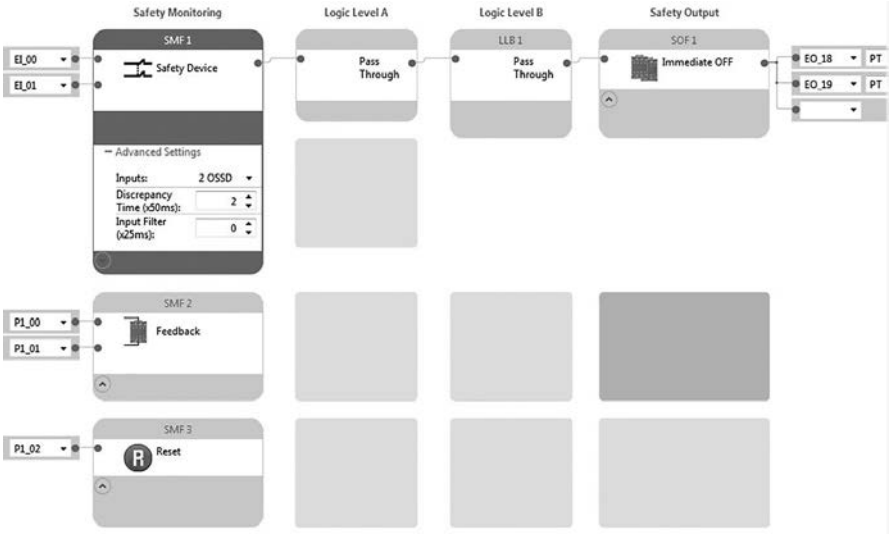
La section Logic détermine le mode de réponse des sorties logiques aux entrées de surveillance de sécurité. Dans ce cas, la sortie de sécurité suit directement l'entrée de surveillance de sécurité.

1. Cliquez sur le point bleu à droite du bloc d'entrée SensaGuard Safety Monitoring. Il devient gris.

2. Cliquez sur le point bleu à gauche du bloc Safety Output pour connecter la logique.

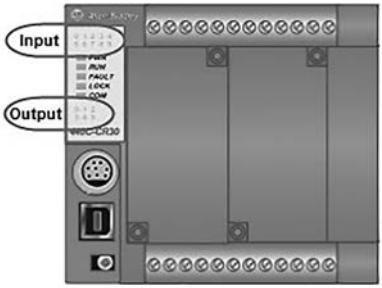


La logique terminée a l'aspect suivant.



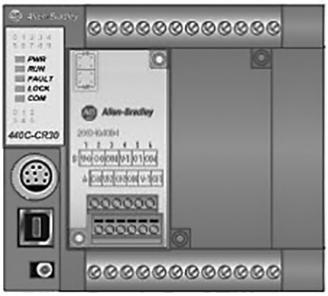
Configuration des indicateurs d'état

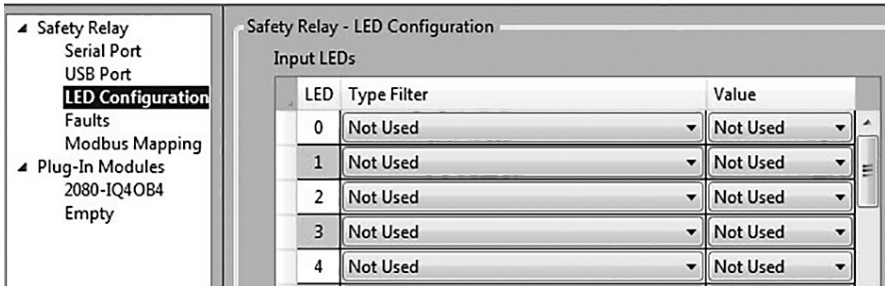
Le relais de sécurité configurable 440C-CR30 fournit dix voyants d'état d'entrée configurables par l'utilisateur et six voyants d'état de sortie configurables par l'utilisateur. Dans de nombreux cas, ils peuvent être très utiles pour l'installation, la mise en service, la surveillance et le dépannage du système de relais de sécurité configurable 440C-CR30. Ils n'affectent nullement le fonctionnement du système et il n'est pas nécessaire de les configurer, mais cette configuration est aisée et il est recommandé de les utiliser.



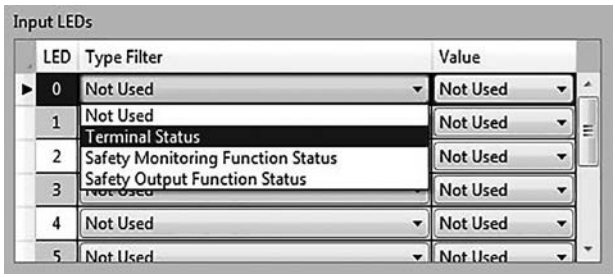
1. Cliquez sur Guardmaster_440C_CR30*.

2. Sélectionnez LED Configuration.

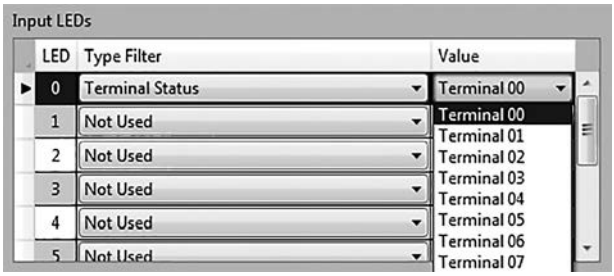




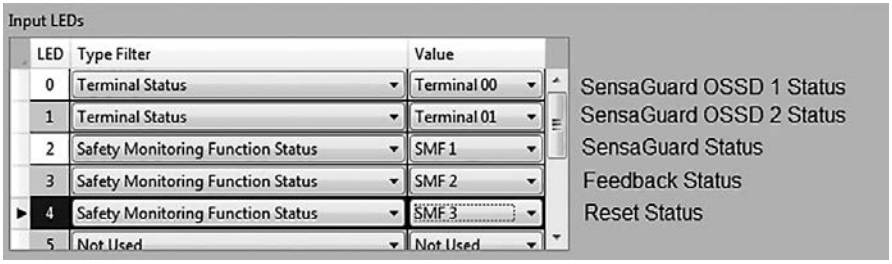
3. Pour Type Filter, sélectionnez Terminal Status pour LED 0.



