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 à l'ensemble des mesures propres à protéger l'opérateur des machines des risques découlant de leur fonctionnement et aux aspects concernant la conception et le choix des dispositifs d'interverrouillage associés aux protecteurs.
Les risques dus à d'autres sources de danger telles que la présence d'électricité, d'appareils à pression, d'atmosphères explosives, etc., qui devront être évalués quand même par le fabricant des machines, ne sont pas traités.
Ce document a été préparé par Pizzato Elettrica au mieux de ses connaissances, en tenant compte des normes et interprétations ainsi que des technologies existantes. 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. La grande variété de produits et de dangers potentiels différents est la raison pour laquelle plusieurs directives ont été publiées au fil du temps. Par exemple on cite la directive Basse Tension 2014/35/UE, la directive sur les Atmosphères Explosives 2014/34/UE, la directive sur la Compatibilité Électromagnétique 2014/30/UE, etc. Les dangers résultants du fonctionnement des machines sont traités par la Directive Machine 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, bruit, etc.)
- B2 : Normes relatives aux dispositifs de sécurité (par exemple dispositifs de commande bimanuelle, dispositifs de verrouillage, protecteurs, etc.)

Normes de type 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 DE TYPE A
par exemple :

EN ISO 12100. Sécurité de la machine - Principes généraux de conception - Appréciation du risque et réduction du risque.

NORMES DE TYPE B1
par exemple :

EN IEC 62061. Sécurité fonctionnelle des systèmes de commande et contrôle électriques, électroniques et électroniques programmables relatifs à la sécurité
EN ISO 13849-1 et -2. Parties des systèmes de commande relatives à la sécurité

NORMES DE TYPE B2
par exemple :

EN ISO 13851. Dispositifs de commande bimanuelle
EN ISO 13850. Arrêt d'urgence
EN ISO 14119. Dispositifs de verrouillage des protecteurs
EN 60204-1. Équipement électrique des machines
EN 60947-5-1. Dispositifs de contrôle électromécaniques.

NORMES DE TYPE C
par exemple :

EN ISO 20430. Machines pour les matières plastiques et le caoutchouc - Machines de moulage par injection
EN 415-1. Sécurité des machines d'emballage
EN ISO 16092-1 et EN ISO 16092-2. Presses mécaniques
EN ISO 16092-1 et EN ISO 16092-3. Presses hydrauliques
EN ISO 19085-6. Sécurité des machines pour le travail du bois - Machines à fraiser sur une face, à outil rotatif - Partie 1 : Fraiseuses monobroches à arbre vertical (toupies)

3 – Concevoir des 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 produise, et le type de dommage possible pour l'opérateur.

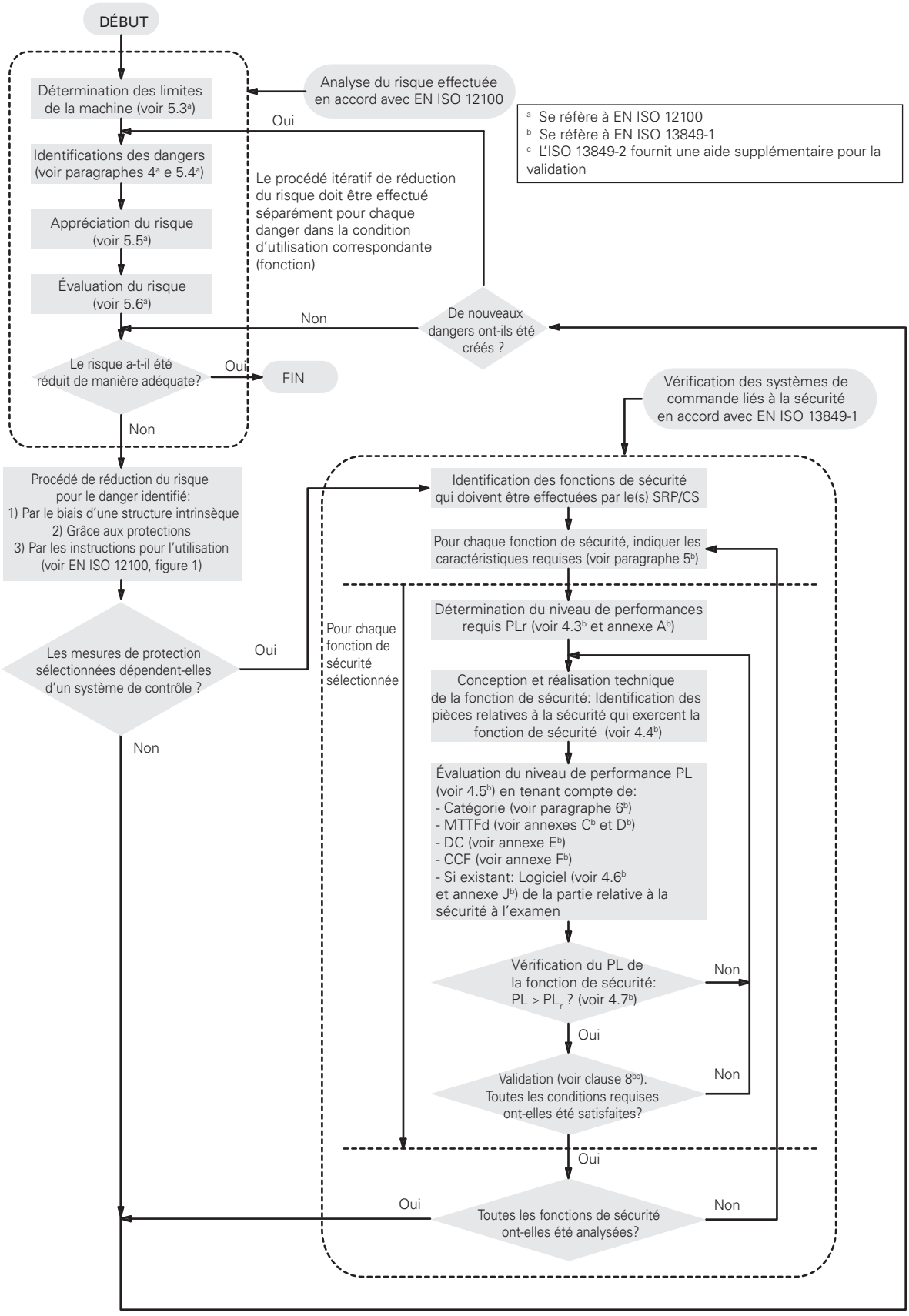
La méthodologie d'analyse des risques, de leur évaluation, de la façon de procéder pour leur réduction est définie par la norme EN ISO 12100, un modèle cyclique d'analyse qui, une fois les objectifs initiaux définis, consiste à évaluer à plusieurs reprises l'analyse des risques et de leurs solutions possibles en vue de limiter ces risques tant que les objectifs initiaux ne sont pas remplis.

Le modèle introduit par cette norme prévoit, après une analyse des risques, de procéder à la réduction/élimination de ces derniers en respectant les étapes suivantes :
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 présente des dangers et qu'il n'est pas possible d'éliminer complètement tous les risques éventuels

associés, l'objectif est de réduire le risque de la machine à un niveau résiduel acceptable.

Si le risque est réduit par un système de contrôle, la norme EN ISO 13849-1, qui fournit un modèle d'évaluation de la qualité de ce système, entre en jeu. 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.

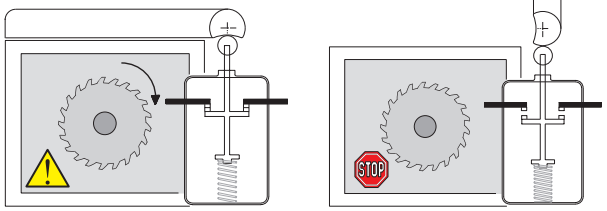


Note : Cette figure a été obtenue par la combinaison des figures 1 et 3 de EN ISO 13849-1. Les textes reportés sont la traduction non officielle des textes cités dans la norme.

4 - Ouverture forcée, redondance, diversification et autocontrôle

Mode positif et mode négatif.
Selon la norme EN ISO 12100, 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**.

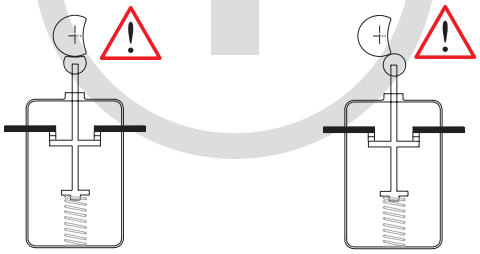
Mode positif



Machine en fonctionnement
Porte fermée

Machine arrêtée
Porte ouverte

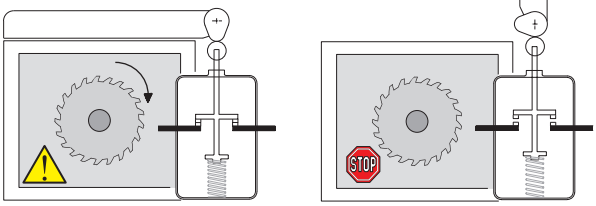
Défaillances dangereuses : la machine continue à fonctionner.



Galet
usé

Galet
décalé

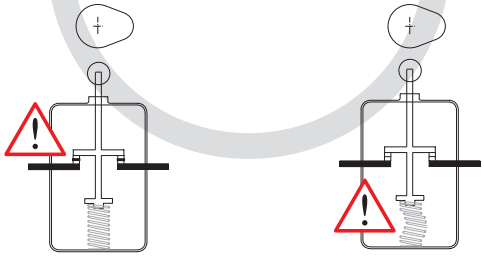
Mode négatif



Machine en fonctionnement
Porte fermée

Machine arrêtée
Porte ouverte

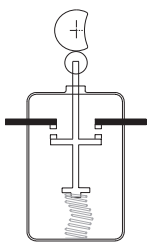
Défaillances dangereuses : la machine continue à fonctionner.



