

1- Préface

Le but de cette section est de fournir aux constructeurs de machines une première introduction à certaines normes relatives à la sécurité des machines, clarifier certains principes de base et donner quelques exemples d'application. Ce petit guide se réfère uniquement aux aspects de la Sécurité Fonctionnelle de la machine, c'est-à-dire l'ensemble de mesures propres à protéger l'opérateur des machines des risques découlant de leur fonctionnement. Ne sont pas traités les risques dus à d'autres sources de danger telles que la présence d'électricité, appareils à pression, atmosphères explosives, etc., qui devront être évalués quand même par le fabricant des machines.

Ce document a été préparé par Pizzato Elettrica au mieux de ses connaissances, en tenant compte les nouvelles normes et interprétations et les technologies existantes dans l'année 2009. Étant donné que certaines normes mentionnées trouvent lors de ces mois leurs premières applications réelles, on ne peut pas exclure qu'avec le temps des normes supplémentaires ou interprétations par les organismes notifiés modifient les évaluations fournies dans ce document. Les exemples devraient donc toujours être évalués par le client final selon l'état de l'art technologique /normatif et ils ne le déchargent pas de sa responsabilité. Pizzato Elettrica n'assume aucune responsabilité sur les exemples donnés et n'exclut pas la présence éventuelle d'erreurs involontaires ou d'inexactitudes dans les données fournies.

2- Concevoir en toute sécurité. La structure normative européenne.

Tout dispositif ou machine, pour être librement commercialisé à l'intérieur des pays de la Communauté européenne, doit satisfaire aux prescriptions des directives communautaires.

Elles fournissent les principes généraux pour que les fabricants mettent en vente des produits qui ne sont pas dangereux pour les opérateurs. L'ensemble des produits et des différents dangers potentiels est très large et donc au cours de temps ont été émises plusieurs directives. Par exemple on cite la directive Basse Tension 2006/95/EC, la directive 94/9/EC sur les Atmosphères Explosives, la directive sur la Compatibilité Electromagnétique 2004/108/EC, etc. Les dangers résultants du fonctionnement des machines sont traités par la Directive Machine 98/37/EC qui à partir de 29/12/2009 sera remplacée par la nouvelle directive 2006/42/EC.

La conformité aux directives est certifiée par l'émission de la Déclaration de Conformité par le constructeur et par l'apposition du marquage CE sur la machine.

Pour l'évaluation des risques que la machine présente et pour la réalisation des systèmes de sécurité aptes à protéger l'opérateur de ces risques, les comités européens de normalisation CEN et CENELEC ont promulgué une série de normes qui traduisent le contenu des directives sous forme d'indications techniques.

Les normes qui sont publiées dans le Journal Officiel de l'Union Européenne s'entendent harmonisées. Le constructeur qui utilise ces normes pour la certification de ses machines a la présomption de conformité aux directives.

Les normes pour la sécurité des machines se divisent en trois types: A, B et C.

Normes de type A: Ce sont des normes qui exposent les concepts de base et les principes de conception générale pour la réalisation de toutes les machines.

Normes de type B: Ce sont des normes qui exposent plus spécifiquement un ou plusieurs aspects relatifs à la sécurité et qui à leur tour sont divisées en normes de type:

- B1: Normes relatives à certains aspects de la sécurité (par exemple distances de sécurité, températures, bruits, etc.)
- B2: Normes relatives aux dispositifs de sécurité (par exemple contrôles bimanuels, dispositifs de verrouillage, protecteurs, etc.)

Normes de types C: Ce sont des normes qui exposent de manière détaillée les prescriptions de sécurité pour des groupes de machines particulières (ex. presses hydrauliques, machines à injecter,...)

Le constructeur de dispositifs ou de machines devra tout d'abord vérifier si son produit entre dans une norme de type C. Dans le cas positif, ce sera cette norme qui établira les prescriptions pour la sécurité, sinon, ce seront les normes de type B qui feront foi pour tout aspect ou dispositif spécifique du produit. En absence de spécifications supplémentaires, le constructeur suivra les principes généraux énoncés dans les normes de type A.

NORMES DETYPE A

par exemple:

EN 12100-1 et -2 (remplace EN 292-1 et EN 292-2).
Concepts fondamentaux, principes généraux de conception.
EN 61508-1-7. Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables pour applications de sécurité.
EN 14121: Principes pour l'évaluation du risque.

NORMES DETYPE B1

par exemple:

EN 62061:2005 Sécurité fonctionnelle des systèmes de commande et de contrôle électriques, électroniques et électroniques programmables relatifs à la sécurité
EN ISO 13849-1:2006 et -2:2003 Parties des systèmes de commande liées à la sécurité

NORMES DETYPE B2

par exemple:

EN 574:1996 Dispositifs de commande bimanuelle
EN 13850:2006 (remplace EN 418:1992)
Arrêt d'urgence
EN 1088:1995 Dispositifs de verrouillage des protecteurs
EN 60204-1:2006 Équipement électrique des machines
EN 60947-5-1:2004 Dispositifs de contrôle électromécaniques

NORMES DETYPE C

par exemple:

EN 201:1997. Machines pour le caoutchouc et les matières plastiques – Machines à injecter
EN 415-1.-7:2000 Sécurité des machines d'emballage
EN 692:2005 Presses mécaniques
EN 693:2001 Presses hydrauliques
EN 848-1:2007 Sécurité des machines pour le travail du bois – Machines à fraiser sur une face, à outil rotatif
- Partie 1: Toupie monobroche à arbre vertical

3 – Concevoir machines sûres. Analyse des risques.

La première étape dans la construction d'une machine sûre est d'identifier quels sont tous les éventuels dangers auxquels sont exposés les opérateurs d'une machine. L'identification et la classification des risques permettent de définir le risque pour l'opérateur c'est-à-dire la combinaison de la probabilité que le danger se produit et du type de dommage possible à l'opérateur.

La méthodologie d'analyse des risques, de leur évaluation, de la façon de procéder pour leur réduction est définie par les normes EN 12100 et EN 14121. Ces normes introduisent un modèle cyclique d'analyse afin que, défini les objectifs initiaux, l'analyse des risques et des solutions possibles pour limiter ces risques sont évalués plusieurs fois jusqu'à ce que les objectifs initiaux ne sont pas remplis.

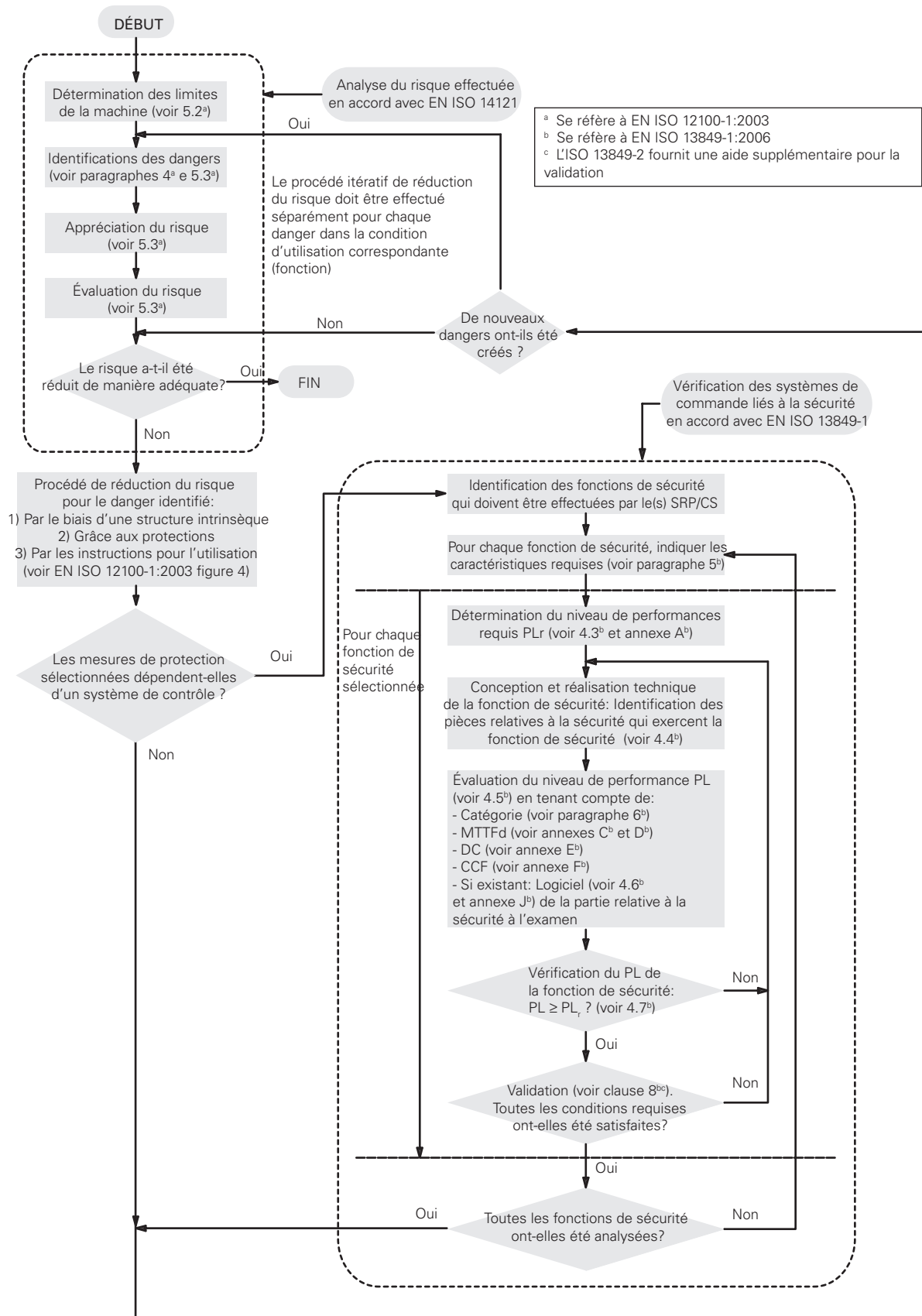
Le modèle introduit par cette paire de normes prévoit que, après une analyse des risques selon EN 14121, on procède pour leur réduction / élimination par un processus qui comprend par ordre:

- 1) L'élimination des risques à l'origine, grâce à la structure du système et l'utilisation de principes de conception intrinsèquement sûrs
- 2) La réduction des risques par des systèmes de protection et de contrôle
- 3) La mise en évidence des risques résiduels au moyen de signalisation et information aux opérateurs.