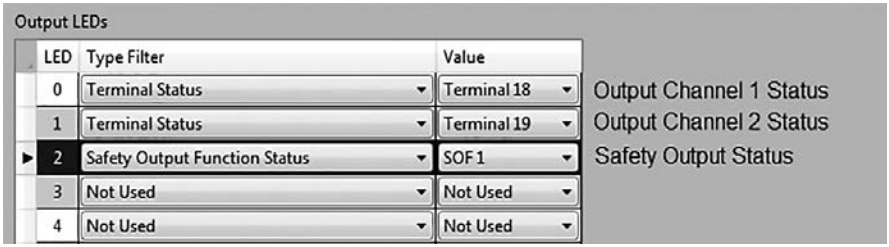
4. Pour LED 0, sélectionnez Terminal 00 dans le menu déroulant Value. Le voyant d'état 0 est maintenant configuré pour afficher l'état de la borne 00.



5. Affectez les quatre prochains voyants d'entrée (1 à 4) de la même manière. Les voyants d'état d'entrée sont maintenant configurés.



6. Affectez les trois voyants de sortie comme suit.

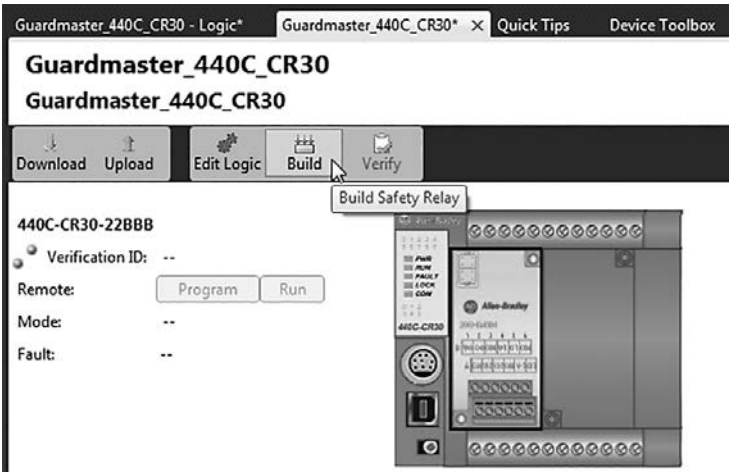


Confirmation de la validité de la configuration

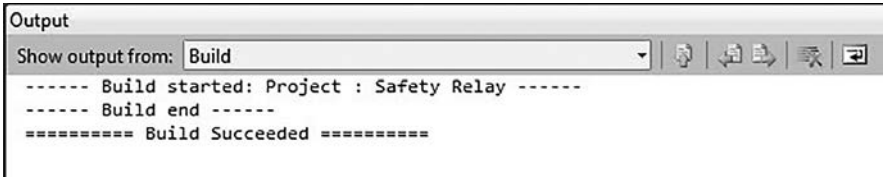
Procédez comme suit pour confirmer la validité de la logique en utilisant la fonction Build dans le logiciel Connected Components Workbench.

1. Cliquez sur Guardmaster_440C_CR30 dans la barre au-dessus de l'espace de travail.

2. Cliquez sur Build.



Un message Build Succeeded confirme que la configuration est valide.



Si une erreur ou une omission est découverte pendant la création d'une configuration, un message affiche les détails de l'erreur afin qu'elle soit corrigée. Une fois l'erreur corrigée, il faut recréer la configuration.

Enregistrement et téléchargement du projet

Procédez comme suit pour enregistrer et télécharger le projet.

1. Dans le menu File, sélectionnez Save pour enregistrer le projet.

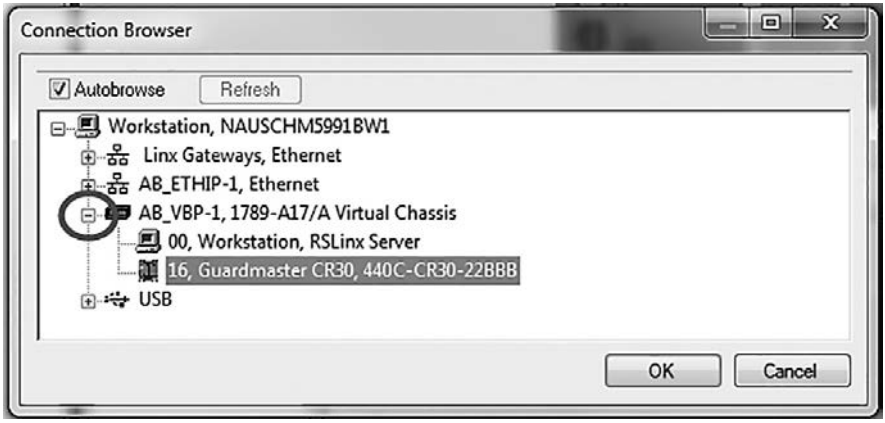
2. dans la fenêtre Project Organizer, cliquez deux fois sur Guardmaster_440C_CR30 pour ouvrir l'espace de travail.

3. Mettez sous tension le relais de sécurité 440C-CR30.

4. Branchez le câble USB sur le relais 440C-CR30.

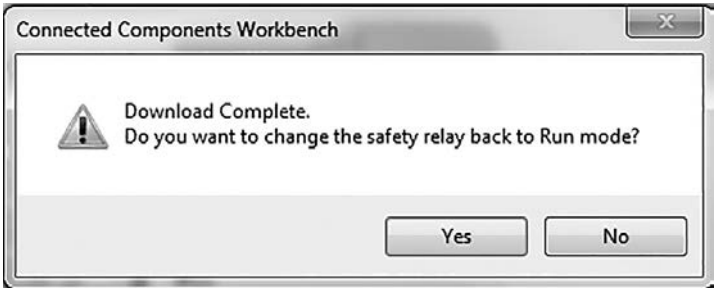
5. Cliquez sur Download.

6. Dans le volet Connection Browser, développez AB_VBP-1 Virtual Chassis et sélectionnez Guardmaster 440C-CR30-22BBB. Cliquez sur OK.