Contacts
collés

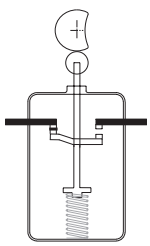
Ressort
endommagé

Le mode positif permet, grâce à un entretien préventif, d'éluder les défaillances dangereuses schématisées ci-dessus. En mode négatif par contre, les défaillances sont internes à l'interrupteur et donc difficilement détectables.
En 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.



Ressort
endommagé

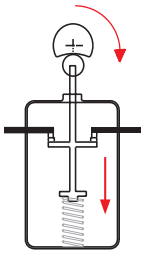
Machine
arrêtée

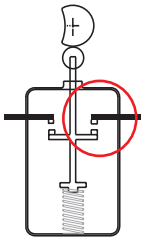


Contacts
collés

Machine
arrêtée

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 de type à **ouverture forcée**, tous les interrupteurs accompagnés du symbole ⊖ sont équipés de contacts NC à ouverture forcée.





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

S'il y a deux interrupteurs ou plus, il convient de les faire fonctionner 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 courante qui n'exclut pas, lorsqu'elle 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 présentant 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 autre à commande non mécanique (ex. capteur électronique) ou encore de deux interrupteurs à commande mécanique à action positive, mais de principes d'actionnement différents (ex. un interrupteur à clé FR 693-M2 et un interrupteur à goujon FR 1896-M2).

Redondance
La **redondance** consiste à utiliser 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 assurer les 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. Le cycle suivant peut être interdit ou autorisé en conséquence.

Redondance et autocontrôle
La combinaison dans un 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 une deuxième défaillance qui pourrait entraîner la perte de la fonction de sécurité.

5- Conception et choix des dispositifs d'interverrouillage associés aux protecteurs (norme EN ISO 14119)

La troisième édition de la norme ISO 14119 « Dispositifs de verrouillage associés à des protecteurs — Principes de conception et de choix » a été publiée en septembre 2024. La publication de cette nouvelle édition introduit quelques nouveautés intéressantes, en particulier en ce qui concerne la classification des dispositifs et les modes de fixation non amovible.

NEW ISO 14119:2024

La norme s'adresse tant aux fabricants des dispositifs d'interverrouillage qu'aux constructeurs des machines (et des systèmes intégrateur), en ajoutant les qualités nécessaires à la réalisation et à la bonne installation de ces dispositifs.
La norme met en lumière quelques aspects pas toujours clairs et prend en compte les dernières technologies utilisées dans la construction des dispositifs de verrouillage. En outre, elle définit quelques paramètres (type d'actionneur et niveau de codification) et présente les mesures à prendre lors de l'installation pour éviter le contournement des dispositifs de protection.
La norme prend en compte quelques autres aspects relatifs aux dispositifs de blocage (par exemple : principes de verrouillage, verrouillage électromagnétique, déverrouillage auxiliaire, commande d'anti-enfermement et déverrouillage d'urgence, etc.) qui ne sont pas traités dans ce document.

Niveau de codification des actionneurs

La norme comprend la définition d'un actionneur codifié et la classification des niveaux de codification :

- **actionneur codifié** – actionneur conçu spécialement pour être combiné à un dispositif d'interverrouillage spécifique ;
- **actionneur de niveau de codification bas** – actionneur codifié pouvant avoir 1 à 9 codifications différentes (par exemple la série de capteurs magnétiques SR ou les interrupteurs de sécurité à actionneur séparé avec détection mécanique FS, FG, FR, FD…) ;
- **actionneur de niveau de codification moyen** – actionneur codifié pouvant avoir 10 à 1000 codifications différentes ;
- **actionneur de niveau de codification élevé** – actionneur codifié pouvant avoir plus que 1000 codifications différentes (par exemple la série de capteurs ST à technologie RFID ou les dispositifs d'interverrouillage des séries NG, NS et NX à technologie RFID avec blocage de la protection).

Typologie de dispositifs d'interverrouillage

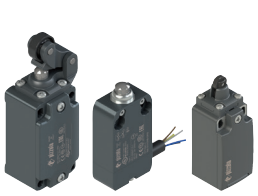
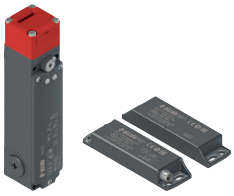
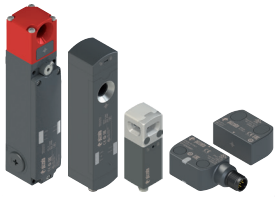
La troisième édition de la norme ISO 14119 introduit un nouveau type de dispositif d'interverrouillage, le type 5, pour les dispositifs à clé prisonnière, en plus de ceux déjà définis dans la seconde édition :

- **Dispositifs d'interverrouillage de type 1** – Dispositifs d'interverrouillage actionnés mécaniquement par un actionneur non codifié (par exemple les dispositifs d'interverrouillage à charnière de la série HP).
- **Dispositifs d'interverrouillage de type 2** – Dispositifs d'interverrouillage actionnés mécaniquement par un actionneur non codifié (par exemple les interrupteurs de sécurité à actionneur séparé des séries FR, FS, FG, ...).
- **Dispositifs d'interverrouillage de type 3** – Dispositifs d'interverrouillage actionnés sans contact par un actionneur non codifié.
- **Dispositifs d'interverrouillage de type 4** – Dispositifs d'interverrouillage actionnés sans contact par un actionneur non codifié (par exemple les capteurs de sécurité avec technologie RFID de la série ST et les interrupteurs de sécurité avec technologie RFID des séries NG, NS et NX).
- **Dispositifs d'interverrouillage de type 5** – Dispositifs d'interverrouillage à clé prisonnière dont la fonction est de verrouiller ou de déverrouiller une ou plusieurs clés dans un certain système d'interverrouillage à clé prisonnière.

Type	Principe d'actionnement	Actionneur	Surveillance des protections	Exemples d'actionneurs		
				Principe d'actionnement	Actionneur	Annexe
Type 1	Mécanique	Non codifié	Directe	Contact physique / force	Came en rotation	A.1
					Came linéaire	A.2, A.4
					Charnière	A.3
Type 2	Mécanique	Codifié	Directe	Contact physique / force	Actionneur à languette préformée	B.1
Type 3	Sans contact	Non codifié	Directe	Magnétique	Aimant, solénoïde	C.1
				Inductif	Métal ferrique	
				Capacitif	Tout objet adapté	
				Ultrasons	Tout objet adapté	
				Optique	Tout objet adapté	
Type 4	Sans contact	Codifié	Directe	Magnétique	À codage magnétique	D.1
				RFID	RFID codifié	D.2
				Optique	Optique codifié	-
Type 5	Mécanique (clé prisonnière)	Codifié	Indirecte ou directe		Préformé	K

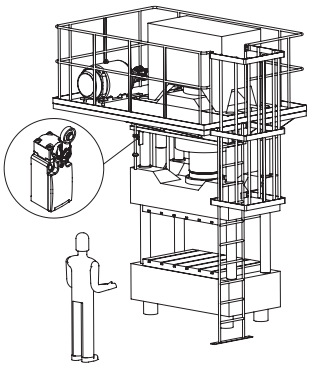
Extrait d'ISO 14119:2024 - Tableau 2

Conditions de conception et d'installation de dispositifs d'interverrouillage conformément à la norme ISO 14119:2024 afin de réduire le risque de contournement des protecteurs.

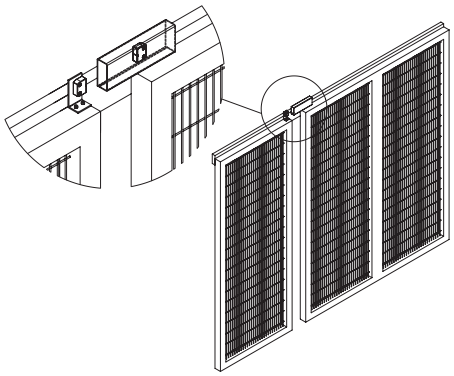
Principes et mesures pour éviter le contournement	Référence	Dispositifs de type 1		Dispositifs de type 2 et type 4	
		Interrupteurs de sécurité à came en rotation ou linéaire	Interrupteurs de sécurité à charnière	Actionneurs de niveau de codification bas et moyen	Actionneur de niveau de codification élevé
					
Deuxième dispositif d'interverrouillage et vérification de la plausibilité	8.3 d) 2)	R		R	
Montage hors de portée (1)	8.3 a) 1)	X		X	
Obstacle physique, écran (2)	8.3 a) 2)				
Montage en position cachée (3)	8.3 a) 3)				
Test du circuit de commande (4)	8.3 d) 1)				
Fixation non amovible de l'actionneur	8.3 c)			M	M
Fixation non amovible du dispositif	8.3 c)			R	R
Fixation non amovible du dispositif et de l'actionneur	8.3 c)	X	M		

Extrait d'ISO 14119:2024 - Tableau 5
Légende : X = obligation d'appliquer au moins une des mesures mentionnées dans la colonne « Principes et mesures pour éviter le contournement » ; M = mesure obligatoire ; R = mesure recommandée.

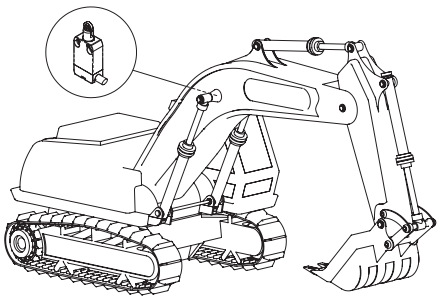
Afin de satisfaire aux exigences de la norme ISO 14119, il est évidemment plus simple d'utiliser les dispositifs avec la technologie RFID de niveau de codification élevé et des interrupteurs à charnière puisqu'il est nécessaire de satisfaire à ces quelques exigences afin d'éviter le contournement de ces dispositifs.
Les dispositifs de niveau de codification bas ou moyen nécessitent des exigences supplémentaires pour assurer que l'application soit correctement protégée contre la manipulation.