Étant donné que chaque machine a des dangers et qu'il n'est pas possible d'éliminer complètement tous les possibles risques associés,

l'objectif est de réduire le risque de la machine à des niveaux résiduels acceptables.

Si le risque est réduit par un système de contrôle, entre en jeu la norme EN ISO 13849, qui fournit un modèle d'évaluation de la qualité de ce système. De cette façon, étant donné le risque d'un certain niveau, il est possible d'utiliser une fonction de sécurité de même niveau ou supérieur.



Note: Cette figure a été obtenue par la combinaison des Figures 1 et 3 de EN ISO 13849-1:2006. Les textes reportés sont la traduction non officielle des textes en anglais.

1
1A
1B
2
2A
2B
2C
2D
2E
3
3A
3B
3C
4
4A
4B
4C
4D
4E
4F
4G
4H
5
6

4 – Situation normative actuelle (année 2009). Les raisons du changement, les nouvelles normes et quelques superpositions

Les normes "traditionnelles" pour la sécurité fonctionnelle, telles que l'EN 954-1, ont eu le grand mérite de formaliser certains principes de base dans l'analyse des circuits de sécurité selon principes déterministes. D'autre part, elles ne traitent absolument pas les dispositifs électroniques programmables et, en général, souffrent des années passées. Pour inclure les dispositifs électroniques programmables dans l'analyse des systèmes de contrôle, l'approche de nouvelles normes est fondamentalement de type probabiliste et on a ensuite introduit de nouvelles variables de type statistiques.

La norme «mère» de cette approche est la IEC 61508 qui définit la sécurité des systèmes électroniques programmables complexes et est une norme imposante (divisée en 8 sections, pour un total de plus de 500 pages) adaptée à des champs d'application même très différents (industrie de procédés, machines industrielles, installations nucléaires); ce sont les raisons pour lesquelles elle a assumé le statut de norme de type A (non harmonisée). Cette norme introduit le concept de SIL (Safety Integrity Level), c'est-à-dire une indication probabiliste du risque résiduel d'un système.

De l'IEC 61508 dérive l'EN 62061, en particulier pour ce qui concerne la sécurité des systèmes avec électronique complexe ou quand même programmable dans les machines industrielles. Les concepts introduits permettent l'application en général à tout système de contrôle avec technologie de type électrique, électronique et électronique programmable (à l'exclusion de systèmes avec technologies non-électriques).

L'EN ISO 13849, développée par le CEN sous l'égide de l'ISO, dérive de cette approche probabiliste mais tente de faire en sorte que le constructeur habitué aux concepts de l'EN 954-1 peut passer d'une façon moins traumatisante aux nouveaux concepts. La norme s'applique aux systèmes électromécaniques, hydrauliques, électroniques «non complexes» et certains systèmes électroniques programmables avec des structures prédéfinies. La norme EN ISO 13849 est une norme de type B1, introduit la notion de PL (Performance Level) c'est-à-dire, comme pour le SIL, une indication probabiliste du risque résiduel d'une machine. Cette norme indique une corrélation entre SIL et PL, utilise des concepts (comme DC et CCF) changés par la IEC 61508 et établi une référence avec les catégories de sécurité de l'EN 954-1.

Dans le domaine de la sécurité fonctionnelle, pour la sécurité des circuits de contrôle, trois normes sont donc actuellement en vigueur (année 2009):

- EN 954-1:1996. C'est une norme de type B1, qui a introduit le concept des Catégories de Sécurité, maintenant sur le point d'expirer. L'actuelle EN 954-1:1996 restera en vigueur jusqu'à Novembre 2009, date à laquelle elle sera officiellement remplacé par l'EN ISO 13849. Pour la diffusion qu'elle a eu dans les années passées cette norme sera encore pour longtemps une référence technique.
- EN ISO 13849:2006. Norme de type B1 qui utilise le concept de PL.
- EN 62061:2005. Norme de type B1 qui utilise le concept de SIL.

| PL | a | b | c | d | e | |
|--|------------------|------------------|--------------------|------------------|------------------|------------------|
| EN ISO 13849-1 | | | | | | |
| SIL | - | 1 | 2 | 3 | (4) | |
| EN 62061 - IEC 61508 | | | | | | |
| PFHd | 10 ⁻⁴ | 10 ⁻⁵ | 3x10 ⁻⁶ | 10 ⁻⁶ | 10 ⁻⁷ | 10 ⁻⁸ |
| Une défaillance dangereuse chaque n° ans | ~1 | ~10 | ~40 | ~100 | ~1000 | ~10000 |

Les deux normes EN 62061 et EN 13849 ont donc une raisonnable superposition en ce qui concerne le domaine d'application et pour de nombreux aspects sont similaires à tel point qu'il existe une corrélation précise entre les deux différents noms symbole (SIL et PL), qui indiquent le résultat de l'analyse selon les deux normes.

Les recommandations sur le domaine d'application des deux normes est reporté dans le tableau 1 de l'EN 13849 et comme on peut le voir, sur de grandes typologies de produits tous les deux normes sont applicables.

Tableau 1 – Applications recommandées par IEC 62061 et EN ISO 13849-1

| | Technologie utilisée par la partie du système de commande liée à la sécurité | EN ISO 13849-1 | IEC 62061 |
|---|--|---|---|
| A | Non électrique, par exemple hydraulique | X | Non traitée |
| B | Électromécanique, par exemple relais et/ou électronique non complexe | D'une manière limitée aux architectures dessinées et jusqu'à PL=e | Toutes les architectures et jusqu'à SIL 3 |
| C | Électronique complexe, par exemple programmable | D'une manière limitée aux architectures dessinées et jusqu'à PL=d | Toutes les architectures et jusqu'à SIL 3 |
| D | A associée à B | D'une manière limitée aux architectures dessinées et jusqu'à PL=e | X ^c |
| E | C associée à B | D'une manière limitée aux architectures dessinées (voir note 1) et jusqu'à PL=d | Toutes les architectures et jusqu'à SIL 3 |
| F | C associée à A ou C associée à A et B | X ^b | X ^c |

X indique que la ligne est traitée par la norme internationale indiquée dans l'en-tête de la colonne

- Les architectures dessinées sont définies au point 6.2 (de l'EN ISO 13849-1) pour fournir une approche simplifiée à la quantification du niveau de performances
- Pour l'électronique complexe: utiliser les architectures dessinées en accord avec cette partie de l'EN ISO 13849-1 et jusqu'à PL=d ou toute autre architecture en accord avec l'IEC 62061
- Pour les technologies non électriques, utiliser les parties comme sous-systèmes en accord avec cette partie de l'EN ISO 13849-1

Note. Le présent tableau est la traduction non officielle en français du tableau 1 présent dans la version anglaise de la norme EN ISO 13849-1:2006

Le choix de la norme à utiliser reviendra au constructeur, selon la technologie utilisée. Nous retenons que l'EN 13849, avec une approche intermédiaire et la réutilisation des concepts déjà connus dans le marché, est une norme d'application plus facile.

Note: L'institution pour la prévention et la sécurité allemande BGIA a introduit en 2008 un rapport (BGIA Report 2/2008) sur l'application de l'EN 13849 où il est indiqué que les recommandations et les limites sur l'application de l'13849 doivent être considérés comme obsolètes et donc aussi dans le cas d'électronique programmable (cas C et E du tableau ci-dessus) on peut considérer le limite PL_e.

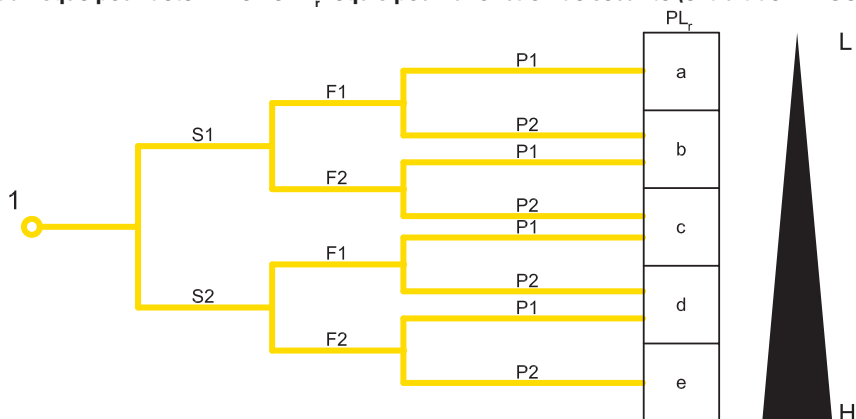
5- La norme EN ISO 13849 et les nouveaux paramètres: PL, MTTF_d, DC, CCF

La norme EN ISO 13849 offre au constructeur une méthode itérative pour évaluer si les risques d'une machine peuvent être limités à un niveau résiduel acceptable par l'utilisation des fonctions de sécurité appropriées. La méthode adoptée prévoit, pour chaque risque, un cycle d'hypothèse-analyse-validation à la fin de lequel on doit être en mesure de démontrer que chaque fonction de sécurité choisie est adaptée au relatif risque à l'examen.

La première étape consiste donc dans l'évaluation du niveau de performance requis pour chaque fonction de sécurité. Comme pour l'EN 954-1 même l'EN ISO 13849 utilise un graphique pour l'analyse du risque d'une fonction d'une machine (Figure A.1) mais au lieu d'une catégorie de sécurité requise, elle définit, en fonction du risque, un niveau de performance requis ou PL_r (Required Performance Level) pour la fonction de sécurité qui devra protéger cette partie de machine.

Le constructeur de la machine, à partir du point 1 du graphique et en répondant aux questions S, F et P, identifiera le PL_r pour la fonction de sécurité examinée. Ensuite il devra réaliser un système pour protéger l'opérateur de la machine qui aura un niveau de performance PL égal ou meilleur de celui requis.