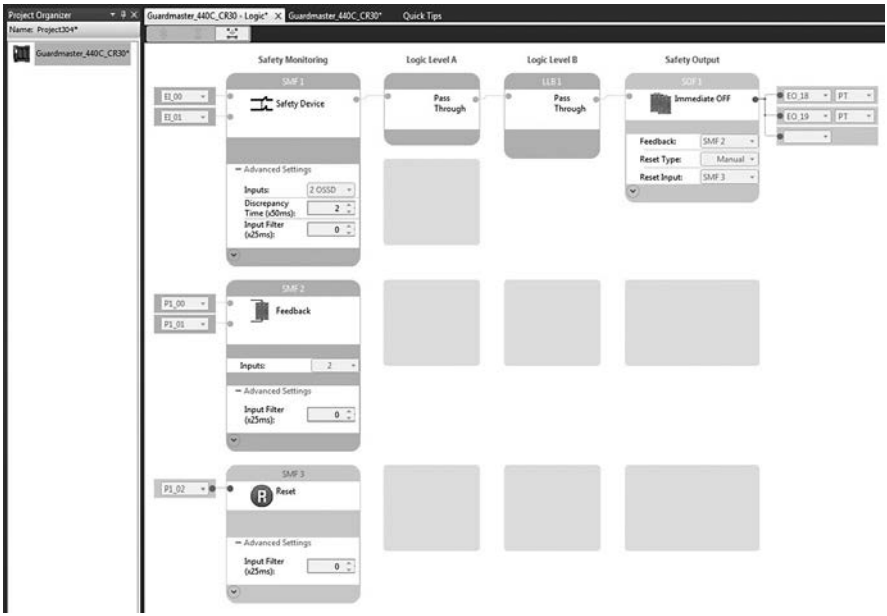


7. Cliquez sur Yes pour passer du mode Exécution (Run) au mode Programmation (Program).

8. Une fois le téléchargement terminé, cliquez sur Yes pour passer du mode Program au mode Run.



9. Cliquez sur Edit Logic pour voir les diagnostics en ligne.

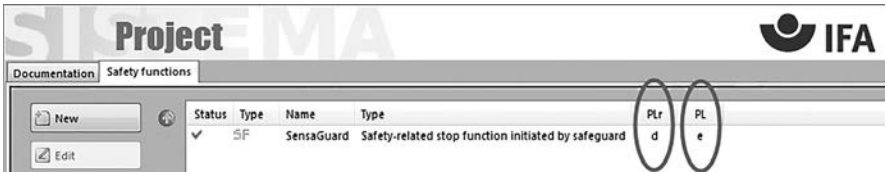


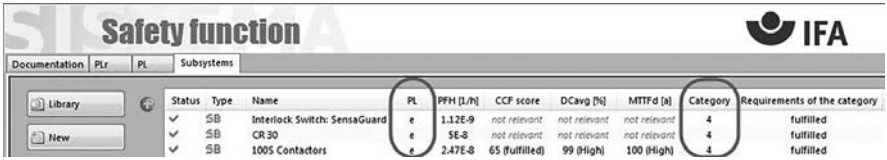
La couleur verte indique qu'un bloc a la valeur True (Vrai) ou qu'une borne d'entrée ou de sortie est active (ON). Un clignotement vert indique qu'une fonction de sortie de sécurité est prête à être réinitialisée.
Le mode de diagnostic en ligne du relais 440C-CR30 peut être très utile pendant le processus de vérification.

10. Examinez les informations dans le calcul du niveau de performance et le plan de vérification et de validation avant de passer à la vérification de la configuration.

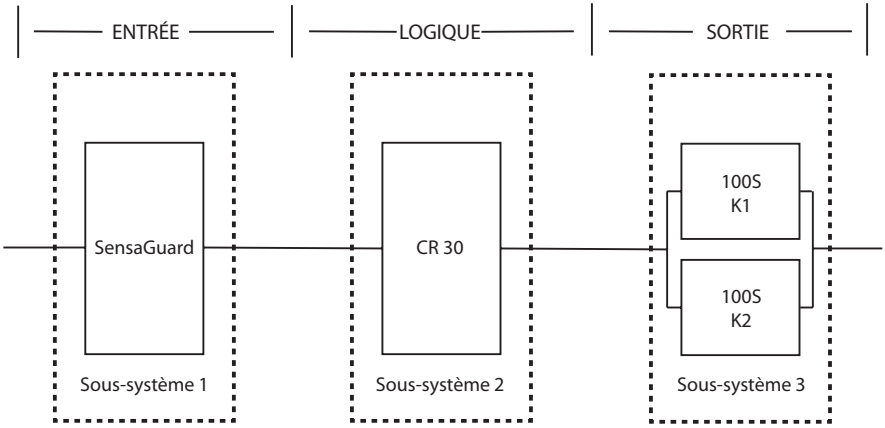
Calcul du niveau de performance

Lorsqu'elle est mise en œuvre correctement, cette fonction d'arrêt de sécurité peut atteindre un niveau de sécurité de Catégorie 4, niveau de performance e (Cat. 4, PLe), selon la norme ISO 13849-1: 2008, comme calculé au moyen de l'outil de calcul de niveau de performance SISTEMA.
Le niveau de performance requis (PLr) minimum découlant de l'évaluation de risque pour cette fonction de sécurité est PLd.





Cet arrêt de sécurité déclenché par une fonction de sécurité peut être modélisé comme suit :



Comme il s'agit de dispositifs électromécaniques, les contacteurs de sécurité incluent les données suivantes :

- Durée moyenne de fonctionnement avant défaillance dangereuse ($MTTF_D$)
- Taux de couverture des tests de diagnostic (DCavg)
- Défaillance de cause commune (CCF)

Les évaluations de sécurité fonctionnelle des dispositifs électromécaniques incluent les aspects suivants :

- La fréquence de leur fonctionnement
- Leur surveillance efficace concernant les défauts
- Leur spécification et leur installation appropriées

SISTEMA calcule la valeur MTTFd en utilisant les données B10d fournies pour les contacteurs, ainsi que la fréquence d'utilisation estimée, laquelle est entrée pendant la création du projet SISTEMA.

La valeur DCavg (99 %) pour les contacteurs est sélectionnée dans le tableau des dispositifs de sortie de la norme ISO 13849-1, Annexe E sur la surveillance directe.

La valeur CCF est générée en utilisant le processus de notation exposé dans l'Annexe F de la norme ISO 13849-1. Le processus de notation de CCF complet doit être réalisé lors de la mise en œuvre effective d'une application. Une note minimum de 65 doit être atteinte.

Plan de vérification et de validation

La vérification et la validation jouent des rôles importants pour éviter les défauts tout au long du processus de conception et de développement du système de sécurité. La norme ISO 13849-2 définit les exigences afférentes à la vérification et à la validation. La norme requiert un plan documenté pour confirmer le respect de toutes les exigences fonctionnelles de sécurité.

La vérification est une analyse du système de commande de sécurité résultant. Le niveau de performance (PL) du système de commande de sécurité est calculé afin de confirmer le respect du niveau de performance requis (PLr) par le système. Le logiciel SISTEMA sert généralement à réaliser les calculs et à faciliter le respect des exigences de la norme ISO 13849-1.

La validation est un test fonctionnel du système de commande de sécurité visant à démontrer que le système répond bien aux exigences spécifiées de la fonction de sécurité. Le système de commande de sécurité est testé afin de confirmer que toutes les sorties de sécurité répondent de manière appropriée à leurs entrées de sécurité correspondantes. Le test fonctionnel inclut les conditions de fonctionnement normales en plus de l'injection de défauts potentiels de modes de défaillance. Une liste de contrôle sert généralement à documenter la validation du système de commande de sécurité.