(1) - Montage hors de portée



(2) - Obstacle physique, écran



(3) - Montage en position cachée

(4) - Un test du circuit de commande peut par exemple être réalisé sur une machine dont le cycle de travail est facilement prévisible, afin de vérifier qu'à la fin ou pendant des phases déterminées du cycle de travail, les protecteurs sont effectivement ouverts (pour retirer le matériau usiné ou pour effectuer les contrôles de qualité par exemple) ; dans le cas où le système de contrôle n'effectue pas ces actions d'ouverture des protecteurs, une alarme est générée et la machine s'arrête.

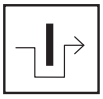
Fixation non amovible

La fixation non amovible constitue l'une des solutions prévues dans la norme pour empêcher le démontage ou le repositionnement des éléments qui composent le dispositif d'interverrouillage. La norme présente quelques exemples de fixation non amovible. En particulier, la troisième édition introduit formellement **la possibilité d'utiliser des bouchons pour fermer l'ouverture des boulons et vis qui ne peuvent être retirés qu'en les détruisant.** Les exemples présentés dans la norme sont les suivants :

- soudage ;
- collage des filetages (avec une colle suffisamment forte qui nécessite de la chaleur ou un agent chimique pour être éliminée) ;
- vis one-way ;
- rivetage ;
- fraisage de la fente de la tête des vis pour en empêcher le dévissage ;
- remplissage de l'ouverture des boulons et vis (avec du plastique, de la résine, **des capuchons ou des bouchons qui ne peuvent être retirés qu'en les détruisant** ou une boule métallique).

Dispositifs de verrouillage et force de retenue

Le constructeur du dispositif d'interverrouillage avec verrouillage doit s'assurer que, dans les conditions de verrouillage, le dispositif résiste au moins à la force de retenue spécifiée F_{ZH}. Cette force peut être égale au maximum à la force maximale de retenue divisée par un coefficient de sécurité de 1,3.
Par exemple, un dispositif avec une force maximale spécifiée F_{ZH} =2000 N doit être soumis à un test avec une force de retenue maximale F_{TEST} =2600 N.
Un dispositif d'interverrouillage avec verrouillage peut prévoir soit la fonction de surveillance de la position du protecteur (protecteur ouvert/fermé), soit la fonction de verrouillage du protecteur (protecteur verrouillé/déverrouillé). Chacune de ces fonctions peut demander un niveau de performance PL (réf. EN ISO 13849-1) différent. En effet, la fonction de verrouillage nécessite normalement un PL inférieur à la fonction de surveillance de la position. (Voir point 9.3, remarque 2 de la norme ISO 14119:2024).
Pour mettre en évidence qu'un dispositif d'interverrouillage effectue également la surveillance de la condition du verrouillage, la nouvelle norme prévoit le report du symbole représenté ici sur le côté du produit.



6 –Situation normative actuelle. Les raisons du changement, les nouvelles normes et quelques superpositions

Les normes « traditionnelles » pour la sécurité fonctionnelle, comme 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 des nouvelles normes est de type essentiellement probabiliste et introduit donc de nouvelles variables de type statistique.

La norme « mère » de cette approche est la norme 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 procès, machines industrielles, installations nucléaires). 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 IEC 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).

Développée par le CEN sous l'égide de l'ISO, la norme EN ISO 13849-1 dérive de cette approche probabiliste, mais tente de faire en sorte que le constructeur habitué aux concepts de l'EN 954-1 puisse 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 13849-1 est une norme de type B1 ; elle 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 l'IEC 61508 et établit 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, deux normes sont donc actuellement en vigueur :
EN ISO 13849-1. Norme de type B1 qui utilise le concept de PL
EN IEC 62061. Norme de type B1 qui utilise le concept de SIL.

Note importante
EN ISO 13849-1 est une norme de type B1 et, donc, si une machine est déjà couverte par une norme de type C, c'est cette dernière qui fait autorité. Certaines normes de type C pas encore mises à jour sont encore basées sur les concepts de la norme EN 954-1. Pour les constructeurs des machines couvertes par une norme de type C, les temps d'introduction des nouvelles réglementations pourraient varier en fonction de la rapidité à laquelle les différents comités techniques les mettront à jour.

Les normes EN IEC 62061 et EN ISO 13849-1 se superposent donc relativement bien en ce qui concerne leur domaine d'application et sont similaires sur de nombreux aspects. En effet, 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.

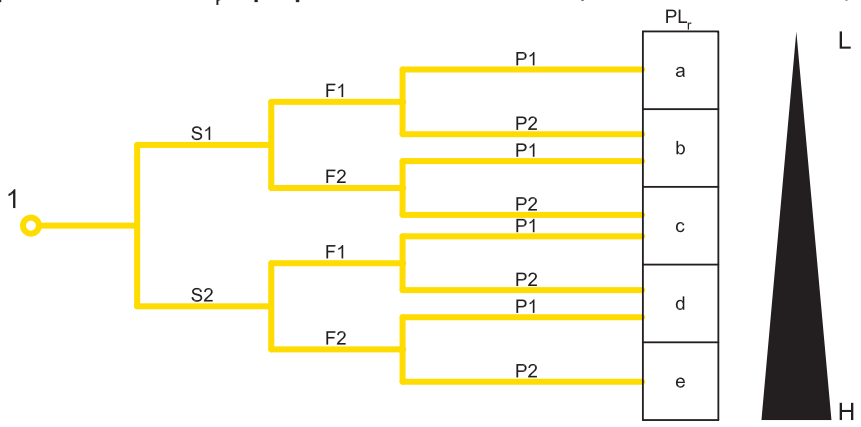
PL EN ISO 13849-1	**a**	**b**	**c**	**d**	**e**
SIL EN IEC 62061 - IEC 61508	**-**	**1**	**1**	**2**	**3**
PFH_D	de 10^{-5} à 10^{-4}	de $3x10^{-6}$ à 10^{-5}	de 10^{-6} à $3x10^{-6}$	de 10^{-7} à 10^{-6}	de 10^{-8} à 10^{-7}
Une défaillance dangereuse tous les n ans	de ~1 à ~10	de ~10 à ~40	de ~40 à ~100	de ~100 à ~1000	de ~1000 à ~10000

Le choix de la norme à utiliser reviendra au constructeur, selon la technologie utilisée. Nous retenons que la norme EN ISO 13849-1, avec une approche intermédiaire et la réutilisation des concepts déjà connus dans le marché, est une norme d'application plus facile.

7- La norme EN ISO 13849-1 et les nouveaux paramètres : PL, $MTTF_D$, DC, CCF

La norme EN ISO 13849-1 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 duquel on doit être en mesure de démontrer que chaque fonction de sécurité choisie est adaptée au risque relatif concerné.
La première étape consiste donc à évaluer le niveau de performance requis pour chaque fonction de sécurité. Comme pour l'EN 954-1, l'EN ISO 13849-1 utilise aussi un graphique pour l'analyse du risque d'une fonction d'une machine (fig. 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 que celui requis.

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

* F1 devrait être choisi lorsque l'accumulation des temps d'exposition ne dépasse pas 1/20e du temps de travail total et que la fréquence d'exposition ne va pas au-delà d'une fois toutes les 15 minutes

****** En l'absence d'autres justifications, F2 devrait être choisi lorsque la fréquence d'exposition est supérieure à une fois toutes les 15 minutes.

Paramètres de risque

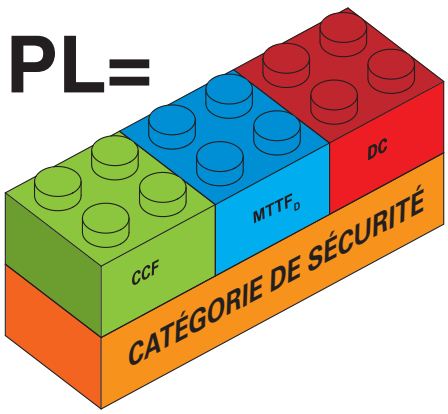
S Gravité de la blessure
S1 blessure légère (normalement réversible)
S2 blessure grave (normalement irréversible ou mortelle)
F Fréquence et/ou durée de l'exposition au danger
***F1** de rare à assez fréquente et/ou de courte durée
****F2** de fréquente à continue et/ou de longue durée
P Possibilité 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 de ne pas devoir répéter l'analyse des risques de la machine, mais de chercher à réutiliser ce qui a déjà été fait avec l'analyse des risques de la norme EN 954-1.
Cela n'est généralement pas possible car la nouvelle norme a changé le graphique du risque (voir figure précédente). Les niveaux de fonction de sécurité requise peuvent donc être modifiés pour un même risque. L'institution allemande BGIA dans le rapport 2008 / 2 sur la norme EN ISO 13849-1 suggère que, en adoptant une approche de type « worst case », on peut adopter une conversion comme dans le tableau ci-contre. Pour d'ultérieures informations, se référer au texte en question.

Catégorie requise par EN 954-1		Niveau de performance requis (PLr) et, catégorie requise selon EN ISO 13849-1
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 défaillances dangereuses 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.