Graphique du risque pour déterminer le PL_r requis pour la fonction de sécurité (extrait de EN ISO 13849-1, figure A.1)



Clés de lecture

- 1** Point de départ pour l'évaluation de la contribution à la réduction du risque des fonctions de sécurité
- L** Faible contribution à la réduction du risque
- H** Forte contribution à la réduction du risque
- PL_r** Niveau de performance requis

Paramètres de risque

- S** Gravité de la blessure
 - S1** blessure légère (normalement réversible)
 - S2** blessure grave (normalement irréversible ou mort)
- F** Fréquence et/ou durée de l'exposition au danger
 - F1** de rare à assez fréquente et/ou de courte durée
 - F2** de fréquente à continue et/ou de longue durée
- P** Possibilité d'éviter le phénomène dangereux ou de limiter le dommage
 - P1** possible sous certaines conditions
 - P2** quasiment impossible

Note: Il peut être intéressant pour un constructeur de machines ne devoir pas répéter l'analyse des risques de la machine, mais chercher à réutiliser ce qui a déjà été fait avec l'analyse des risques de la norme EN 954-1. Cela en général n'est pas possible parce que la nouvelle norme a changé le graphique du risque (voir figure A.1), et donc avec le même risque peuvent être modifiés les niveaux de fonction de sécurité requise. L'institution allemande BGIA dans le rapport 2008 / 2 sur la norme EN ISO 13849 suggère que, en adoptant une approche de type «worst case », on peut adopter une conversion comme dans le tableau ci-dessous. Pour d'ultérieures informations se référer au texte en question.

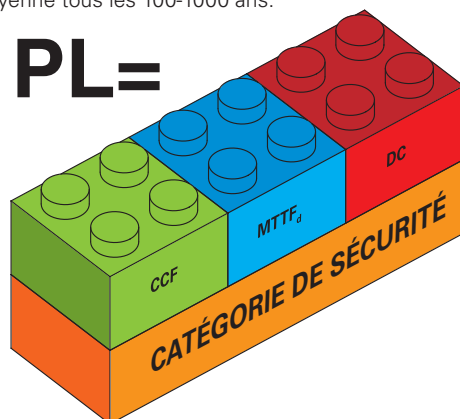
| Catégorie requise par l'EN 954-1:1996 | Performance Level requis (PL _r) et Catégorie requise selon EN ISO 13849-1:2006 |
|---------------------------------------|--|
| B | → b |
| 1 | → c |
| 2 | → d, Catégorie 2 |
| 3 | → d, Catégorie 3 |
| 4 | → e, Catégorie 4 |

Les PL sont classés en cinq niveaux, de PL_a à PL_e en fonction de l'augmentation du risque et chacun d'eux identifie un domaine numérique de probabilité moyenne de défaillance dangereuse par heure. Par exemple PL_d indique que la probabilité moyenne de défaillance dangereuse par heure est comprise entre 1x10⁻⁶ et 1x10⁻⁷ c'est-à-dire environ 1 défaillance dangereuse en moyenne tous les 100-1000 ans.

| PL | Probabilité moyenne de défaillances dangereuses par heure PFHd (1/h) |
|----|--|
| a | 10 ⁻⁵ et < 10 ⁻⁴ |
| b | 3 x 10 ⁻⁶ et < 10 ⁻⁵ |
| c | 10 ⁻⁶ et < 3 x 10 ⁻⁶ |
| d | 10 ⁻⁷ et < 10 ⁻⁶ |
| e | 10 ⁻⁸ et < 10 ⁻⁷ |

Pour l'évaluation du PL d'un système de contrôle sont nécessaires plusieurs paramètres:

1. La Catégorie de sécurité du système qui à son tour découle de l'architecture (structure) du système de contrôle et de son comportement en cas de défaillance
2. MTTF_d des composants
3. DC ou Couverture du diagnostic du système
4. CCF ou Défaillance de cause commune du système.





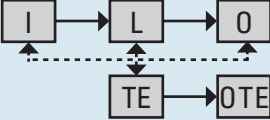
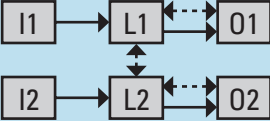
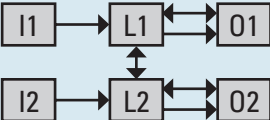
Catégorie de Sécurité.

La grande majorité des circuits de contrôle normalement utilisés sont représentables par une structure de blocs logiques de type:

- Input ou entrée des signaux
- Logic ou logique de traitement des signaux
- Output ou sortie du signal de contrôle

diversement interconnectés les uns aux autres en fonction de la structure du circuit de contrôle.

L'EN ISO 13849 admet cinq différentes structures de circuit de base en les définissant Architecture Désignées du système. Les architectures combinées avec les exigences de comportement en cas de défaillance du système et avec des valeurs minimales des $MTTF_{cr}$, DC et CCF indiquent la Catégorie de Sécurité du système de contrôle, comme indiqué dans le tableau ci-dessous. Donc les Catégories de Sécurité de l'EN ISO 13849-1 ne sont pas équivalentes, mais étendent le concept de Catégorie de Sécurité introduit dans la précédente 954-1.

| Catégorie | Résumé des exigences | Comportement du système | Principes pour la sécurité | $MTTF_{cr}$ de chaque canal | DC _{avg} | CCF |
|-----------|---|--|---|-----------------------------|---|-----------------|
| B | Les parties des systèmes de commande relatives à la sécurité et/ou leurs dispositifs de sécurité et leurs composants doivent être conçus, sélectionnés, composés et combinés conformément aux normes applicables, de sorte qu'ils puissent résister aux influences prévisibles. Il faut utiliser les principes base de sécurité. Architecture:  | Une défaillance peut entraîner la perte de la fonction de sécurité. | Essentiellement caractérisé par le choix des composants | Faible ou Moyenne | Nulle | Pas relevant |
| 1 | Les exigences de la catégorie B doivent être remplies. Nécessité d'appliquer des composants éprouvés et des principes de sécurité fiables. Architecture:  | Une défaillance peut entraîner la perte de la fonction de sécurité, mais la probabilité d'occurrence d'une telle défaillance est plus petite qu'en catégorie B. | Essentiellement caractérisé par le choix des composants | Élevée | Nulle | Pas relevant |
| 2 | Les exigences de la catégorie B et l'utilisation des principes de sécurité fiables doivent être remplies. La fonction de sécurité doit être vérifiée régulièrement par le système de contrôle.  Architecture: | Une défaillance peut entraîner la perte de la fonction de sécurité entre les contrôles. La perte de la fonction de sécurité est détectée par le système de contrôle. | Essentiellement caractérisé par la structure | De Faible à Élevée | De Faible à Moyenne | Voir l'annexe F |
| 3 | Les exigences de la catégorie B et l'utilisation des principes de sécurité fiables doivent être remplies. Les parties relatives à la sécurité sont conçues de manière à ce que : - une défaillance unique dans une de ses parties n'entraîne pas la perte de la fonction de sécurité, et - la défaillance unique soit détectée si raisonnablement possible.  Architecture: | La fonction de sécurité est toujours maintenue en cas d'une défaillance unique. Quelques défaillances sont détectées mais pas toutes. Une accumulation de défaillances non-détectées peut entraîner la perte de la fonction de sécurité. | Essentiellement caractérisé par la structure | De Faible à Élevée | De Faible à Moyenne | Voir l'annexe F |
| 4 | Les exigences de la catégorie B et l'utilisation des principes de sécurité fiables doivent être remplies. Les parties relatives à la sécurité sont conçues de manière à ce que : - une défaillance unique dans une de ses parties n'entraîne pas la perte de la fonction de sécurité, et - la défaillance unique soit détectée avant ou pendant la sollicitation suivante de la fonction de sécurité. Si ceci n'est pas possible, une accumulation de défaillances n'entraîne pas la perte de la fonction de sécurité  Architecture: | La fonction de sécurité est toujours maintenue en cas d'une défaillance unique. La détection de défaillances accumulées réduit la probabilité de la perte de la fonction de sécurité (DC élevée). Les défaillances sont détectées à temps pour éviter la perte de la fonction de sécurité. | Essentiellement caractérisé par la structure | Élevée | Élevée (Incluse l'accumulation de défaillances) | Voir l'annexe F |

MTTF_d ("Mean Time To Dangerous Failure", Temps moyen avant défaillance dangereuse).

Ce paramètre essaie de définir la bonne qualité des composants du système en définissant la durée de vie moyenne avant la défaillance dangereuse (noter qu'il ne s'agit pas de défaillance générale) exprimée en années. En pratique le calcul de l'MTTF_d se base sur des valeurs numériques fournies par les constructeurs de chaque composant formant le système. En cas d'absence de données, la norme fournit des valeurs dans tableaux de référence spéciaux. (Annexe C de EN ISO 13849-1). Le comptage portera à une valeur numérique qui rentrera dans trois catégories : élevée, moyenne ou faible.

| Classification | Valeurs |
|----------------|--------------------------------------|
| Non permis | MTTF _d < 3 ans |
| Faible | 3 ans MTTF _d < 10 ans |
| Moyen | 10 ans MTTF _d < 30 ans |
| Élevé | 30 ans MTTF _d 100 ans |

Dans le cas de composants sensibles à l'usure (typiquement dispositifs mécaniques ou hydrauliques), le constructeur du composant fournira, plutôt que le MTTF_d du composant, la valeur B10d du composant c'est-à-dire le nombre de cycles du composant dans lequel 10% des prototypes testés présentent une défaillance dangereuse.

La valeur B10d doit être convertie par le constructeur de la machine en MTTF_d par la formule:

$$MTTF_d = \frac{B_{10d}}{0,1 \cdot n_{op}}$$

Où n_{op} = nombre moyen de manœuvres par an du composant.

En supposant la fréquence d'utilisation quotidienne et le nombre d'heures de service par jour de la machine, le n_{op} peut être obtenu de:

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600s/h}{t_{ciclo}}$$

Où

d_{op} = nombre moyen de jours de service par an

h_{op} = nombre moyen d'heures de service par jour

t_{ciclo} = temps cycle (s)

On peut noter donc que le paramètre MTTF_d, quand il est obtenu à partir d'un composant sujet à l'usure, ne dépend pas seulement du composant même, mais aussi de l'application. Un dispositif mécanique avec basse fréquence d'utilisation, tel qu'un télérupteur utilisé seulement pour les arrêts d'urgence, aura généralement un MTTF_d élevé; mais si le même dispositif est également utilisé pour les normales manœuvres de cycle, alors le MTTF_d du même télérupteur, avec un temps de cycle bas, pourrait diminuer drastiquement.