Avant la validation du système, vérifiez que le relais de sécurité configurable Guardmaster 440C-CR30 est câblé et configuré conformément aux instructions d'installation.

Liste de contrôle de vérification et de validation

Informations générales sur la machine Description	
Nom de machine/numéro de modèle	
Numéro de série de la machine	
Nom du client	
Date du test	
Noms des testeurs	
Numéro du schéma de câblage	
Dispositifs d'entrée	440N-Z21S16B
Relais de sécurité configurable	440C-CR30-22BBB
Variateur de fréquence	
Contacteur de sécurité	100S-C23EJ23BC

Câblage de sécurité et configuration de relais			
Étape de test	**Vérification**	**Bon/ Mauvais**	**Changements/ Modifications**
1	Vérifiez que les caractéristiques des composants sont adaptées à l'application. Reportez-vous aux principes de sécurité de base et aux principes de sécurité éprouvés de la norme ISO 13849-2.		
2	Inspectez visuellement le circuit du relais de sécurité pour vous assurer qu'il est câblé conformément aux schémas.		
3	Vérifiez que la configuration du relais de sécurité configurable 440C-CR30 est la configuration correcte souhaitée.		

Vérification du fonctionnement normal – Le système de sécurité répond correctement à toutes les entrées normales de démarrage, d'arrêt, de réinitialisation, d'arrêt d'urgence et d'interrupteur SensaGuard.			
Étape de test	**Vérification**	**Bon/ Mauvais**	**Changements/ Modifications**
1	Vérifiez qu'aucune personne n'est dans la zone protégée.		
2	Vérifiez que le mouvement dangereux est arrêté.		
3	Vérifiez que la porte est fermée.		
4	Alimentez électriquement le système de sécurité.		
5	Vérifiez que les voyants d'état d'entrée Terminal 00, Terminal 01 et SMF1 du relais de sécurité 440C-CR30 sont allumés en vert. Vérifiez que tous les indicateurs d'état de sortie sont éteints. Assurez-vous que les voyants d'état Power et Run sont allumés en vert. Surveillez l'état approprié du relais de sécurité 440C-CR30 au moyen du logiciel Connected Components Workbench.		
6	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Vérifiez que les voyants d'état de sortie Terminal 18, Terminal 19 et SOF1 sont allumés en vert. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
7	Vérifiez que le mouvement dangereux ne démarre pas à la mise sous tension.		

8	Enfoncez et relâchez le bouton de démarrage du variateur. Vérifiez que le mouvement dangereux commence et que la machine commence à fonctionner.		
9	Enfoncez le bouton d'arrêt externe. La machine doit s'arrêter selon la procédure configurée normale. Le système de sécurité ne doit pas réagir.		
10	Enfoncez et relâchez le bouton de démarrage externe. Vérifiez que le mouvement dangereux démarre et que la machine commence à fonctionner.		
11	Ouvrez la porte protégée. Le système de sécurité doit se déclencher. Le mouvement dangereux doit s'arrêter en moins de 0,7 seconde. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
12	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Le relais de sécurité configurable 440C-CR30 ne doit pas réagir. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
13	Fermez la porte protégée. La machine ne doit pas démarrer. Le relais de sécurité 440C-CR30 ne doit pas réagir. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
14	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. La sortie SOF1 du relais de sécurité 440C-CR30 doit être activée. Le mouvement dangereux ne doit pas démarrer. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
15	Enfoncez et relâchez le bouton de démarrage externe. Vérifiez que le moteur démarre et que la machine commence à fonctionner.		

Validation de la réponse de sécurité à un fonctionnement anormal – Le système de sécurité réagit correctement à tous les défauts prévisibles avec les diagnostics correspondants.			
Tests du relais de sécurité configurable 440C-CR30 et de l'interrupteur SensaGuard			
Étape de test	**Vérification**	**Bon/ Mauvais**	**Changements/ Modifications**
1	Conservez la porte protégée fermée. Alors que le mouvement dangereux se poursuit, débranchez le fil SensaGuard OSSD1 de la borne EI_00 du relais de sécurité 440C-CR30. Le relais de sécurité 440C-CR30 doit se déclencher immédiatement. Le voyant d'état de défaut rouge sur le relais doit clignoter. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
2	Rebranchez le fil sur E1_00. Le relais de sécurité 440C-CR30 ne doit pas réagir. Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Le relais de sécurité 440C-CR30 ne doit pas réagir. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
3	Ouvrez et fermez la porte protégée. Le voyant d'état de défaut rouge doit être éteint. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
4	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. La sortie SOF 1 sur le relais 440C-CR30 doit être activée. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		

5	Enfoncez le bouton de démarrage externe. La machine doit commencer à fonctionner. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench. Cette étape est facultative dans les tests de validation SensaGuard (étapes 6 à 27).		
6	Avec la porte protégée fermée, branchez OSSD 1 sur l'alimentation 24 Vc.c. Après environ 40 secondes, l'interrupteur SensaGuard se déclenche. Le relais de sécurité 440C-CR30 se déclenche. Le voyant d'état de défaut rouge sur le relais de sécurité 440C-CR30 doit clignoter. L'indicateur d'état sur l'interrupteur SensaGuard clignote en rouge. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
7	Débranchez OSSD 1 de l'alimentation 24 V c.c. Ni l'interrupteur SensaGuard, ni le relais de sécurité 440C-CR30 ne réagissent. Enfoncez et relâchez le bouton de redémarrage sur le relais de sécurité 440C-CR30. Ni l'interrupteur SensaGuard, ni le relais de sécurité 440C-CR30 ne réagissent. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
8	Coupez et rétablissez l'alimentation de l'interrupteur SensaGuard. Environ cinq secondes après le rétablissement de l'alimentation au niveau de l'interrupteur SensaGuard, son voyant d'état s'allume en vert et reste allumé. Le voyant d'état de défaut rouge clignotant sur le relais de sécurité 440C-CR30 s'éteint. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
9	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
10	Branchez OSSD 1 sur DC COM. Le relais de sécurité 440C-CR30 se déclenche immédiatement. La lumière rouge d'arrêt de sécurité sur la colonne lumineuse s'allume. La lumière orange de Grille 1 sur la colonne lumineuse s'allume. Le voyant d'état de défaut rouge sur le relais de sécurité 440C-CR30 doit clignoter. L'indicateur d'état sur l'interrupteur SensaGuard clignote en rouge.		
11	Débranchez OSSD1 de DC COM. Ni l'interrupteur SensaGuard, ni le relais de sécurité 440C-CR30 ne réagissent. Enfoncez et relâchez le bouton de redémarrage sur le relais de sécurité 440C-CR30. Ni l'interrupteur SensaGuard, ni le relais de sécurité 440C-CR30 ne réagissent.		
12	Coupez et rétablissez l'alimentation de l'interrupteur SensaGuard. Environ cinq secondes après le rétablissement de l'alimentation au niveau de l'interrupteur SensaGuard, son voyant d'état s'allume en vert et reste allumé. La lumière orange de Grille 1 sur la colonne lumineuse s'éteint. La lumière rouge d'arrêt de sécurité sur la colonne lumineuse reste allumée. Le voyant d'état de défaut rouge clignotant sur le relais de sécurité 440C-CR30 s'éteint.		
13	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. La sortie SOF 1 du relais de sécurité 440C-CR30 doit activer les contacteurs. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
14 à 27	Répétez les étapes 1 à 13 en utilisant EI_01 à la place de EI_00, et OSSD 2 à la place d'OSSD 1.		