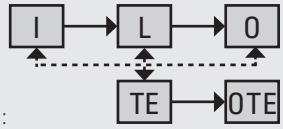
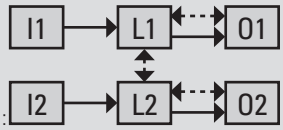
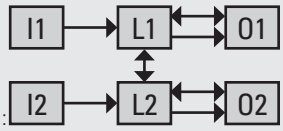
PL	Probabilité moyenne de défaillances dangereuses par heure PFHD (1/h)		
a	$\geq 10^{-5}$	et	$< 10^{-4}$
b	$\geq 3 \times 10^{-6}$	et	$<10^{-5}$
c	$\geq 10^{-6}$	et	$< 3 \times 10^{-6}$
d	$\geq 10^{-7}$	et	$< 10^{-6}$
e	$\geq 10^{-8}$	et	$<10^{-7}$



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.

La norme EN ISO 13849-1 admet cinq différentes structures de circuit de base qu'elle appelle « architectures désignées du système ». Les architectures combinées avec les exigences de comportement en cas de défaillance du système et avec des valeurs minimales des $MTTF_D$, 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 EN 954-1.

Catégorie	Résumé des exigences	Comportement du système	Principes pour la sécurité	$MTTF_D$ 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	Basse ou Moyenne	Nulle	Sans objet
1	Les exigences de la catégorie B doivent être remplies. Nécessité d'appliquer des composants 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	Sans objet
2	Les exigences de la catégorie B doivent être remplies, des principes de sécurité éprouvés doivent être utilisés. 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 Basse à Élevée	De Basse à Moyenne	Voir l'annexe F
3	Les exigences de la catégorie B doivent être remplies, des principes de sécurité éprouvés doivent être utilisés. 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 Basse à Élevée	De Basse à Moyenne	Voir l'annexe F
4	Les exigences de la catégorie B doivent être remplies, des principes de sécurité éprouvés doivent être utilisés. 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 (accumulation de défaillances incluse)	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 du $MTTF_D$ se base sur des valeurs numériques fournies par les constructeurs de chaque composant formant le système. En l'absence de données, la norme fournit des valeurs dans des tableaux de référence spéciaux (annexe C de la norme EN ISO 13849-1). Le comptage portera à une valeur numérique qui rentrera dans trois catégories : Élevé, Moyen ou Bas.

Classification	Valeurs
Non acceptable	$MTTF_D$< 3 ans
Basse	3 ans ≤ $MTTF_D$< 10 ans
Moyenne	10 ans ≤ $MTTF_D$< 30 ans
Élevée	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 B_{10D} du composant c'est-à-dire le nombre de cycles du composant dans lequel 10% des prototypes testés présentent une défaillance dangereuse.
La valeur B_{10D} du composant doit être convertie par le constructeur de la machine en $MTTF_D$ par la formule :

$$MTTF_D = \frac{B_{10_D}}{0{,}1 \cdot n_{op}}$$

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, il est possible d'obtenir n_{op} à partir 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_{cycle}= 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 électromécanique 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 manœuvres de cycle normales, alors le $MTTF_D$ du même télérupteur, avec un temps de cycle bas, pourrait diminuer considérablement.

Tous les éléments du circuit de contrôle, en fonction de sa structure, contribuent au calcul du $MTTF_D$ de ce dernier. Dans les circuits avec une architecture à 1 canal (comme dans le cas des catégories B, 1 et 2), la contribution de chaque composant est linéaire et le calcul du $MTTF_d$ du canal est obtenu à partir de :

$$\frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{D\ i}}$$

Pour éviter des interprétations trop optimistes la valeur maximale de $MTTF_D$ de chaque canal est limitée à 100 ans (pour les catégories B, 1, 2 et 3) ou 2500 ans (catégorie 4). Ne sont pas permis canaux avec un $MTTF_D$ inferieur 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 :

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right]$$

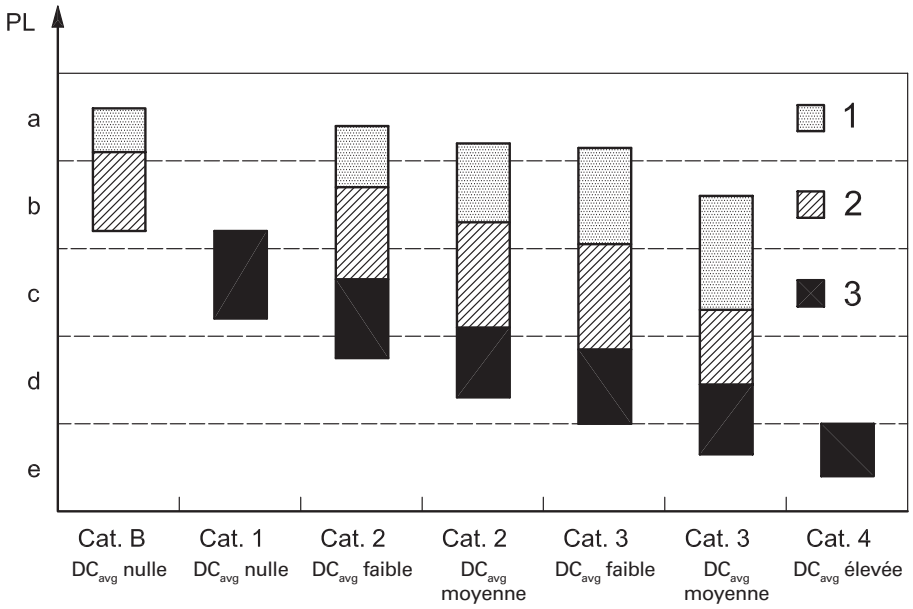
DC ("Diagnostic Coverage", couverture du diagnostic).

Ce paramètre essaie d'indiquer à quel point le système est en mesure d' « auto-surveiller » un éventuel dysfonctionnement. 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 la norme EN ISO 13849-1) en fonction des précautions adoptées par le fabricant pour détecter les anomalies de son circuit. Comme en général il existe plusieurs précautions dans le même circuit pour détecter différentes anomalies, 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 DC_{avg} < 60%
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 il sera aussi nécessaire, pour le calcul du PL, 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.

PL (« Performance Level »)
En connaissance de ces données, la norme EN ISO 13849-1 fournit le PL du système au moyen d'un tableau de corrélation (annexe K de la norme EN ISO 13849-1), ou sous forme graphique simplifiée (paragraphe 4.5 de de la norme EN ISO 13849-1), par la figure suivante :

Relations entre les catégories DC_{avg}, $MTTF_D$ de chaque canal et PL (extrait de EN ISO 13849-1, fig. 5)



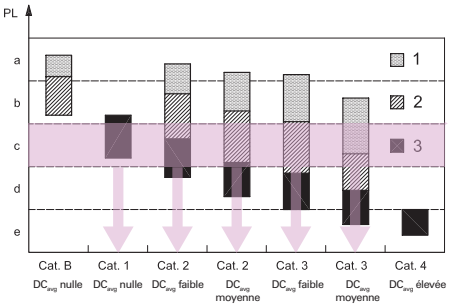
1 = $MTTF_D$ de chaque canal Basse
(3 ans ≤ $MTTF_D$< 10 ans)

2 = $MTTF_D$ de chaque canal Moyenne
(10 ans ≤ $MTTF_D$< 30 ans)

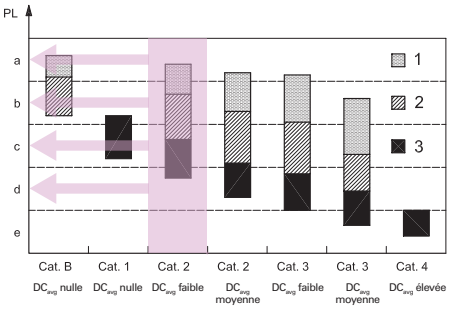
3 = $MTTF_D$de chaque canal Élevée
(30 ans ≤ $MTTF_D$ ≤ 100 ans)

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 remarque que toutes les solutions ci-après sont possibles pour obtenir un système avec PL égal à « c » :
1. Système de catégorie 3 avec composants peu fiables ($MTTF_D$=basse) 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 DC 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.