Pour le calcul de l'MTTF_d du circuit de contrôle contribuent tous les éléments du circuit, en fonction de sa structure. Dans les circuits avec une architecture à 1 canal (comme dans les cas des B, 1 et 2) la contribution de chaque composants est linéaire et le calcul du MTTF_d du canal est obtenu de:

$$\frac{1}{MTTF_d} = \sum_{i=1}^N \frac{1}{MTTF_{di}}$$

Pour éviter des interprétations trop optimistes la valeur maximale de MTTF_d de chaque canal est limitée à 100 ans. Ne sont pas permis canaux avec un MTTF_d inférieur à 3 ans.

Dans le cas des systèmes à 2 canaux (catégories 3 et 4) le calcul du MTTF_d du circuit est obtenu par la symétrisation des MTTF_d des deux canaux en utilisant la formule:

$$MTTF_d = \frac{2}{3} \left[MTTF_{dc1} + MTTF_{dc2} - \frac{1}{\frac{1}{MTTF_{dc1}} + \frac{1}{MTTF_{dc2}}} \right]$$

DC ("Diagnostic Coverage", couverture du diagnostic).

Ce paramètre essaie d'indiquer à quel point le système est en mesure d' "auto-surveiller" un éventuel mauvais fonctionnement. En fonction du pourcentage de défaillances dangereuses détectables par le système, on aura une couverture du diagnostic plus ou moins bonne.

Le paramètre numérique DC est une valeur en pourcent qui est calculée à travers des valeurs données dans un tableau (annexe E de l'EN ISO 13849-1) en fonction des précautions adoptées par le fabricant pour détecter les anomalies de son circuit. Comme en général ils existent plusieurs précautions dans le même circuit pour détecter anomalies différentes, à la fin on calcule une valeur moyenne ou DC_{avg} qui sera répartie dans les quatre groupes suivants:

Élevée DC_{avg} 99%

Moyenne 90% DC_{avg} <99%

Faible 60% DC_{avg} <90%

Nulle 60% < DC_{avg}

La couverture du diagnostic nulle est admise seulement pour les systèmes avec architecture B ou 1.

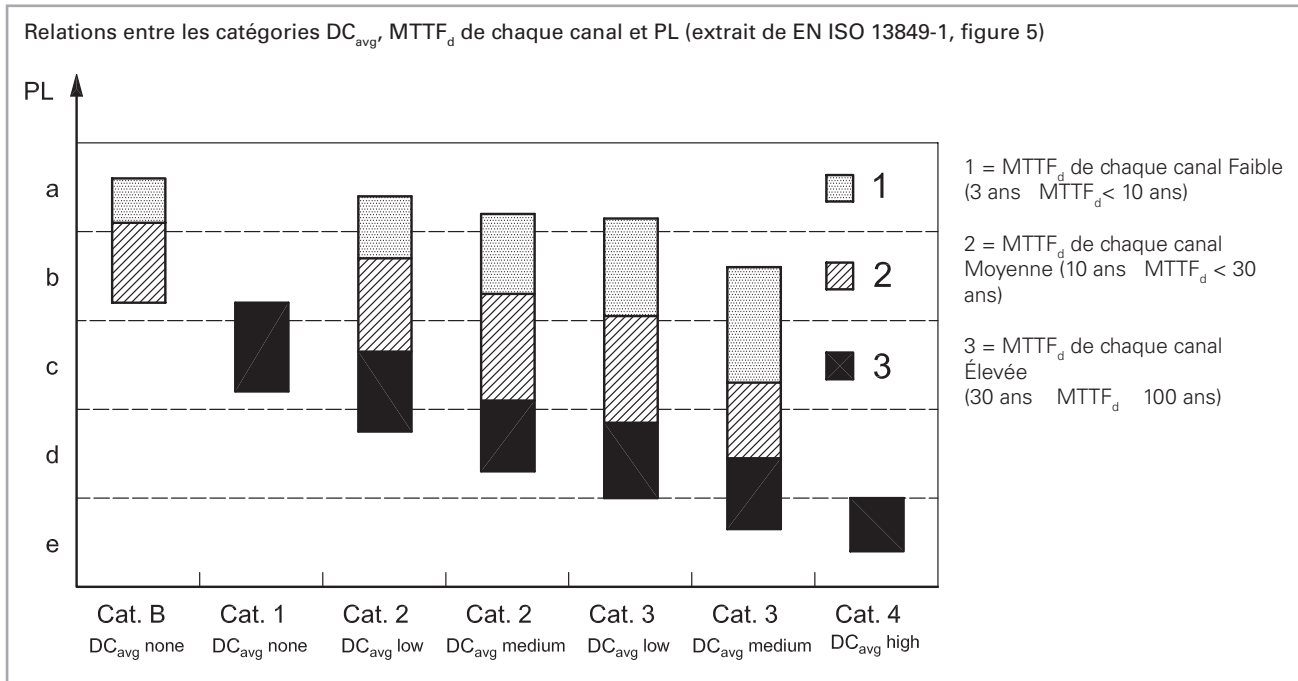
CCF ("Common Cause Failure", Défaillance de cause commune)

Dans le cas de systèmes de catégorie 2,3 ou 4 pour le calcul du PL il sera nécessaire aussi d'évaluer une éventuelle défaillance de cause commune ou CCF qui peut invalider la redondance des systèmes. L'évaluation se fait par une check-list de contrôle (annexe F de l'EN ISO 13849-1), qui, selon le type de solutions adoptées contre les défaillances de cause commune, donne une valeur de 0 à 100. La valeur minimale permise pour les catégories 2, 3 et 4 est de 65 points.

1
1A
1B
2
2A
2B
2C
2D
2E
3
3A
3B
3C
4
4A
4B
4C
4D
4E
4F
4G
4H
5
6

PL ("Performance Level")

Étant connus ces paramètres, la norme EN ISO 13849-1 fournit le PL du système au moyen d'un tableau de corrélation (annexe K de l'EN ISO 13849-1), ou, sous forme graphique simplifiée (paragraphe 4.5 de l'EN ISO 13849-1), par la figure suivante.



Cette image est très utile parce qu'on a plusieurs modalités de lecture. Étant donné une certaine valeur PL_r , l'image met en évidence toutes les solutions possibles qui offrent ce niveau de PL c'est-à-dire les structures de circuit possibles qui offrent le même PL.

Par exemple en observant la figure, on peut noter comme pour obtenir un système avec PL égal à « c », toutes les solutions suivantes sont possibles:

1. Système de catégorie 3 avec composants peu fiables ($MTTF_d$ =faible) et DC moyenne
2. Système de catégorie 3 avec composants fiables ($MTTF_d$ =moyenne) e DC faible.
3. Système de catégorie 2 avec composants fiables ($MTTF_d$ =moyenne) e moyenne.
4. Système de catégorie 2 avec composants fiables ($MTTF_d$ =moyenne) e DC faible.
5. Système de catégorie 1 avec composants très fiables ($MTTF_d$ =élevée).

En même temps la figure, choisi une structure de circuit, permet de voir immédiatement les maximum PL réalisables en fonction de la couverture du diagnostic moyenne et du $MTTF_d$ des composants. Le constructeur peut donc exclure a priori certaines structures de circuit car inappropriées au PL_r requis.

Cependant en général, pour d'identifier le PL du système, on ne se réfère pas à la figure en question puisque dans de nombreux cas, les zones du graphique se superposent aux lignes de la marge des différentes PL.

Au lieu de cela, on utilise le tableau dans l'annexe K de l'EN ISO 13849-1 pour une détermination précise du PL du circuit.

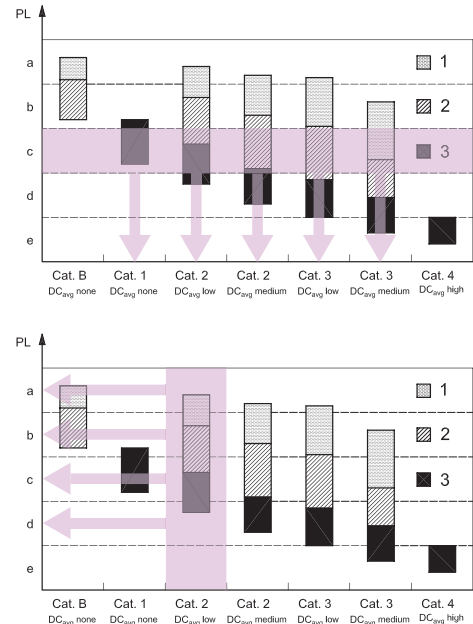


Tableau Paramètres de sécurité (2009)

Les données B10 et B10d indiqués dans le tableau se réfèrent à la durée mécanique des contacts sûres (NC a à ouverture positive) des dispositifs en conditions environnementales normales.