28	Connectez OSSD 1 à OSSD 2 (borne EI_00 à borne EI_01). Après environ 50 secondes, l'interrupteur SensaGuard se déclenche. Le relais de sécurité 440C-CR30 se déclenche. L'indicateur d'état sur l'interrupteur SensaGuard clignote en rouge. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
29	Déconnectez OSSD 1 d'OSSD 2. Ni l'interrupteur SensaGuard, ni le relais de sécurité 440C-CR30 ne réagissent. Enfoncez et relâchez le bouton de redémarrage sur le relais de sécurité 440C-CR30. Ni l'interrupteur SensaGuard, ni le relais de sécurité 440C-CR30 ne réagissent.		
30	Coupez et rétablissez l'alimentation de l'interrupteur SensaGuard. Environ cinq secondes après le rétablissement de l'alimentation au niveau de l'interrupteur SensaGuard, son voyant d'état s'allume en vert et reste allumé. Le voyant d'état de défaut rouge clignotant sur le relais de sécurité 440C-CR30 s'éteint. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
31	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. La lumière rouge d'arrêt de sécurité sur la colonne lumineuse doit être éteinte. La sortie SOF1 sur le relais de sécurité 440C-CR30 doit activer les contacteurs. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		

Validation de la réponse de sécurité à un fonctionnement anormal – Le système de sécurité réagit correctement à tous les défauts prévisibles avec les diagnostics correspondants.

Contacteur – Tests du relais de sécurité configurable 440C-CR30

Étape de test	Vérification	Bon/ Mauvais	Changements/ Modifications
1	Alors que la machine continue à fonctionner, rompez la connexion entre la borne EO_18 du relais de sécurité configurable 440C-CR30 et la borne A1 de la bobine K1. Le mouvement dangereux doit ralentir en roue libre jusqu'à l'arrêt.		
2	Enfoncez le bouton d'arrêt externe. Rétablissez la connexion. Enfoncez le bouton de démarrage externe pour reprendre le mouvement dangereux.		
3	Alors que le mouvement dangereux se poursuit, branchez la borne A1 de la bobine K1 sur l'alimentation 24V c.c. Après environ 18 secondes, le relais de sécurité 440C-CR30 doit se déclencher. K2 doit se désactiver. Le mouvement dangereux ralentit en roue libre jusqu'à l'arrêt. Le voyant d'état de défaut rouge sur le relais de sécurité 440C-CR30 est allumé.		
4	Débranchez de l'alimentation 24 V c.c., la borne A1 de la bobine K1. Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Le relais de sécurité 440C-CR30 ne doit pas réagir.		
5	Coupez et rétablissez l'alimentation au niveau du relais de sécurité 440C-CR30. Il réagit. Le voyant d'état de défaut sur le relais de sécurité 440C-CR30 est éteint.		
6	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Enfoncez le bouton de démarrage externe. Le mouvement dangereux doit reprendre.		
7	Alors que la machine continue à fonctionner, raccordez la borne A1 de la bobine K1 à DC COM. Le relais de sécurité 440C-CR30 doit se déclencher. Le voyant d'état de défaut rouge sur le relais de sécurité 440C-CR30 est allumé.		

8	Débranchez de DC COM, la borne A1 de la bobine K1. Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Le relais de sécurité 440C-CR30 ne doit pas réagir.		
9	Coupez et rétablissez l'alimentation au niveau du relais de sécurité 440C-CR30. Le relais de sécurité 440C-CR30 réagit. Le voyant d'état de défaut sur le relais de sécurité 440C-CR30 est éteint.		
10	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Enfoncez le bouton de démarrage externe. Le mouvement dangereux reprend.		
11 à 21	Renouvelez les étapes 1 à 10 avec EO_19 à la place de EO_18, et K2 à la place de K1.		
22	Branchez la borne A1 de K1 à la borne A1 de K2. Après environ 18 secondes, le relais de sécurité 440C-CR30 doit se déclencher. Le mouvement dangereux ralentit en roue libre jusqu'à l'arrêt. Le voyant d'état de défaut rouge sur le relais de sécurité 440C-CR30 est allumé.		
23	Débranchez la borne A1 de K1 de la borne A1 de K2. Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Le relais de sécurité 440C-CR30 ne doit pas réagir.		
24	Coupez et rétablissez l'alimentation au niveau du relais de sécurité 440C-CR30. Il réagit. Le voyant d'état de défaut sur le relais de sécurité 440C-CR30 est éteint.		
25	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Enfoncez le bouton de démarrage externe. Le mouvement dangereux doit reprendre.		

Validation de la réponse de sécurité à un fonctionnement anormal – Le système de sécurité réagit correctement à tous les défauts prévisibles avec les diagnostics correspondants.

Signal de retour du contacteur – Tests du relais de sécurité configurable 440C-CR30

Étape de test	Vérification	Bon/ Mauvais	Changements/ Modifications
1	Alors que la machine continue de fonctionner, débranchez la connexion de retour K1 au niveau de la borne P1_00. La machine doit continuer à fonctionner.		
2	Ouvrez la porte protégée. Le système de sécurité doit se déclencher. Le mouvement dangereux doit s'arrêter en moins de 0,7 seconde. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
3	Fermez la porte protégée. La machine ne doit pas démarrer. Le relais de sécurité 440C-CR30 ne doit pas réagir. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
4	Enfoncez et relâchez le bouton de réinitialisation sur le relais de sécurité 440C-CR30. Le relais de sécurité 440C-CR30 ne doit pas réagir. Surveillez le fonctionnement approprié au moyen des voyants d'état et l'état approprié du relais de sécurité 440C-CR30 au moyen de Connected Components Workbench.		
5	Remettez en place la connexion au niveau de P1_00. Coupez et rétablissez l'alimentation au niveau du relais 440C-CR30. Enfoncez le bouton de réinitialisation sur le relais 440C-CR30. Les sorties du relais 440C-CR30 doivent être activées. Enfoncez et relâchez le bouton de démarrage externe. Vérifiez que le moteur démarre et que la machine commence à fonctionner.		
6	Répétez les étapes 1 à 5 en utilisant la connexion de retour K2 au niveau de la borne P1_01.		