Notes

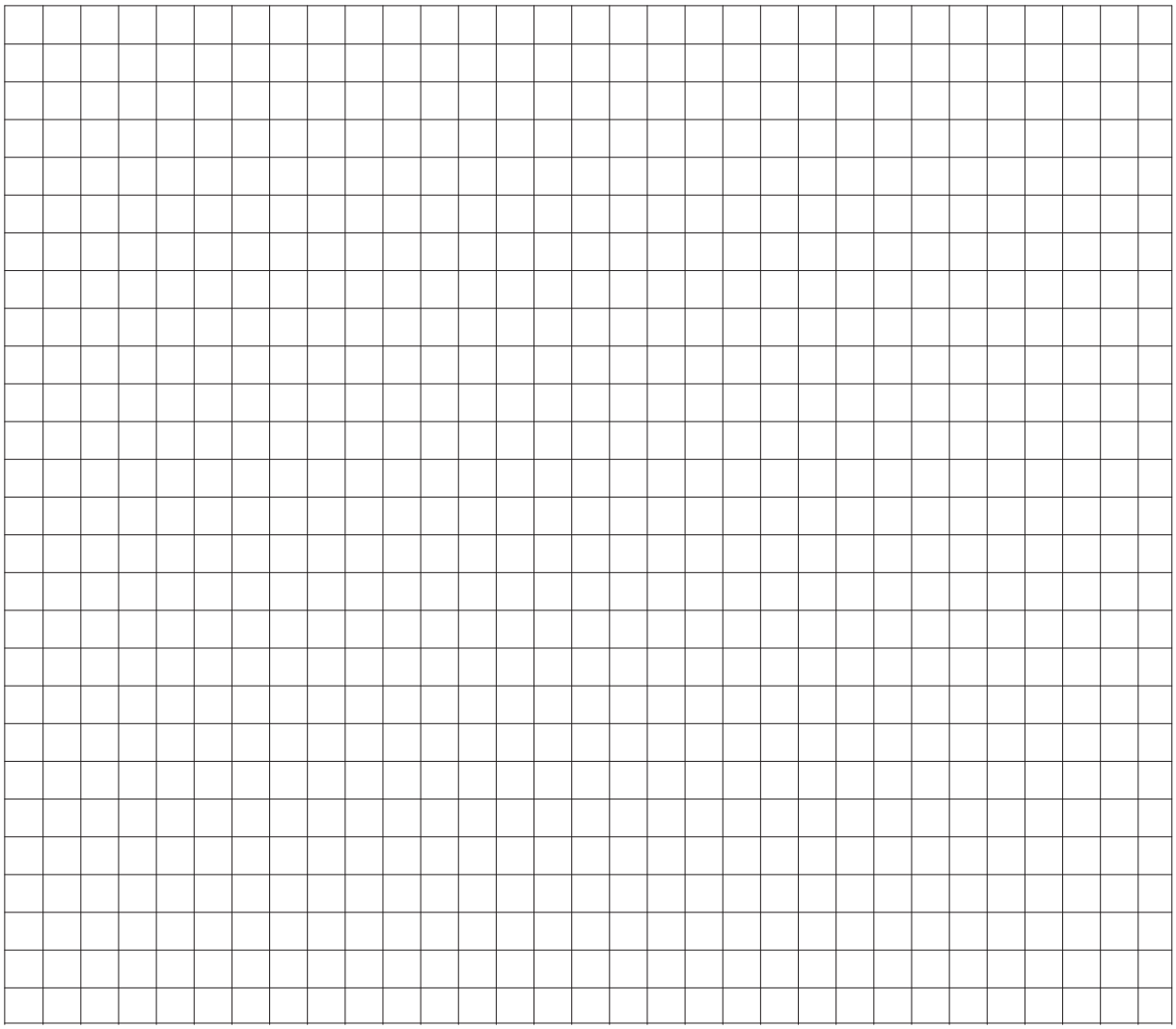


Tableau des paramètres de sécurité

Les données B_{10D} indiquées dans le tableau font référence à la vie mécanique des contacts des dispositifs dans des conditions ambiantes normales. La valeur B_{10D} pour les contacts NC et NO se réfère à une charge électrique maximale égale à 10% de la valeur du courant indiqué dans les catégories d'utilisation. Mission time (pour tous les articles indiqués ci-dessous) : 20 ans.

Dispositifs électromécaniques

Série	Description de l'article	B_{10D} (NO)	B_{10D} (NC)	B_{10}/B_{10D}
F• ••••	Interrupteurs de position	1.000.000	40.000.000	50%
F• ••93 F• ••92	Interrupteurs de sécurité à actionneur séparé	1.000.000	2.000.000	50%
F• ••99 F• ••R2	Interrupteurs de sécurité à actionneur séparé avec verrouillage	1.000.000	1.000.000	50%
FG, FY	Interrupteurs de sécurité à actionneur séparé avec verrouillage	1.000.000	5.000.000	20%
FS	Interrupteurs de sécurité à actionneur séparé avec verrouillage	1.000.000	4.000.000	20%
F• ••96 F• ••95	Interrupteurs de sécurité à goujon pour charnières	1.000.000	5.000.000	20%
F• ••C•	Interrupteurs à levier à fente pour protections à battant	1.000.000	2.000.000	50%
F• ••••	Interrupteurs à câble pour l'arrêt d'urgence	100.000	200.000	50%
HP - HX B•22-•••	Charnières de sécurité	1.000.000	5.000.000	20%
SR	Capteurs magnétiques de sécurité (utilisés avec des modules de sécurité Pizzato Elettrica compatibles)	20.000.000	20.000.000	50%
SR	Capteurs magnétiques de sécurité (utilisés à charge maximale : DC12 24V 250mA)	400.000	400.000	100%
PX, PA	Interrupteurs à pédale	1.000.000	20.000.000	50%
MK	Micro-interrupteurs de position	1.000.000	20.000.000	50%
NA B•• - NA G•• - NA H•• - NA L•• NB B•• - NB G•• - NB H•• - NB L•• NF B•• - NF G•• - NF H•• - NF L••	Interrupteurs de position précâblés modulaires	1.000.000	40.000.000	50%
NA C•• - NB C•• - NF C••	Interrupteurs de position précâblés modulaires	1.000.000	10.000.000	50%
E2 C•••••••	Blocs de contact	1.000.000	40.000.000	50%

Série	Description de l'article	B_{10D}	B_{10}/B_{10D}
E2 •PU1••••••, E2 •PL1••••••	Boutons simples à accrochage	2.000.000	50%
E2 •PU2••••••, E2 •PL2••••••	Boutons simples à impulsion	30.000.000	50%
E2 •PD••••••, E2 •PT••••••	Boutons doubles et triples	2.000.000	50%
E2 •PQ••••••	Boutons quadruples	2.000.000	50%
E2 •PE••••••	Boutons d'arrêt d'urgence	600.000	50%
VN NG-AC2605•	Boutons d'arrêt d'urgence intégrés aux dispositifs des séries NG, NS, BN	100.000	50%
E2 •SE••••••, E2 •SL••••••	Sélecteurs et sélecteurs lumineux	2.000.000	50%
E2 •SC••••••	Sélecteurs à clé	600.000	50%
E2 •MA••••••	Joysticks	2.000.000	50%

Série ATEX	Description de l'article	B_{10D} (NO)	B_{10D} (NC)	B_{10}/B_{10D}
F• ••••-EX•	Interrupteurs de position	500.000	20.000.000	50%
F• ••93-EX•	Interrupteurs de sécurité à actionneur séparé	500.000	1.000.000	50%
F• ••99-EX• F• ••R2-EX•	Interrupteurs de sécurité à actionneur séparé avec verrouillage	500.000	500.000	50%
F• ••96-EX• F• ••95-EX•	Interrupteurs de sécurité à goujon pour charnières	500.000	2.500.000	20%
F• ••C•-EX•	Interrupteurs à levier à fente pour protections à battant	500.000	1.000.000	50%
F• ••••-EX•	Interrupteurs à câble pour l'arrêt d'urgence	500.000	1.000.000	50%

Dispositifs électroniques

Code/série	Description de l'article	$MTTF_D$	DC	PFH_D	SIL	PL	Cat
HX BEE1-•••	Charnières de sécurité avec bloc électronique	2413	High	1,24E-09	3	e	4
ST D••••••	Capteurs de sécurité avec technologie RFID	4077	High	1,20E-11	3	e	4
ST G••••••, ST H••••••	Capteurs de sécurité avec technologie RFID	1551	High	1,19E-09	3	e	4
NG	Interrupteurs de sécurité RFID avec verrouillage						
	Fonction de surveillance de l'actionneur verrouillé - mode 1	2968	High	1,15E-09	3	e	4
	Fonction de surveillance de la présence de l'actionneur - mode 2	3946	High	1,15E-09	3	e	4
	Fonction de surveillance de l'actionneur verrouillé - mode 3	2957	High	1,48E-09	2	d	2
	Fonction de surveillance de la présence de l'actionneur - mode 3	3927	High	1,48E-09	2	d	2
	Commande à double canal de la fonction de verrouillage de l'actionneur	4011	High	1,51E-10	3	e	4
	Commande à canal unique de la fonction de verrouillage de l'actionneur	4011	High	1,51E-10	2	d	2
NS	Interrupteurs de sécurité RFID avec verrouillage						
	Fonction de surveillance de l'actionneur verrouillé - mode 1	2657	High	1,23E-09	3	e	4
	Fonction de surveillance de la présence de l'actionneur - mode 2	1840	High	1,22E-09	3	e	4
	Fonction de surveillance de l'actionneur verrouillé - mode 3	2627	High	1,50E-09	2	d	2
	Fonction de surveillance de la présence de l'actionneur - mode 3	3987	High	1,49E-09	2	d	2
	Commande à double canal de la fonction de verrouillage de l'actionneur	2254	High	2,04E-10	3	e	4
	Commande à canal unique de la fonction de verrouillage de l'actionneur	2254	High	2,04E-10	2	d	2
NX	Interrupteurs de sécurité RFID avec verrouillage						
	Fonction de surveillance de l'actionneur verrouillé - mode 1	1688	High	3,07E-10	3	e	4
	Fonction de surveillance de la présence de l'actionneur - mode 2	1694	High	3,07E-10	3	e	4
	Commande à double canal de la fonction de verrouillage de l'actionneur	1639	High	2,82E-10	3	e	4
	Commande à canal unique de la fonction de verrouillage de l'actionneur	1639	High	2,82E-10	2	d	2