| Série | Description article | B10 | B10 _d | B10/ B10 _d |
|---|--|------------|------------------|--------------------------|
| F ••••• F •••93 F •••92 F •••99 F •••R2 | Interrupteurs de position | 20.000.000 | 40.000.000 | 50% |
| FS, FG F •••96 F •••95 | Interrupteurs de sécurité à actionneur séparé | 1.000.000 | 2.000.000 | 50% |
| F •••C• | Interrupteurs de sécurité à actionneur séparé avec verrouillage | 1.000.000 | 5.000.000 | 20% |
| F ••••• | Interrupteurs de sécurité pivotant pour charnières | 1.000.000 | 5.000.000 | 20% |
| HP | Interrupteurs à levier à fente pour protections battantes | 1.000.000 | 2.000.000 | 50% |
| SR | Interrupteurs à câble pour arrêt d'urgence | 1.000.000 | 2.000.000 | 50% |
| SR | Charnières de sécurité | 1.000.000 | 5.000.000 | 20% |
| SR | Capteurs magnétiques de sécurité (utilisés avec modules de sécurité Pizzato) | 10.000.000 | 20.000.000 | 50% |
| SR | Capteurs magnétiques de sécurité (utilisés à max charge: 24V 250mA) | 5.000.000 | 10.000.000 | 50% |
| CC | Bouton d'urgence | | 100.000 | |
| PX, PA | Interrupteurs à pédale | 20.000.000 | 40.000.000 | 50% |
| MK | Micro-interrupteurs de position | 10.000.000 | 20.000.000 | 50% |

| Code | Description article | MTTF _d | DC | PFHd | SIL CL | PL | Cat |
|----------|--|-------------------|----|----------|--------|----|-----|
| CS AM-01 | Module de sécurité pour détection d'arrêt moteur | 145 | M | 1.94E-09 | 2 | d | 3 |
| CS AR-01 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 147 | H | 6.38E-10 | 3 | e | 4 |
| CS AR-02 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 147 | H | 6.38E-10 | 3 | e | 4 |
| CS AR-04 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 147 | H | 6.38E-10 | 3 | e | 4 |
| CS AR-05 | Module de sécurité pour contrôle protecteurs, arrêts d'urgence et barrières optiques | 147 | H | 6.61E-10 | 3 | e | 4 |
| CS AR-06 | Module de sécurité pour contrôle protecteurs, arrêts d'urgence et barrières optiques | 147 | H | 6.61E-10 | 3 | e | 4 |
| CS AR-07 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 111 | H | 7.56E-10 | 3 | e | 4 |
| CS AR-08 | Module de sécurité pour contrôle protecteurs, arrêts d'urgence et barrières optiques | 218 | H | 4.58E-09 | 3 | e | 4 |
| CS AR-20 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 358 | M | 8.71E-09 | 3 | e | 3 |
| CS AR-21 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 358 | M | 8.71E-09 | 3 | e | 3 |
| CS AR-22 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 201 | H | 8.87E-09 | 3 | e | 3 |
| CS AR-23 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 201 | H | 8.87E-09 | 3 | e | 3 |
| CS AR-24 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 111 | H | 1.18E-09 | 3 | e | 3 |
| CS AR-25 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 111 | H | 1.18E-09 | 3 | e | 3 |
| CS AR-40 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 356 | M | 1.08E-08 | 2 | d | 2 |
| CS AR-41 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 356 | M | 1.08E-08 | 2 | d | 2 |
| CS AR-46 | Module de sécurité pour contrôle protecteurs et arrêts d'urgence | 435 | | 3.32E-08 | 1 | c | 1 |
| CS AR-51 | Module de sécurité pour contrôle tapis et bords sensibles | 209 | H | 9.43E-09 | 3 | e | 4 |
| CS AR-90 | Module de sécurité pour contrôle de zone d'iso-nivelage des ascenseurs | 382 | H | 5.03E-10 | 3 | e | 4 |
| CS AR-94 | Module de sécurité pour contrôle de zone d'iso-nivelage des ascenseurs | 213 | H | 5.62E-09 | 3 | e | 4 |
| CS AT-0x | Module de sécurité temporisateur pour contrôle protecteurs et arrêts d'urgence | 84 | H | 9.01E-09 | 3 | e | 4 |
| CS AT-1x | Module de sécurité temporisateur pour contrôle protecteurs et arrêts d'urgence | 84 | H | 9.01E-09 | 3 | e | 4 |
| CS AT-2x | Module de sécurité temporisateurs pour contrôle protecteurs et arrêts d'urgence | 74 | H | 4,05E-09 | 3 | e | 4 |
| CS DM-01 | Module de sécurité pour contrôle commande bimanuelle | 142 | H | 2.99E-08 | 3 | e | 4 |
| CS FS-0 | Module temporisateur de sécurité | 146 | H | 1.62E-09 | 3 | e | 4 |
| CS FS-20 | Module temporisateur de sécurité | 205 | M | 1.10E-08 | 2 | d | 3 |
| CS FS-30 | Module temporisateur de sécurité | 205 | M | 1.10E-08 | 2 | d | 3 |
| CS FS-50 | Module temporisateur de sécurité | 349 | M | 1.17E-08 | 2 | d | 3 |
| CS ME-01 | Module d'extensions contacts | 76 | H | 6.38E-10 | 3 | e | 4 |
| CS ME-20 | Module d'extensions contacts | 113 | H | 3.07E-09 | 3 | e | 4 |
| CS ME-30 | Module d'extensions contacts | 112 | H | 2.77E-09 | 3 | e | 4 |
| CS ME-31 | Module d'extensions contacts | 112 | H | 2.77E-09 | 3 | e | 4 |

B10d: Nombre d'opérations dans lequel 10% des composants présentent une défaillance dangereuse

B10: Nombre d'opérations dans lequel 10% des composants présentent une défaillance

B10/B10_d: rapport entre défaillances dangereuses et défaillances totales

MTTF_d: Mean Time To Failure Dangerous (Temps moyen avant défaillance dangereuse)

DC: Diagnostic coverage (Couverture du diagnostic)

PFHd: Probability of Dangerous Failure per hour (Probabilité de défaillance dangereuse par heure)

SIL CL: Safety Integrity Level Claim Limit. (Max SIL selon EN 62061)

PL: Performance Level (PL selon EN ISO 13849-1)

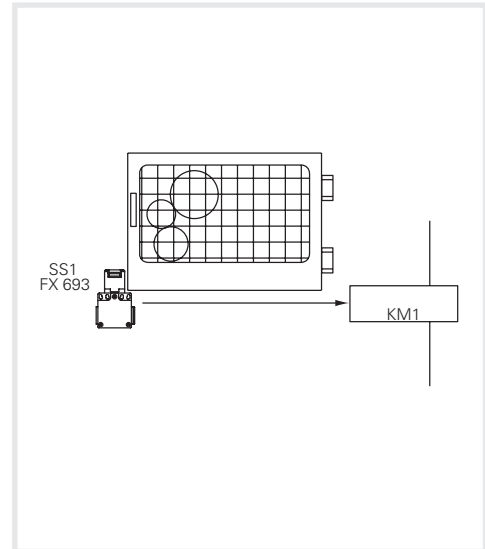
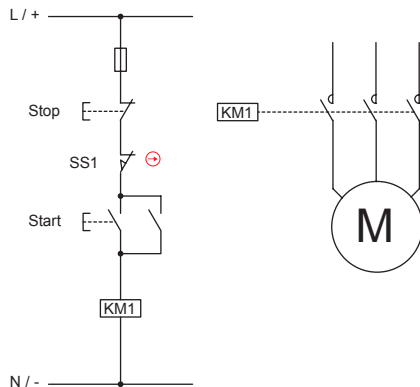
EXEMPLE 1**Application: Contrôle protections**

Norme de référence EN ISO 13849-1:2006

Catégorie de sécurité

1

Performance Level

PL c

Le circuit de contrôle de la figure a la fonction de surveillance de la protection. Si la protection est ouverte le moteur ne doit pas être en mesure de démarrer. L'analyse des dangers a souligné que le système n'est pas doté d'inertie c'est-à-dire que le moteur, après avoir coupé l'alimentation, il s'arrête plus rapidement que l'ouverture de la protection. De l'analyse des risques on a mis en évidence que le PL_r target requis est PLc. On veut vérifier si le circuit de contrôle supposé, qui a une structure avec 1 canal, a un PL_r supérieur ou égal à PL_r .

Description de la fonction de sécurité

La position de la protection est détectée par l'interrupteur avec actionneur séparé SS1 qui agit directement sur le contacteur KM1. Le contacteur KM1 qui vérifie les organes en mouvement est normalement activé par les boutons de Start et Stop, mais l'analyse du cycle de fonctionnement a montré que même la protection est ouverte à chaque cycle de service. Il s'ensuit que le nombre d'opérations du télérupreur et de l'interrupteur de sécurité peut être considéré comme égal.

La structure du circuit est du type à 1 canal sans supervision (catégorie B ou 1) où il y a seulement le composant de Input (interrupteur) et Output (contacteur).

La fonction de sécurité n'est pas maintenue en cas de défaillance sur un des dispositifs.

Ne sont pas mis en œuvre des mesures pour vérifier les défaillances.

Données des dispositifs

- SS1 (FX 693) est un interrupteur à ouverture positive (selon l'annexe K de l'EN 60947-5-1). L'interrupteur est un dispositif bien éprouvé selon le tableau D.4 de l'EN ISO 13849-2. La valeur du $B10_d$ du dispositif est fournie par le constructeur (voir page 6/32) et est égale à 2000000 manœuvres.
- KM1 est un contacteur utilisé à charge nominale et est un composant bien éprouvé, selon le tableau D.4 de l'EN ISO 13849-2. Sa valeur $B10_d$ est égale à 2000000 manœuvres, étant dérivée cette valeur des tableaux de la norme (voir tableau C.1 de l'EN ISO 13849-1).

Hypothèse de fréquence d'utilisation

- Il est supposé que la machine est utilisée pour un maximum de 365 jours par an, pour trois services de travail de 8 heures avec un temps cycle de 600 secondes. Le nombre d'opérations par an, pour le contacteur et pour l'interrupteur, est donc égal au maximum à $n_{op} = (365 \times 24 \times 3.600) / 600 = 52560$.
- On suppose l'actionnement du bouton de start tous les 300 secondes. Le nombre d'opérations annuelles est donc égal au maximum à $n_{op}/an = 105120$
- Le contacteur KM1 sera actionné pour le normal start-stop de la machine, et pour le redémarrage suite à l'ouverture d'un protecteur. $n_{op}/an = 52560 + 105120 = 157680$

Calcul $MTTF_d$

L' $MTTF_d$ de l'interrupteur SS1 est égal à : $MTTF_d = B10_d / (0,1 \times n_{op}) = 2000000 / (0,1 \times 52560) = 381$ ans

L' $MTTF_d$ de contacteur KM1 est égal à : $MTTF_d = B10_d / (0,1 \times n_{op}) = 2000000 / (0,1 \times 157680) = 127$ ans

Il s'ensuit que le $MTTF_d$ du circuit à 1 canal est égal à : $1 / (1/381 + 1/127) = 95$ ans

Couverture du diagnostic DC_{avg}

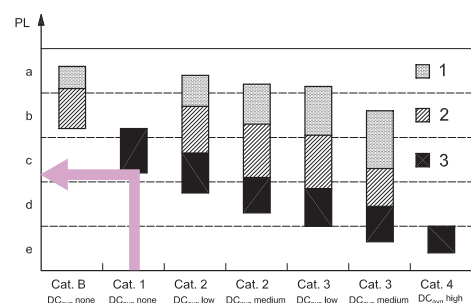
Ne sont pas mis en œuvre des mesures pour vérifier les défaillances et donc la couverture du diagnostic est Nulle, condition admise pour le circuit examiné qui est en catégorie 1.