Vérification de la configuration

Le système doit vérifier la configuration de chaque application individuelle au moyen de la commande Verify. Si le relais de sécurité configurable 440C-CR30 n'est pas vérifié, il sera placé en défaut après 24 heures de fonctionnement.

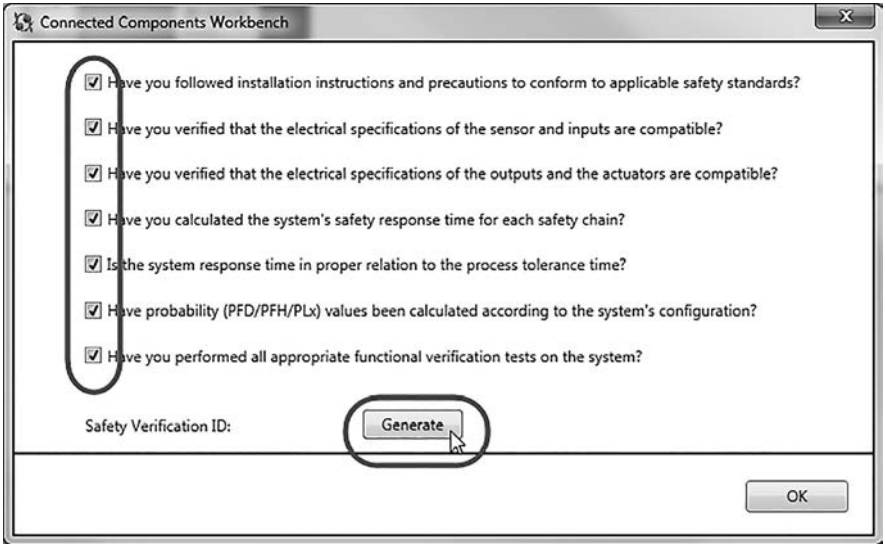
ATTENTION : le processus de vérification doit être documenté dans le dossier technique du système de sécurité.

Procédez comme suit pour télécharger et vérifier la configuration.

1. Vérifiez que le relais 440C-CR30 est sous tension et connecté à votre station de travail via le câble USB.
2. Vérifiez l'indication de relais 440C-CR30 connecté en haut à droite dans l'onglet Project de Connected Components Workbench. Si ce n'est pas le cas, cliquez sur Connect to Device pour établir la connexion logicielle.

3. Cliquez sur Verify.

4. Répondez à toutes les questions et cochez chaque case si nécessaire. Cliquez sur Generate.

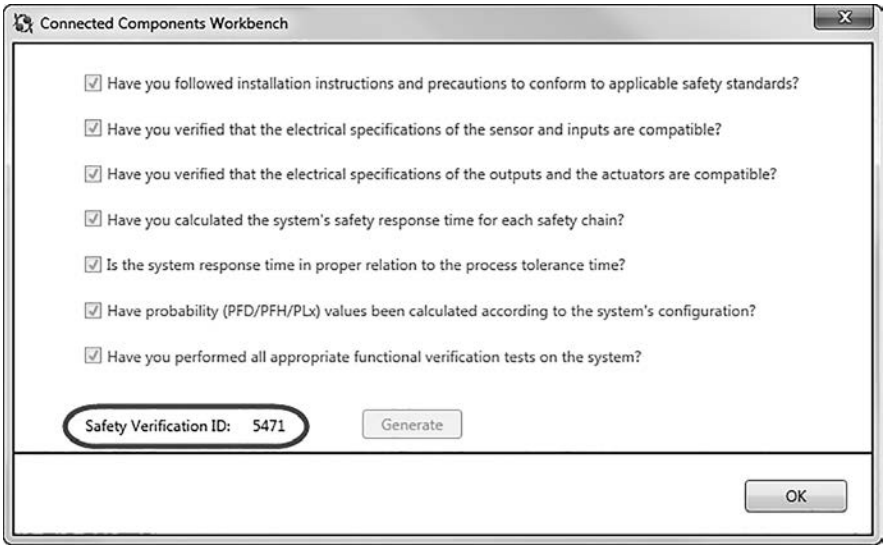


IMPORTANT : toutes les cases doivent être sélectionnées pour générer l'ID de vérification.

6. Cliquez sur Yes pour poursuivre la vérification.

7. Cliquez sur Yes pour passer au mode Exécution (Run).

8. Notez l'ID de vérification de sécurité dans la documentation de la machine.



Ce processus fournit au relais 440C-CR30 l'information que la vérification du système et les tests fonctionnels ont été réalisés. L'ID de vérification unique peut servir à vérifier si des modifications ont été apportées à un fichier de configuration. Toute modification de la configuration supprime l'ID de vérification de sécurité. Les actions de vérification consécutives génèrent un ID de vérification différent. L'ID de vérification de sécurité est visible dans Connected Components Workbench uniquement lorsque vous êtes connecté au relais 440C-CR30.

Chapitre 11 : Produits, outils et services

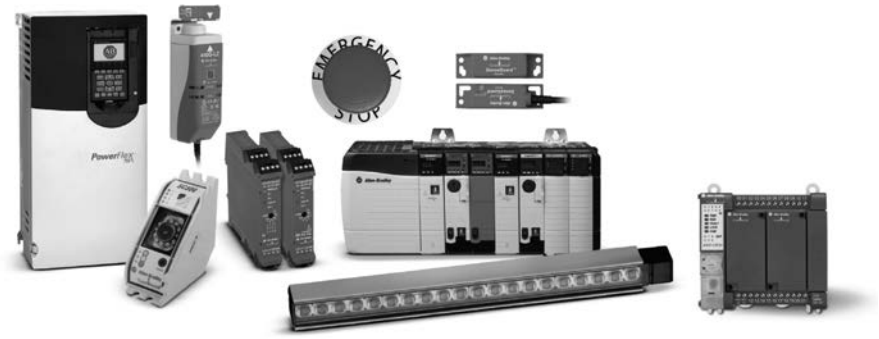
Présentation

Rockwell Automation est un leader mondial en matière de solutions industrielles d'alimentation, de commande et d'information, et la société se tient au côté de ses clients dans de nombreux secteurs depuis plus de 100 ans. Une partie de sa gamme d'automatisation industrielle propose des technologies, outils et services complets de sécurité des machines.

Des produits et technologies pour vos applications

Rockwell Automation propose la plus grande gamme de solutions de sécurité pour machines et peut fournir les trois composantes d'un système de sécurité (dispositif d'entrée, logique de commande et élément de puissance final).