Dispositifs électroniques

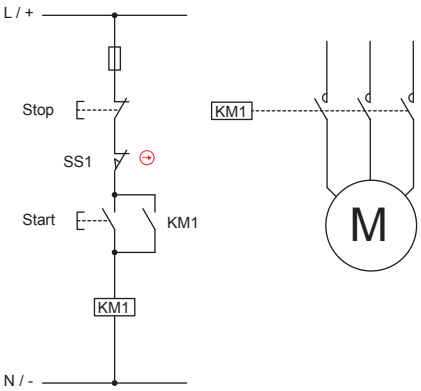
Code/série	Description de l'article	$MTTF_D$	DC	PFH_D	SIL	PL	Cat
CS AM-01	Module de sécurité pour la détection d'arrêt moteur	218	Medium	8,70E-09	2	d	3
CS AM••							
SF1 (standstill)	Détection d'arrêt moteur	70	High	1,00E-09	3	e	4
SF2 (speed)	Détection de la vitesse du moteur	70	High	1,00E-09	3	e	4
SF3 (rotation)	Détection du sens de rotation du moteur	67	High	2,06E-08	2	d	2
SF2 + SF3 (speed & rotation)	Détection de la vitesse du moteur et du sens de rotation	67	High	2,06E-08	2	d	2
SF2 + SF3 (dual speed)	Détection de vitesse du moteur (dual range)	67	High	2,06E-08	2	d	2
CS AR-01, CS AR-02	Modules de sécurité pour le contrôle de protecteurs et d'arrêts d'urgence	227	High	1,18E-10	3	e	4
CS AR-04	Module de sécurité pour le contrôle de protecteurs et d'arrêts d'urgence	152	High	1,84E-10	3	e	4
CS AR-05, CS AR-06	Modules de sécurité pour le contrôle de protecteurs, d'arrêts d'urgence et de barrières optiques	152	High	1,84E-10	3	e	4
CS AR-07	Module de sécurité pour le contrôle de protecteurs et d'arrêts d'urgence	111	High	7,56E-10	3	e	4
CS AR-08	Module de sécurité pour le contrôle de protecteurs, d'arrêts d'urgence et de barrières optiques	1547	High	9,73E-11	3	e	4
CS AR-20, CS AR-21	Modules de sécurité pour le contrôle de protecteurs et d'arrêts d'urgence	225	High	4,18E-10	3	e	3
CS AR-22, CS AR-23	Modules de sécurité pour le contrôle de protecteurs et d'arrêts d'urgence	151	High	5,28E-10	3	e	3
CS AR-24, CS AR-25	Modules de sécurité pour le contrôle de protecteurs et d'arrêts d'urgence	113	High	6,62E-10	3	e	3
CS AR-40, CS AR-41	Modules de sécurité pour le contrôle de protecteurs et d'arrêts d'urgence	225	High	4,18E-10	2	d	2
CS AR-46	Module de sécurité pour le contrôle de protecteurs et d'arrêts d'urgence	435	-	3,32E-08	1	c	1
CS AR-51	Module de sécurité pour le contrôle de tapis et bords sensibles	212	High	3,65E-09	3	e	4
CS AR-90	Module de sécurité pour le contrôle du nivelage à l'étage des ascenseurs	382	High	5,03E-10	3	e	4
CS AR-91	Module de sécurité pour le contrôle du nivelage à l'étage des ascenseurs	227	High	1,18E-10	3	e	4
CS AR-93	Module de sécurité pour le contrôle du nivelage à l'étage des ascenseurs	227	High	1,34E-10	3	e	4
CS AR-94	Module de sécurité pour le contrôle du nivelage à l'étage des ascenseurs	227	High	1,13E-10	3	e	4
CS AR-95	Module de sécurité pour le contrôle du nivelage à l'étage des ascenseurs	213	High	5,42E-09	3	e	4
CS AT-0•, CS AT-1•	Modules de sécurité temporisés pour le contrôle de protecteurs et d'arrêts d'urgence	88	High	1,23E-08	3	e	4
CS AT-3•	Module de sécurité temporisé pour le contrôle de protecteurs et d'arrêts d'urgence	135	High	1,95E-09	3	e	4
CS DM-01	Module de sécurité pour le contrôle de commande bimanuelle	142	High	2,99E-08	3	e	4
CS DM-02	Module de sécurité pour le contrôle de commande bimanuelle	206	High	2,98E-08	3	e	4
CS DM-20	Module de sécurité pour le contrôle de commande bimanuelle	42	-	1,32E-06	1	c	1
CS FS-1•	Module temporisateur de sécurité	404	High	5,06E-10	3	e	4
CS FS-2•, CS FS-3•	Modules temporisateurs de sécurité	205	High	1,10E-08	2	d	3
CS FS-5•	Module temporisateur de sécurité	379	Medium	1,31E-09	2	d	3
CS ME-01	Module d'extension de contacts	91	High	5,26E-10	①	①	①
CS ME-02	Module d'extension de contacts	114	High	4,17E-10	①	①	①
CS ME-03	Module d'extension de contacts	152	High	3,09E-10	①	①	①
CS ME-20	Module d'extension de contacts	114	High	6,14E-10	①	①	①
CS ME-31	Module d'extension de contacts	110	High	4,07E-09	①	①	①
CS M•201	Modules de sécurité multifonctions	135	High	1,44E-09	3	e	4
CS M•202	Modules de sécurité multifonctions	614	High	1,32E-09	3	e	4
CS M•203	Modules de sécurité multifonctions	103	High	1,61E-09	3	e	4
CS M•204	Modules de sécurité multifonctions	134	High	1,52E-09	3	e	4
CS M•205	Modules de sécurité multifonctions	373	High	2,19E-09	3	e	4
CS M•206	Modules de sécurité multifonctions	3314	High	1,09E-09	3	e	4
CS M•207	Modules de sécurité multifonctions	431	High	7,08E-09	3	e	4
CS M•208	Modules de sécurité multifonctions	633	High	7,02E-09	3	e	4
CS M•301	Modules de sécurité multifonctions	128	High	1,88E-09	3	e	4
CS M•302	Modules de sécurité multifonctions	535	High	1,57E-09	3	e	4
CS M•303	Modules de sécurité multifonctions	485	High	1,76E-09	3	e	4
CS M•304	Modules de sécurité multifonctions	98	High	2,05E-09	3	e	4
CS M•305	Modules de sécurité multifonctions	535	High	1,57E-09	3	e	4
CS M•306	Modules de sécurité multifonctions	100	High	1,86E-09	3	e	4
CS M•307	Modules de sécurité multifonctions	289	High	8,38E-09	3	e	4
CS M•308	Modules de sécurité multifonctions	548	High	7,27E-09	3	e	4
CS M•309	Modules de sécurité multifonctions	496	High	7,46E-09	3	e	4
CS M•310	Modules de sécurité multifonctions	288	High	3,46E-09	3	e	4
CS M•311	Modules de sécurité multifonctions	363	High	7,52E-09	3	e	4
CS M•312	Modules de sécurité multifonctions	380	High	8,20E-09	3	e	4
CS M•401	Modules de sécurité multifonctions	434	High	1,73E-09	3	e	4
CS M•402	Modules de sécurité multifonctions	478	High	7,24E-09	3	e	4
CS M•403	Modules de sécurité multifonctions	438	High	7,42E-09	3	e	4
CS M•406	Modules de sécurité multifonctions	473	High	1,54E-09	3	e	4

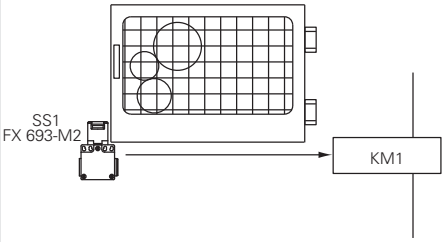
B_{10D} : Nombre d'opérations après lesquelles 10% des composants présentent une défaillance dangereuse
B_{10} : Nombre d'opérations après lesquelles 10% des composants présentent une défaillance
B_{10}/B_{10D} : Rapport entre les défaillances totales et les défaillances dangereuses.
$MTTF_D$: Mean Time To Failure Dangerous (temps moyen avant défaillance dangereuse) exprimé en années
DC : Diagnostic coverage (couverture du diagnostic)
PFH_D : Probability of Dangerous Failure per hour (Probabilité de défaillance dangereuse par heure)
SIL CL : Safety Integrity Level Claim Limit. SIL maximal possible selon EN IEC 62061
PL : Niveau de performance. PL selon EN ISO 13849-1

① = dépendant du module de base

EXEMPLE 1
Application : Contrôle des protecteurs

Norme de référence EN ISO 13849-1	
Catégorie de sécurité	**1**
Niveau de performance	**PL c**





Description de la fonction de sécurité
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 mis en évidence que le système n'est pas doté d'inertie c'est-à-dire que le moteur, après avoir coupé l'alimentation, s'arrête plus rapidement que la protection ne s'ouvre. L'analyse des risques a permis de mettre en évidence que le PL_r ciblé requis est PL c. On veut vérifier si le circuit de contrôle prévu, qui a une structure monocanal, a un PL supérieur ou égal à PL_r.
La position du protecteur est détectée par l'interrupteur avec actionneur séparé SS1 qui agit directement sur le contacteur KM1. Le contacteur KM1 qui contrôle les organes en mouvement est normalement actionné au moyen des boutons de démarrage et d'arrêt, mais l'analyse du cycle de fonctionnement a montré que la protection est également ouverte à chaque cycle de service. Il s'ensuit que le nombre d'opérations du télérupteur et de l'interrupteur de sécurité peut être considéré comme égal.
La structure du circuit est du type monocanal 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.
Aucune mesure n'est mise en œuvre pour vérifier les défaillances.

Données des dispositifs :
- SS1 (FX 693-M2) est un interrupteur à ouverture forcée (selon l'annexe K de la norme EN 60947-5-1). L'interrupteur est un dispositif bien éprouvé selon le tableau D.4 de la norme EN ISO 13849-2. La valeur de B_{10D} du dispositif est fournie par le constructeur et est égale à 2.000.000 manœuvres.
- KM1 est un contacteur utilisé à charge nominale et est un composant bien éprouvé en accord avec tableau D.4 de l'EN ISO 13849-2. Sa valeur B_{10D} est égale à 1.300.000 manœuvres, valeur dérivée des tableaux de la norme (voir tableau C.1 de l'EN ISO 13849-1).