Défaillance de cause commune CCF

Pour un circuit en catégorie 1 il n'est pas nécessaire le calcul du paramètre CCF.

Vérification du PL

De la table ou de la figure 5 de la norme on vérifie comme pour un circuit en catégorie 1 avec $MTTF_d = 95$ ans, le PL_r résultant du circuit de contrôle est égal à c. Le PL_r objectif est donc atteint.

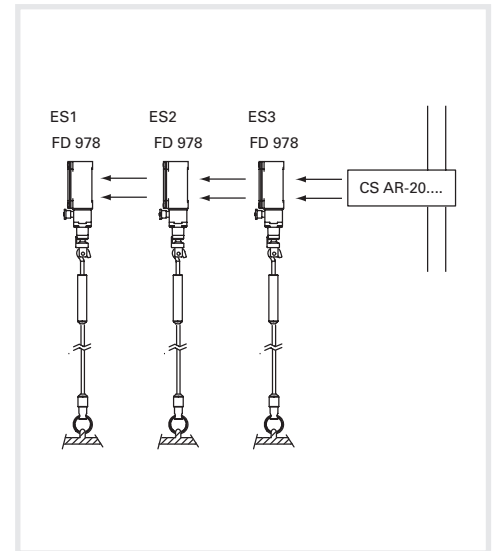
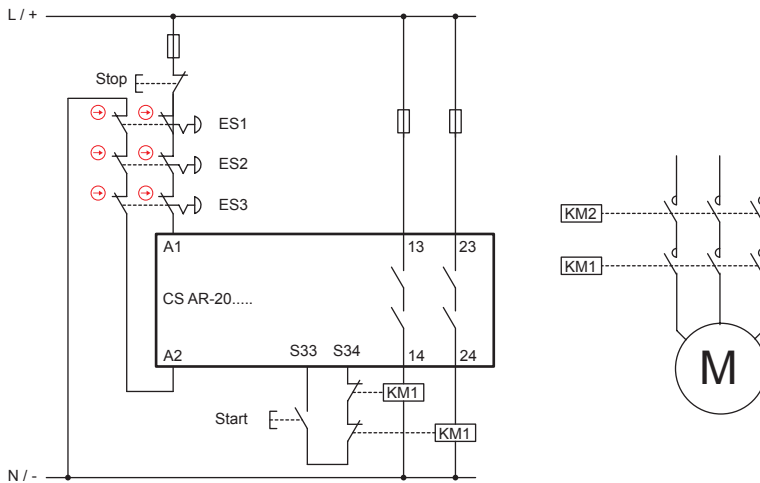


EXEMPLE 2

Application: Contrôle arrêts d'urgence

Norme de référence EN ISO 13849-1:2006

Catégorie de sécurité **3**
Performance Level **PL e**



Description de la fonction de sécurité

Le fonctionnement d'un des dispositifs d'urgence provoque l'intervention du module de sécurité et de deux contacteurs KM1 et KM2. Le signal des dispositifs ES1, ES2, ES3 est lu par le module de sécurité CS de façon redondante. Aussi les contacteurs KM1 et KM2 (avec contacts guidés) sont contrôlés par le CS à travers le circuit de rétroaction.

Données des dispositifs

- ES1, ES2, ES3 (FD 978) sont interrupteurs à câble pour arrêts d'urgence à ouverture positive. La valeur du $B10_d$ est égale à 2000000 (Voir page 6/32)
- KM1, KM2 sont contacteurs utilisés à charge nominale. La valeur du $B10_d$ est égale à 2000000 (voir tableau C.1 de l'EN ISO 13849-1)
- CS est un module de sécurité (CS AR-20) avec $MTTF_d=358$ ans (voir page 6/32) et DC= Moyenne
- L'architecture du circuit est à double canal en catégorie 3

Hypothèse de fréquence d'utilisation

- 2 fois par mois $n_{op}/an = 24$
- Actionnement du bouton de démarrage: 4 fois par jour
- En supposant 365 jours de travail, les contacteurs interviennent $4 \times 365 + 24 = 1484$ fois/an
- Les interrupteurs seront actionnés avec la même fréquence
- On ne prévoit pas que plusieurs boutons peuvent être pressés simultanément

Calcul $MTTF_d$

- $MTTF_d$ ES1, ES2, ES3 = 833333 ans
- $MTTF_d$ KM1, KM2 = 13477 ans
- $MTTF_d$ CS = 358 ans
- $MTTF_d$ CH1 = 349 ans. La valeur est limitée à 100 ans. Les canaux sont symétriques, donc $MTTF_d=100$ ans (élevée)

Couverture du diagnostic DC_{avg}

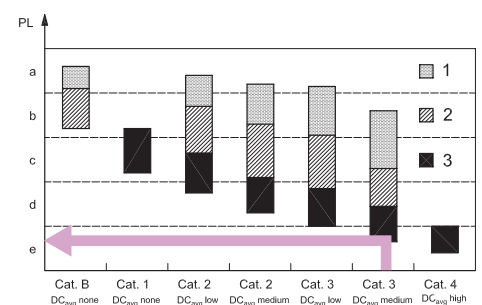
- Les contacts KM1 et KM2 sont contrôlés par le CS à travers le circuit de rétroaction. DC=99% (élevée)
- Le module de sécurité CS AR-20 a une couverture du diagnostic Moyenne.
- Il n'est pas possible de détecter toutes les défaillances dans la série des dispositifs d'urgence. La couverture diagnostique est de 90% (Moyenne)

Défaillance de cause commune CCF

On suppose une valeur > 65 (selon l'annexe F de l'EN ISO 13849-1).

Vérification du PL

Un circuit en catégorie 3 avec $MTTF_d=100$ ans et DC_{avg} = Moyenne peut atteindre un PL e.



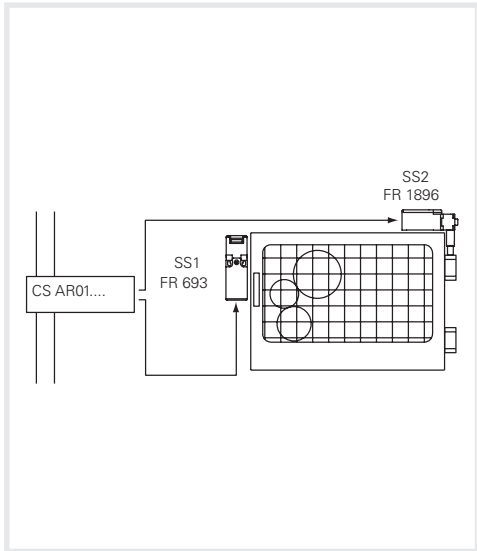
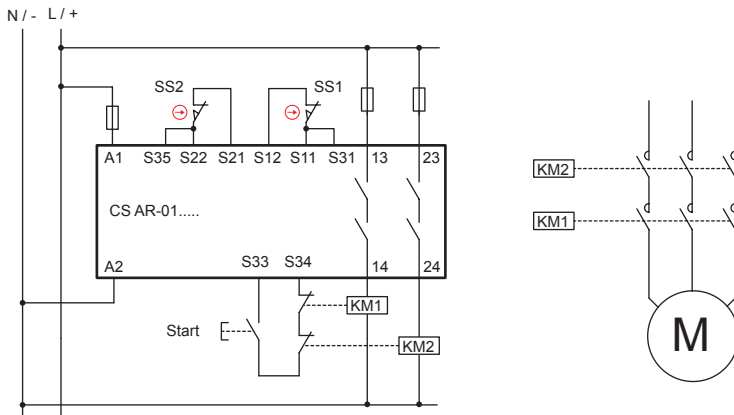
EXEMPLE 3**Application: Contrôle protections**

Norme de référence EN ISO 13849-1:2006

Catégorie de sécurité

4

Performance Level

PL e**Description de la fonction de sécurité**

L'ouverture de la protection provoque l'intervention des interrupteurs SS1 et SS2 et donc du module de sécurité et de deux contacteurs KM1 et KM2.

Le signal des dispositifs SS1, SS2 est contrôlé de façon redondante par le module de sécurité CS.

Les interrupteurs ont un principe de fonctionnement différent.

Aussi les contacteurs KM1 et KM2 (avec contacts guidés) sont contrôlés par le CS à travers le circuit de rétroaction.

Données des dispositifs

- SS1 (FR 693) est un interrupteur à ouverture positive. La valeur du $B10_d$ est égale à 2000000 (voir page 6/32)
- SS2 (FR 1896) est un interrupteur pour charnières à ouverture positive. $B10_d = 5000000$ (voir page 6/32)
- KM1, KM2 sont contacteurs utilisés à charge nominale. $B10_d = 2000000$ (voir tableau C.1 de l'EN ISO 13849-1)
- CS sont modules de sécurité (CS AR-01) avec $MTTF_d = 147$ ans et $DC = 99\%$ (Élevée)

Hypothèse de fréquence d'utilisation

365 jj/an, 16 h/jj, 1 intervention chaque 3 minutes (180 s). $n_{op}/an = 116.800$

Calcul MTTFd

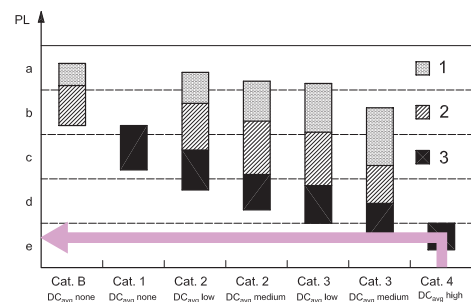
- $MTTF_d$ SS1 = 171 ans
- $MTTF_d$ SS2 = 428 ans
- $MTTF_d$ KM1, KM2 = 171 ans
- $MTTF_d$ CS = 147 ans
- $MTTF_d$ CH1 = 54 ans (SS1, CS, KM1)
- $MTTF_d$ CH2 = 67 ans (SS2, CS, KM2)
- $MTTF_d$: en symétrisant les 2 canaux on obtient $MTTF_d = 61$ ans (élevée)

Couverture du diagnostic DC

- SS1, SS2 ont $DC_{avg} = 99\%$ car les contacts de SS1 et SS2 sont contrôlés par CS et ils ont principes de fonctionnement différents.
- Les contacts de KM1 et KM2 sont contrôlés par CS à travers le circuit de rétroaction. $DC = 99\%$ (élevée)
- CS AR-01 à l'intérieur a un circuit redondant et auto-surveillé. $DC = 99\%$ (élevée)
- $DC_{avg} = 99\%$ (élevée)

Vérification du PL

Un circuit en catégorie 4 avec $MTTF_d = 61$ ans et $DC_{avg} =$ Élevée correspond à un PL e.