Les produits et technologie suivants sont disponibles :



Dispositifs d'entrée de sécurité

- **Dispositifs de sécurité de détection de présence**
  Ces dispositifs détectent l'emplacement des objets et du personnel près des zones dangereuses. On trouve parmi eux : les barrières immatérielles de sécurité, les scrutateurs laser de sécurité, les détecteurs de sécurité de main, les tapis et bourrelets sensibles à la pression

- **Interrupteurs de sécurité**
  Les interrupteurs de sécurité sont conçus et fabriqués conformément aux normes internationales, afin de garantir un niveau élevé de fiabilité, de stabilité et de qualité. Les interrupteurs de sécurité incluent les interrupteurs de fin de course et interrupteurs de verrouillage, ainsi que les interrupteurs d'arrêt d'urgence.

- **Dispositifs d'arrêt d'urgence et de déclenchement**
  Les interrupteurs d'arrêt d'urgence incluent une gamme de boutons-poussoirs « coup de poing » avec contacts à guidage réciproque. Les poignées de sécurité « homme mort » et les interrupteurs à câble assurent la fonction d'urgence sur l'ensemble d'une application ou sont fixes pour permettre le mouvement de l'opérateur au sein de l'application de sécurité.

- **Interface opérateur**
  Les dispositifs d'interface opérateur permettent à l'opérateur d'interagir avec l'application et offrent une fonctionnalité de sécurité dédiée supplémentaire.

Automates de sécurité

- **Relais de sécurité (fonction unique ou configurable)**
  Les relais de sécurité vérifient et surveillent un système de sécurité, et permettent de commander le démarrage ou l'arrêt de la machine. Les relais de sécurité monovalant sont la solution la plus économique pour les petites machines nécessitant un dispositif logique dédié pour la fonction de sécurité. Des relais de surveillance de sécurité modulaires et configurables seront préférables dans le cas où des dispositifs de protection variés et nombreux, ainsi qu'une commande de zone minimale, sont requis.

- **Automates de sécurité intégrés**
  Les API de sécurité apportent les avantages des systèmes d'API traditionnels aux applications de sécurité et remplacent les systèmes de relais câblés généralement requis pour placer les processus automatisés dans un état de sécurité. Les API de sécurité permettent à des programmes standard et de sécurité de résider dans un seul châssis d'automate, d'où une programmation gagnant en flexibilité et un environnement familier et convivial pour les programmeurs. Les solutions d'automate de sécurité assurent un contrôle ouvert et intégré, qui vous aidera à garantir la sécurité des machines et la protection de vos actifs.

- **Dispositifs d'E/S de sécurité**
  Les produits de sécurité Guard I/O™ offrent tous les avantages des E/S distribuées traditionnelles, mais sont conçus pour les systèmes de sécurité. Ils réduisent les coûts de câblage et les délais de démarrage des machines et cellules, et sont disponibles avec une multitude de caractéristiques pour les applications en armoire et On-Machine.

Actionneurs de sécurité

- **Contacteurs de sécurité et démarreurs**
  Les départs-moteurs distribués ArmorStart® proposent une sécurité de Catégorie 4 tout en proposant une solution de sécurité intégrée à votre installation de sécurité DeviceNet™ On-Machine™. Les contacteurs auxiliaires et contacteurs de sécurité CEI contribuent à protéger le personnel des démarrages imprévus de machine et de la perte de la fonction de sécurité.

- **Variateurs c.a. PowerFlex®**
  Les variateurs PowerFlex sont disponibles avec des fonctions de sécurité. Les variateurs c.a. PowerFlex 525 intègrent en standard la fonction d'arrêt sécurisé du couple. L'arrêt sécurisé du couple est en option pour les variateurs c.a. PowerFlex Série 40P, 70, 700H, 700S et 750, ils prennent aussi en charge la fonctionnalité de surveillance de la vitesse de sécurité.

- **Commande d'axe intégrée Kinetix®**
  Les servovariateurs Kinetix 300, 6000, 6200, 6500 et 7000 intègrent tous la fonctionnalité de sécurité. Grâce à l'arrêt sécurisé du couple, une sortie de variateur est désactivée afin de couper le couple moteur sans interrompre l'alimentation électrique de toute la machine. Avec la surveillance de la vitesse de sécurité, les utilisateurs peuvent réduire et surveiller la vitesse de l'application, afin d'aider l'opérateur à réaliser en toute sécurité certains types de travaux sans un arrêt complet de la machine.

Systèmes de connexion/réseaux

- **Systèmes de connexion de type « connexion rapide »**
  Les répartiteurs/raccords en T de sécurité Guardmaster®, les boîtiers de distribution et les fiches de court-circuitage font partie du système de connexion rapide dédié à la sécurité de la machine.

- **GuardLink™**
  GuardLink est un protocole de communications de sécurité qui utilise le câblage standard en topologie « Ligne et dérivation » avec des connexions « plug and play ». Il autorise les communications des dispositifs de sécurité pour les diagnostics et le contrôle, tels que les commandes de réinitialisation et de verrouillage à distance sur un câble unique. 32 dispositifs au maximum sont connectables sur une

distance de câble maximale de 1000 mètres. Les dispositifs de sécurité Allen-Bradley avec technologie GuardLink vous proposent d'accéder aux informations de système de sécurité et permettent leur accessibilité sur EtherNet/IP. GuardLink peut contribuer à simplifier la configuration du système, à réduire le câblage et à augmenter les informations de diagnostic pour la maintenance et le fonctionnement.

- **Sécurité sur EtherNet/IP**
  Le réseau EtherNet/IP™ permet l'interconnexion de systèmes à l'échelle de l'usine, au moyen de technologies de réseau standard et ouvertes. Il propose un contrôle et des informations en temps réel pour les applications de processus continus et discontinus, de sécurité, de variateur, de commande d'axe et de haute disponibilité. Les réseaux EtherNet/IP connectent les dispositifs tels que des démarreurs et détecteurs aux automates et dispositifs IHM, puis dans le reste de l'entreprise. Ils prennent en charge les communications non industrielles et industrielles sur une seule infrastructure réseau commune.

Des outils à votre service

Un large choix d'outils assurent la conformité vis-à-vis des normes de sécurité, réduisent les risques de blessures et améliorent la productivité.