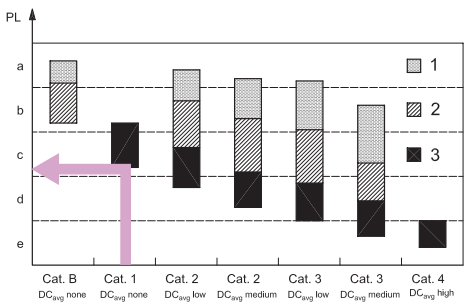
Hypothèse de fréquence d'utilisation
- On suppose que la machine est utilisée au plus 365 jours par an, pour trois équipes de 8 heures avec un temps de cycle de 600 secondes. Le nombre d'opérations par an pour l'interrupteur est donc égal à N_{op} = (365x24x3.600)/600 = 52.560.
- On suppose l'actionnement du bouton de démarrage toutes les 300 secondes. Le nombre d'opérations par an est donc égal au maximum à n_{op}/an = 105.120
- Le contacteur KM1 sera actionné pour la marche-arrêt normale de la machine et pour le redémarrage suite à l'ouverture d'un protecteur. n_{op}/an = 52.560+105.120 = 157.680

Calcul de $MTTF_D$
L'$MTTF_D$ de l'interrupteur SS1 est égal à : $MTTF_D = B_{10D} /(0,1 \times n_{op}) = 2000000/(0,1 \times 52560) = 381$ ans
L'$MTTF_D$ du contacteur KM1 est égal à : $MTTF_D = B_{10D} /(0,1 \times n_{op}) = 1.300.000/(0,1 \times 157680) = 82$ ans
Il s'ensuit que le $MTTF_D$ du circuit monocanal est égal à : 1/(1/381+1/82) = 67 ans

Couverture du diagnostic DCavg
Aucune mesure n'est mise en œuvre pour vérifier les défaillances et donc la couverture du diagnostic est nulle, condition admise pour le circuit examiné qui est de catégorie 1.

Défaillance de cause commune CCF
Pour un circuit de catégorie 1, il n'est pas nécessaire de calculer le paramètre CCF.

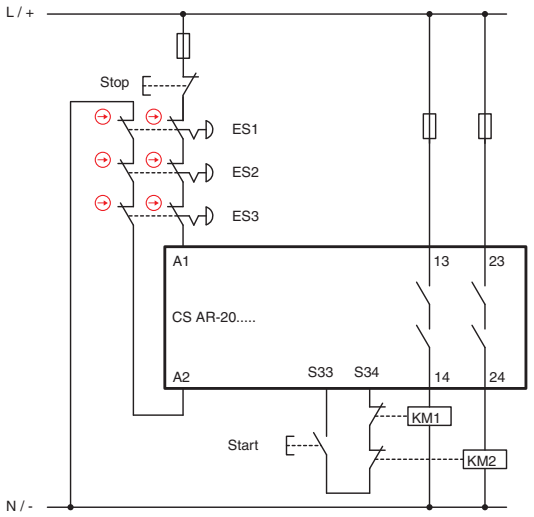
Vérification du PL
Le tableau ou la figure 5 de la norme permet de vérifier comment, pour un circuit de catégorie 1 et de $MTTF_D$ = 95 ans, le PL résultant du circuit de contrôle est PL c. Le PL_r ciblé est donc atteint.

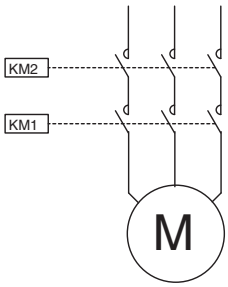


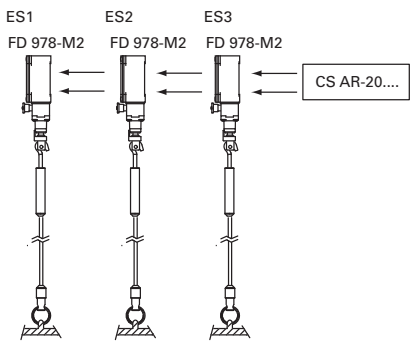
Toutes les informations et les exemples d'application, y compris les schémas de raccordement, illustrés dans cette documentation sont de nature purement descriptive.
C'est l'utilisateur qui a la responsabilité de s'assurer que les produits choisis et appliqués sont utilisés comme il est prescrit dans les normes afin qu'ils ne puissent porter préjudice ni aux biens ni aux personnes.

EXEMPLE 2
Application : Contrôle arrêts d'urgence

Norme de référence EN ISO 13849-1	
Catégorie de sécurité	**3**
Niveau de performance	**PL e**







Description de la fonction de sécurité
L'actionnement d'un des dispositifs d'urgence provoque l'intervention du module de sécurité et des deux contacteurs KM1 et KM2. Le signal des dispositifs ES1, ES2, ES3 est lu de façon redondante par le module de sécurité CS. Les contacteurs KM1 et KM2 (avec contacts forcés) sont aussi contrôlés par CS via le circuit de rétroaction.

Données des dispositifs :
- ES1, ES2, ES3 (FD 978-M2) sont des interrupteurs à câble pour arrêts d'urgence à ouverture forcée. La valeur de B_{10D} est égale à 2.000.000
- KM1, KM2 sont des contacteurs utilisés à charge nominale. La valeur B_{10D} est égale à 1.300.000 (voir tableau C.1 d'EN ISO 13849-1)
- CS est un module de sécurité (CS AR-20) avec $MTTF_D$ = 225 ans et DC = High
- L'architecture du circuit est à double canal en catégorie 3

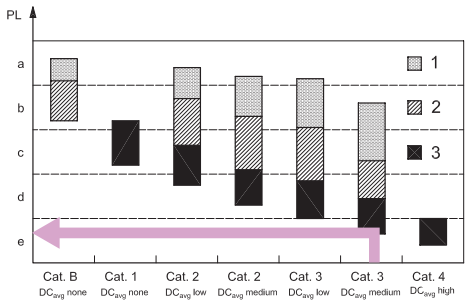
Hypothèse de fréquence d'utilisation
- 2 fois par mois nop/an = 24
- Actionnement du bouton de démarrage : 4 fois par jour
- En supposant 365 jours de travail, les contacteurs interviennent 4 x 365 + 24 = 1484 fois/an
- Les interrupteurs seront actionnés avec la même fréquence.
- On ne prévoit pas que plusieurs boutons puissent être pressés simultanément.

Calcul de $MTTF_D$
- $MTTF_{D\ ES1,ES2,ES3}$ = 833.333 ans
- $MTTF_{D\ KM1,KM2}$ = 8760 ans
- $MTTF_{D\ CS}$ = 225 ans
- $MTTF_{D\ ch1}$ = 219 ans. La valeur est limitée à 100 ans. Les canaux sont symétriques, donc $MTTF_D$ =100 ans (High)

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

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

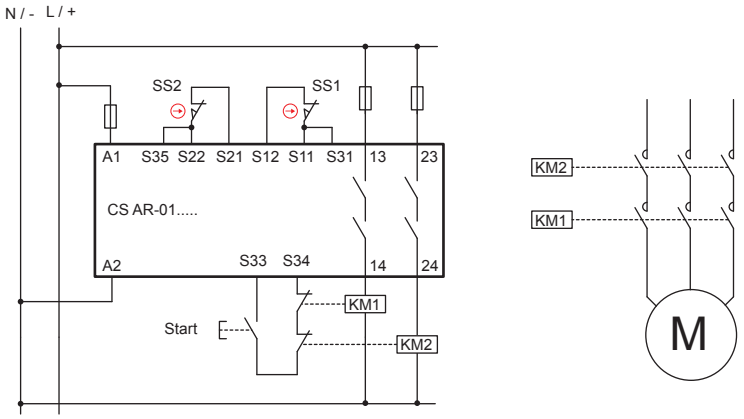
Vérification du PL
Un circuit de catégorie 3 avec $MTTF_D$ = High et DC_{avg} = High peut atteindre un PL e.

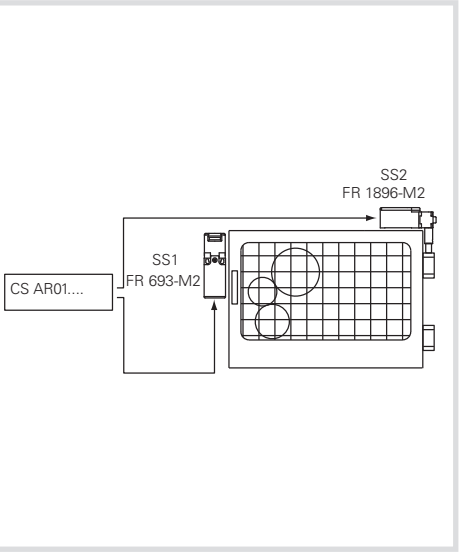


Toutes les informations et les exemples d'application, y compris les schémas de raccordement, illustrés dans cette documentation sont de nature purement descriptive.
C'est l'utilisateur qui a la responsabilité de s'assurer que les produits choisis et appliqués sont utilisés comme il est prescrit dans les normes afin qu'ils ne puissent porter préjudice ni aux biens ni aux personnes.

EXEMPLE 3
Application : Contrôle des protecteurs

Norme de référence EN ISO 13849-1	
Catégorie de sécurité	**4**
Niveau de performance	**PL e**





Description de la fonction de sécurité
L'ouverture du protecteur provoque l'intervention des interrupteurs SS1 et SS2 et donc du module de sécurité et des deux contacteurs KM1 et KM2.
Le signal des dispositifs SS1 et SS2 est contrôlé de façon redondante par le module de sécurité CS.
Les interrupteurs ont un principe de fonctionnement différent.
Les contacteurs KM1 et KM2 (avec contacts forcés) sont aussi contrôlés par CS via le circuit de rétroaction.