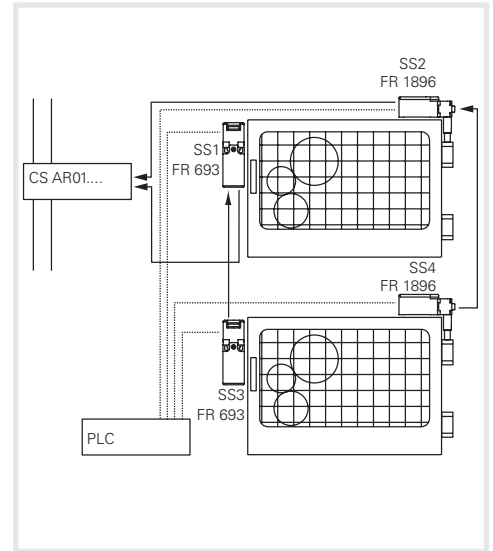
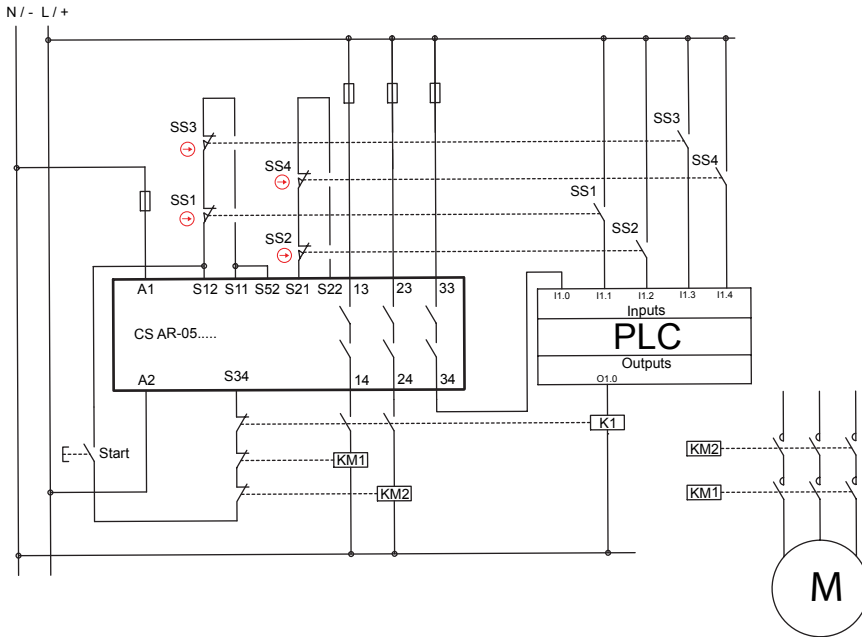


EXEMPLE 4

Application: Contrôle protections

Norme de référence EN ISO 13849-1:2006

Catégorie de sécurité **4**
Performance Level **PL e**



Description de la fonction de sécurité

L'ouverture de la protection provoque l'intervention des interrupteurs SS1, SS2 dans la première protection et SS3, SS4 dans la deuxième protection; les interrupteurs font intervenir le module de sécurité et les deux contacteurs KM1 et KM2.

Le signal des dispositifs SS1, SS2 et SS3, SS4 est contrôlé de façon redondante par le module de sécurité CS, en outre un contact auxiliaire des interrupteurs est contrôlé par le PLC.

Les interrupteurs ont un principe de fonctionnement différent.

Aussi les contacteurs KM1 et KM2 (avec contacts guidés) sont contrôlés par le CS à travers le circuit de rétroaction.

Données des dispositifs

- SS1,SS3 (FR 693) sont des interrupteurs à ouverture positive. La valeur du $B10_d$ est égale à 2000000 (voir page 6/32)
- SS2,SS4 (FR 1896) sont des interrupteurs pour charnières à ouverture positive. $B10_d = 5000000$ (voir page 6/32)
- KM1, KM2 sont des contacteurs utilisés à charge nominale. La valeur du $B10_d = 2000000$ (voir tableau C.1 de l'EN ISO 13849-1)
- CS est un module de sécurité (CS AR-05) avec $MTTF_d = 147$ ans et $DC = 99\%$

Hypothèse de fréquence d'utilisation

- 4 fois par heure pour 24 heures/jj pour 365 jj/an, égal à $n_{op}/an = 35040$
- Les contacteurs interviennent pour un nombre double de opérations = 70080

Calcul MTTFd

- $MTTF_d$ SS1,SS3 = 571 ans; $MTTF_d$ SS2,SS4 = 1427 ans
- $MTTF_d$ KM1,KM2 = 285 ans
- $MTTF_d$ CS = 147 ans
- $MTTF_d$ Ch1 = 72 ans (SS1,SS3,CS,KM1)
- $MTTF_d$ Ch2 = 85 ans (SS2,SS4,CS,KM2)
- $MTTF_d$: en symétrisant les 2 canaux on obtient $MTTF_d = 79$ ans (élevée)

Couverture du diagnostic DC_{avg}

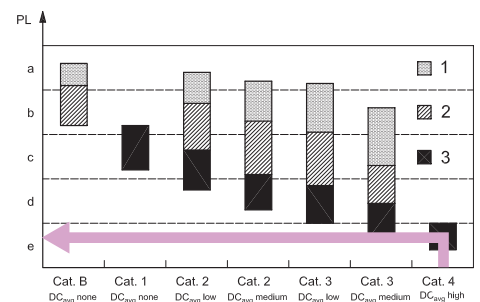
- Les contacts de KM1 et KM2 sont contrôlés par CS à travers le circuit de rétroaction. $DC = 99\%$ (élevée)
- Les contacts auxiliaires des interrupteurs sont tous contrôlés par le PLC. $DC = 99\%$
- Le module CS AR-05 a une $DC = 99\%$ (voir page 6/32)
- La couverture du diagnostic pour tous les deux canaux est de 99% (élevée)

Défaillance de cause commune CCF

- On suppose une valeur > 65 (selon l'annexe F de l'EN ISO 13849-1).

Vérification du PL

- Un circuit en catégorie 4 avec $MTTF_d = 79$ ans (élevée) et $DC_{avg} =$ Elevée correspond à un PL e.



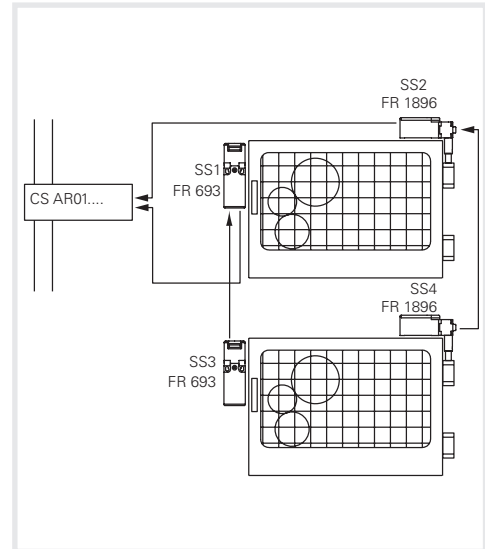
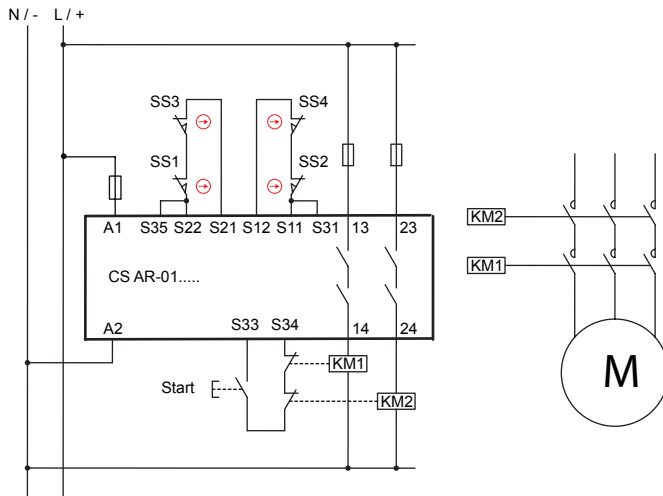
EXEMPLE 5**Application: Contrôle protections**

Norme de référence EN ISO 13849-1:2006

Catégorie de sécurité

3

Performance Level

PL e**Description de la fonction de sécurité**

L'ouverture de la protection provoque l'intervention des interrupteurs SS1, SS2 dans la première protection et SS3, SS4 dans la deuxième protection; les interrupteurs font intervenir le module de sécurité et les deux contacteurs KM1 et KM2.

Le signal des dispositifs SS1, SS2 et SS3, SS4 est contrôlé de façon redondante par le module de sécurité CS.

Les interrupteurs ont un principe de fonctionnement différent.

Aussi les contacteurs KM1 et KM2 (avec contacts guidés) sont contrôlés par le CS à travers le circuit de rétroaction.