Safety Automation Builder

Cet outil logiciel GRATUIT contribue à simplifier la conception et la validation de la sécurité des machines, pour des délais et coûts en baisse. L'intégration au logiciel d'évaluation des risques RASWin offre aux utilisateurs une gestion documentée, fiable et cohérente du cycle de vie de la sécurité fonctionnelle. Safety Automation Builder rationalise la conception d'un système de sécurité, afin d'améliorer la conformité et de réduire les coûts. Pour cela, l'outil guide les utilisateurs pendant le développement des systèmes de sécurité, notamment pendant la configuration, la sélection des produits et l'analyse de sécurité, l'objectif étant de respecter les exigences de la norme internationale (EN) ISO 13849-1 concernant le niveau de performance (PL) de sécurité des machines.

RASWin

Le logiciel RASWin aide les utilisateurs à gérer les différentes phases du cycle de vie de la sécurité fonctionnelle, par une organisation des informations à chaque étape du processus et de la validation des machines. RASWin relie les étapes du cycle de vie de la sécurité afin d'éviter des défaillances systématiques et il inclut les caractéristiques de fonction de sécurité, l'affectation des exigences de niveau de performance (PLr) et le calcul de PLr, la validation du circuit de sécurité et la documentation.

Outil de calcul de niveau de performance SISTEMA

Cet outil développé par L'Institut allemand pour la sécurité au travail et la santé des organismes d'assurance-accident (IFA) automatise le calcul du niveau de

performance atteint des composants de sécurité d'un système de commande de machine par rapport à la norme (EN) ISO 13849-1. Les données concernant les produits de sécurité pour machines de Rockwell Automation sont disponibles sous la forme d'une bibliothèque utilisable avec SISTEMA. L'association des deux procure aux concepteurs de machines et systèmes une assistance complète pour l'évaluation plus rapide de la sécurité selon la norme (EN) ISO 13849-1. Une fonction d'exportation de Safety Automation Builder permet l'importation aisée de la conception de systèmes de sécurité dans SISTEMA, afin qu'un tiers puisse vérifier le niveau de performance requis.

Fonctions de sécurité préconfigurées pour les machines

Les fonctions de sécurité des machines nécessitent de multiples éléments, notamment un détecteur ou dispositif d'entrée, un dispositif logique et un dispositif de sortie. Ensemble, ces éléments fournissent un niveau de protection déterminé sous forme de niveau de performance, comme défini dans la norme (EN) ISO 13849-1. Rockwell Automation a élaboré de nombreux documents de fonction de sécurité. Chacun fournit des recommandations pour une fonction de sécurité spécifique, sur la base des exigences fonctionnelles, de la sélection des équipements et des exigences de niveau de performance. Ils abordent l'installation et le câblage, la configuration, le plan de vérification et de validation, ainsi que le calcul du niveau de performance.

Outil Safety maturity Index

L'outil Safety Maturity Index™ permet une mesure complète des performances dans la culture de sécurité, dans les processus et procédures de conformité, et pour les investissements financiers dans les technologies de sécurité. Il aide les entreprises à comprendre leur niveau de performance actuel et les mesures à prendre pour améliorer la sécurité et la rentabilité.

Les services et l'expérience dont vous avez besoin

En tant que premier fournisseur mondial dans le domaine de la sécurité industrielle, Rockwell Automation peut vous aider à réduire les blessures et les coûts, tout en rehaussant la productivité dans toutes les phases du cycle de vie de la sécurité.

Les services de sécurité sont fournis par du personnel ayant l'expérience et les qualifications requises en la matière ; nombre d'entre eux ont des certifications en sécurité des machines de l'organisme TÜV Rheinland. Rockwell Automation emploie des techniciens, ingénieurs et experts en sécurité fonctionnelle certifiés par le TÜV afin d'aider les clients dans leur démarche holistique du cycle de vie de la sécurité.

L'approche Safety Life Cycle est un processus clairement défini qui contribue à optimiser la productivité et à améliorer la sécurité par une identification des étapes nécessaires à l'évaluation et à l'atténuation des risques pour les machines. Le concept Safety Life Cycle est présenté dans ce document téléchargeable.

Les services suivants sont entre autres proposés :

- **Évaluations de la sécurité**
  Ces services aident à évaluer les risques des usines et à prendre des décisions avisées pour améliorer la sécurité des employés et des machines.

- **Services de conception**
  Services englobant la conception complète de circuits, l'application correcte des dispositifs et des examens de conception, afin d'améliorer la sécurité globale.

- **Services d'installation et de validation**
  Services contrôlant le fonctionnement des systèmes conformément aux paramètres et normes définis.

- **Formation sur la sécurité**
  Programmes de formation complets dispensés par les meilleurs experts de l'industrie.

- **Services personnalisés**
  Prestations couvrant les applications, les technologies, les plates-formes et les configurations propres aux clients.

Le choix de Rockwell Automation

L'intégration de la sécurité à l'automatisation peut améliorer la productivité à de nombreux stades de la fabrication, à savoir de la conception des équipements et des tests, de l'installation et de la mise en service, jusqu'à l'exploitation et la maintenance, puis jusqu'à la modification ou la mise hors service. Toutes les étapes sont optimisables à travers des solutions de sécurité mises en œuvre intelligemment.

En tant que leader mondial dans l'automatisation et la sécurité industrielles et en tant qu'entreprise créatrice de technologies, Rockwell Automation est parfaitement positionnée pour vous aider à développer des solutions de production plus efficaces, plus sûres et plus productives.

Par ses nombreuses années d'expérience dans l'automatisation et la sécurité, ses connaissances des applications et la mise en œuvre de principes directeurs d'avant-garde dictés par les normes de sécurité telles que ISO 12000, (EN) ISO 13849-1 et CEI 62061, Rockwell Automation peut vous aider pour la sélection, l'intégration, la formation et le support technique concernant les solutions de sécurité des machines, de sécurité des processus et de sécurité électrique.

www.rockwellautomation.com

Siège des activités « Power, Control and Information Solutions »

Amériques : Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 Etats-Unis, Tél: +1 414.382.2000, Fax : +1 414.382.4444
Europe / Moyen-Orient / Afrique : Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgique, Tél: +32 2 663 0600, Fax : +32 2 663 0640
Asie Pacifique : Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tél: +852 2887 4788, Fax : +852 2508 1846

Canada : Rockwell Automation, 3043 rue Joseph A. Bombardier, Laval, Québec, H7P 6C5, Tél: +1 (450) 781-5100, Fax: +1 (450) 781-5101, www.rockwellautomation.ca
France : Rockwell Automation SAS – 2, rue René Caudron, Bât. A, F-78960 Voisins-le-Bretonneux, Tél: +33 1 61 08 77 00, Fax : +33 1 30 44 03 09
Suisse : Rockwell Automation AG, Av. des Baumettes 3, 1020 Renens, Tél: 021 631 32 32, Fax: 021 631 32 31, Customer Service Tél: 0848 000 278

Publication : SAFEBK-RM002C-FR-P – Novembre 2016