Données des dispositifs

- SS1, SS3 (FR 693) sont des interrupteurs à ouverture positive. La valeur du $B10_d$ est égale à 2000000 (voir page 6/32)
- SS2, SS4 (FR 1896) sont des interrupteurs pour charnières à ouverture positive. $B10_d = 5000000$ (voir page 6/32)
- KM1, KM2 sont des contacteurs utilisés à charge nominale. La valeur du $B10_d$ est égale à 2000000 (voir tableau C.1 de l'EN ISO 13849-1)
- CS est un module de sécurité (CS AR-01) avec $MTTF_d = 147$ ans et $DC = 99\%$

Hypothèse de fréquence d'utilisation

- 2 fois par heure pour 16 heures/jj pour 365 jj/an, égal à $n_{op}/an = 11680$
- Les contacteurs interviennent pour un nombre double d'opérations = 23360

Calcul $MTTF_d$

- $MTTF_d$ SS1, SS3 = 1712 ans
- $MTTF_d$ SS2, SS4 = 4281 ans
- $MTTF_d$ KM1, KM2 = 856 ans
- $MTTF_d$ CS = 147 ans
- $MTTF_d$ CH1 = 109 ans (SS1, SS3, CS, KM1)
- $MTTF_d$ CH2 = 118 ans (SS2, SS4, CS, KM2)
- $MTTF_d$ = valeur limitée à 100 ans

Couverture du diagnostic DC_{avg}

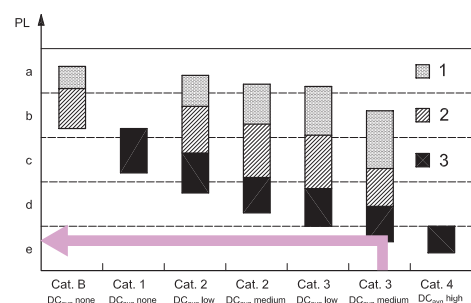
- Les contacts de KM1, KM2 sont contrôlés par CS à travers le circuit de rétroaction. $DC = 99\%$
- Il n'est pas possible de détecter toutes les défaillances dans la série des interrupteurs. $DC = 60\%$
- Le module CS AR-01 a une $DC = 99\%$
- On suppose une couverture du diagnostic de 92% (Moyenne)

Défaillance de cause commune CCF

- On suppose une valeur > 65 (selon l'annexe F de l'EN ISO 13849-1).

Vérification du PL

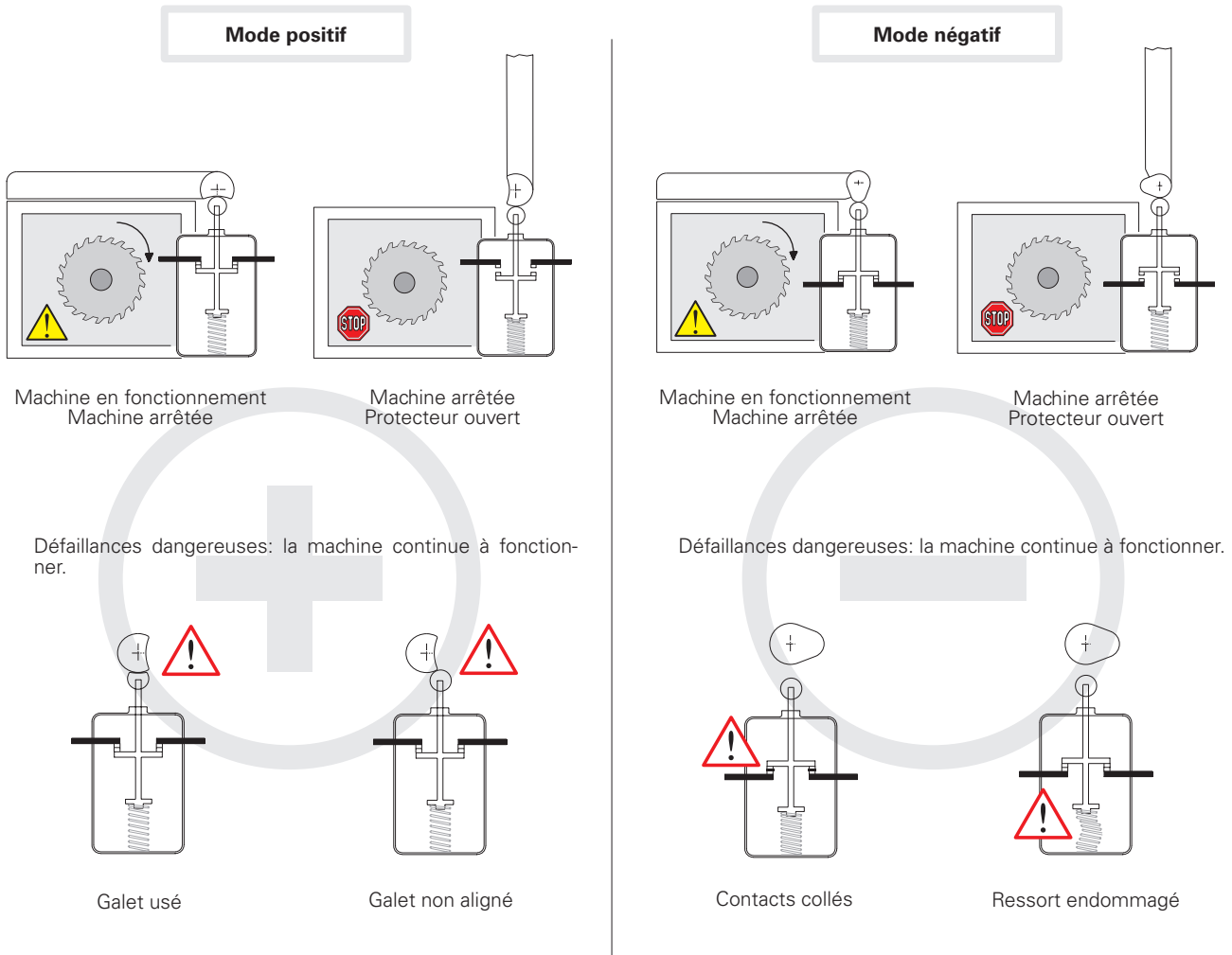
- Un circuit en catégorie 3 avec $MTTF_d = 100$ ans et $DC_{avg} =$ moyenne correspond à un PL e.



6 - Ouverture positive, redondance, diversification et autocontrôle

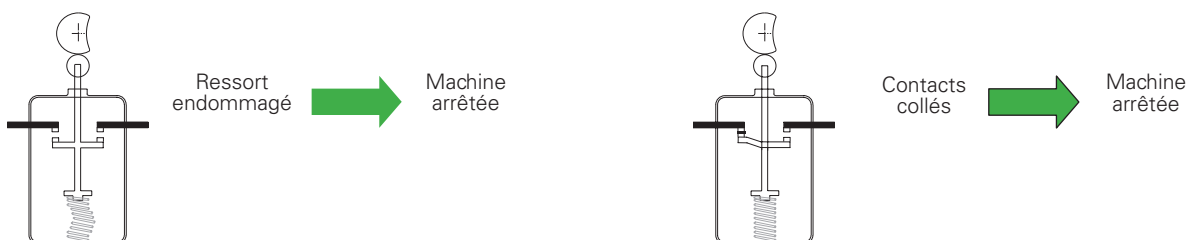
Mode positif et mode négatif

Selon la norme EN 292-2 point 3.5, si un composant mécanique en mouvement entraîne inévitablement un autre composant, par contact direct ou au moyen d'éléments rigides, on dit que ces éléments sont raccordés en **mode positif**. Quand au contraire le déplacement d'un élément mécanique permet à un deuxième élément de se déplacer librement (par exemple gravité, effet d'un ressort, etc.), le raccordement entre les deux est en **mode négatif**.




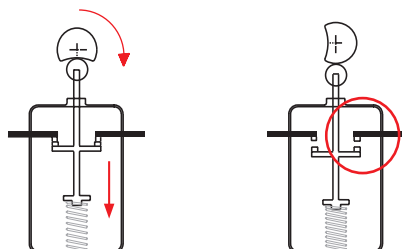
Le mode positif permet, grâce à un entretien préventif, de se soustraire des défaillances dangereuses schématisées ci-dessus. Avec le mode négatif, au contraire, les défaillances sont internes à l'interrupteur et donc difficilement détectables.

Avec le mode positif, les défaillances internes (contacts collés ou ressort endommagé) permettent tout de même l'ouverture des contacts et donc l'arrêt de la machine.



Utilisation des interrupteurs dans les applications de sécurité

Quand un seul interrupteur est utilisé dans une fonction de sécurité, il doit être actionné en mode positif. Pour les applications de sécurité, il faut utiliser le contact d'ouverture (normalement fermé) qui doit toujours être du type à **"ouverture positive"**, tous les interrupteurs qui reportent le symbole  sont équipés de contacts NC à ouverture positive.



Aucun raccordement élastique entre les contacts mobiles et l'actionneur sur lequel est appliquée la force d'actionnement.

S'il y a deux ou plus de deux interrupteurs, il vaut mieux les faire travailler en modes opposés, par exemple :

- Le premier avec un contact normalement fermé (contact d'ouverture) actionné par le protecteur en mode positif.
- L'autre avec un contact normalement ouvert (contact de fermeture), actionné par le protecteur en mode non positif.

Ceci est une pratique commune qui n'exclut pas, lorsque c'est justifiable, l'utilisation de deux interrupteurs actionnés en mode positif (voir diversification).

Diversification

La sécurité dans les systèmes redondants est augmentée par la **diversification**. Elle s'obtient en appliquant deux interrupteurs avec des diversités de conception et/ou de technologie, de manière à éviter des défaillances dues à la même cause. Les exemples de diversification sont: l'utilisation d'un interrupteur à action positive couplé à un autre à action non positive, d'un interrupteur à commande mécanique couplé à un interrupteur non mécanique (ex. capteur électronique) ou l'utilisation de deux interrupteurs à commande mécanique à action positive, mais avec un principe d'actionnement différent (ex. un interrupteur à clé FR 693 et un interrupteur à levier FR 1896).

Redondance

La **redondance** est l'utilisation de plus d'un dispositif ou système, pour garantir qu'en cas de défaillance dans les pièces d'un de ces derniers, un autre soit disponible pour effectuer ces fonctions de sécurité. Si la première défaillance n'est pas détectée, l'apparition d'une deuxième pourra entraîner la perte de la fonction de sécurité.

Autocontrôle

L'**autocontrôle** consiste à vérifier automatiquement le fonctionnement de tous les dispositifs qui interviennent dans le cycle de la machine. Par conséquent, le cycle suivant peut être interdit ou autorisé.

Redondance et autocontrôle

La combinaison en système de la **redondance** et de l'**autocontrôle** fait que la première défaillance dans le circuit de sécurité n'entraîne pas la perte des fonctions de sécurité. Cette première défaillance sera détectée au démarrage suivant ou dans tous les cas avant qu'une deuxième défaillance ne se manifeste, ce qui alors pourrait entraîner la perte de la fonction de sécurité.