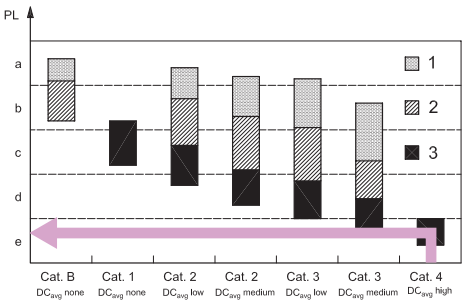
Données des dispositifs :
- SS1 (FR 693-M2) est un interrupteur à ouverture forcée. La valeur de B_{10D} est égale à 2.000.000
- SS2 (FR 1896-M2) est un interrupteur pour charnières à ouverture forcée. B_{10D} = 5.000.000
- KM1, KM2 sont des contacteurs utilisés à charge nominale. B_{10D} = 1.300.000 (voir tableau C.1 d'EN ISO 13849-1)
- CS sont des modules de sécurité (CS AR-01) avec $MTTF_D$=227 ans et DC = High

Hypothèse de fréquence d'utilisation
365 jours/an, 16 h/jour, 1 intervention toutes les 4 minutes (240 s). n_{op}/an = 87.600.

Calcul de $MTTF_D$
- $MTTF_{D\ SS1}$ = 228 ans
- $MTTF_{D\ SS2}$ = 571 ans
- $MTTF_{D\ KM1,KM2}$ = 148 ans
- $MTTF_{D\ CS}$ = 227 ans
- $MTTF_{D\ CH1}$ = 64 ans (SS1,CS,KM1)
- $MTTF_{D\ CH2}$ = 77 ans (SS2,CS,KM2)
- $MTTF_D$: en symétrisant les deux canaux, on obtient $MTTF_D$ = 70,7 ans (High)

Couverture du diagnostic DC_{avg}
- SS1 et SS2 ont DC=99% car les contacts de SS1 et SS2 sont contrôlés par CS et ont des principes de fonctionnement différents.
- Les contacts de KM1 et KM2 sont contrôlés par CS via le circuit de rétroaction. DC = 99% (High)
- CS AR-01 a à l'intérieur un circuit redondant et auto-surveillé. DC = High
- DC_{avg}= High

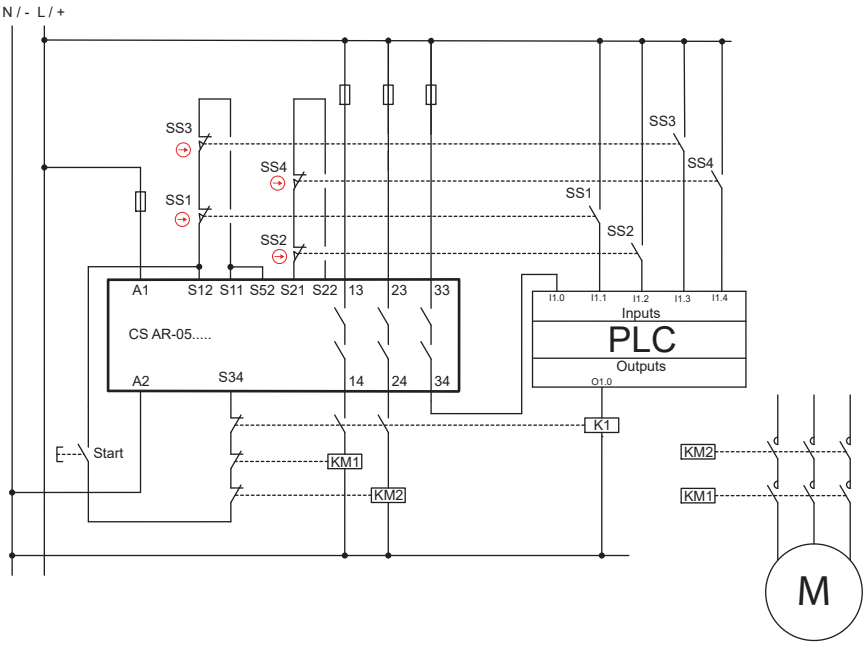
Vérification du PL
Un circuit de catégorie 4 avec $MTTF_D$ =72,1 ans et DC_{avg} = High correspond à un PL e.

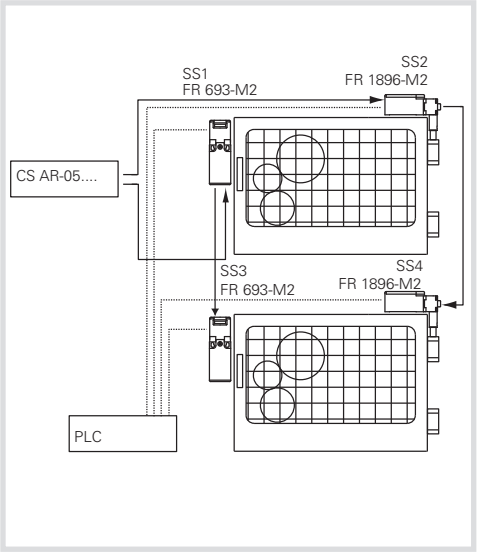


Toutes les informations et les exemples d'application, y compris les schémas de raccordement, illustrés dans cette documentation sont de nature purement descriptive.
C'est l'utilisateur qui a la responsabilité de s'assurer que les produits choisis et appliqués sont utilisés comme il est prescrit dans les normes afin qu'ils ne puissent porter préjudice ni aux biens ni aux personnes.

EXEMPLE 4
Application : Contrôle des protecteurs

Norme de référence	EN ISO 13849-1
Catégorie de sécurité	**4**
Niveau de performance	**PL e**





Description de la fonction de sécurité
L'ouverture d'un protecteur provoque l'intervention des interrupteurs SS1, SS2 dans la première protection et SS3, SS4 dans la deuxième ; les interrupteurs actionnent 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.
Les contacteurs KM1 et KM2 (avec contacts forcés) sont aussi contrôlés par CS via le circuit de rétroaction.

Données des dispositifs :
- SS1, SS3 (FR 693-M2) sont des interrupteurs à ouverture forcée. La valeur de B_{10D} est égale à 2.000.000
- SS2, SS4 (FR 1896-M2) sont des interrupteurs pour charnières à ouverture forcée. B_{10D} = 5.000.000
- KM1, KM2 sont des contacteurs utilisés à charge nominale. La valeur de B_{10D} est égale à 1.300.000 (voir tableau C.1 d'EN ISO 13849-1)
- CS est un module de sécurité (CS AR-05) avec $MTTF_D$ = 152 ans et DC = High

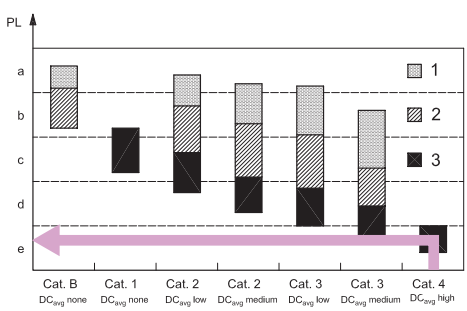
Hypothèse de fréquence d'utilisation
- 4 fois par heure, 24 heures/jour et 365 jours/an, donc n_{op}/an = 35.040
- Les contacteurs interviennent pour un nombre double d'opérations = 70.080

Calcul de $MTTF_D$
- $MTTF_{D\ SS1,SS3}$ = 571 ans ; $MTTF_{D\ SS2,SS4}$ = 1.427 ans
- $MTTF_{D\ KM1,KM2}$ = 185 ans
- $MTTF_{D\ CS}$ = 152 ans
- $MTTF_{D\ Ch1}$ = 73 ans (SS1, CS, KM1) / (SS3, CS, KM1)
- $MTTF_{D\ Ch2}$ = 79 ans (SS2, CS, KM2) / (SS4, CS, KM2)
- $MTTF_D$: en symétrisant les deux canaux, on obtient $MTTF_D$ = 76 ans (High)

Couverture du diagnostic DC_{avg}
- Les contacts de KM1, KM2 sont contrôlés par CS via le circuit de rétroaction. DC = 99%
- Les contacts auxiliaires des interrupteurs sont tous contrôlés par le PLC. DC = 99%
- Le module CS AR-05 a une DC = High
- La couverture du diagnostic pour tous les deux canaux est de 99% (High)

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

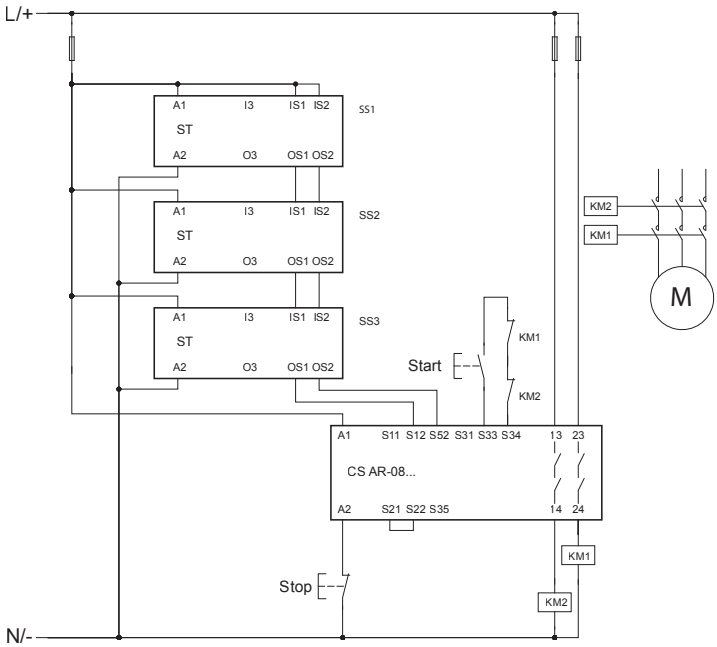
Vérification du PL
- Un circuit de catégorie 4 avec $MTTF_D$ = 88,6 ans (High) et DC_{avg} = High correspond à un PL e.

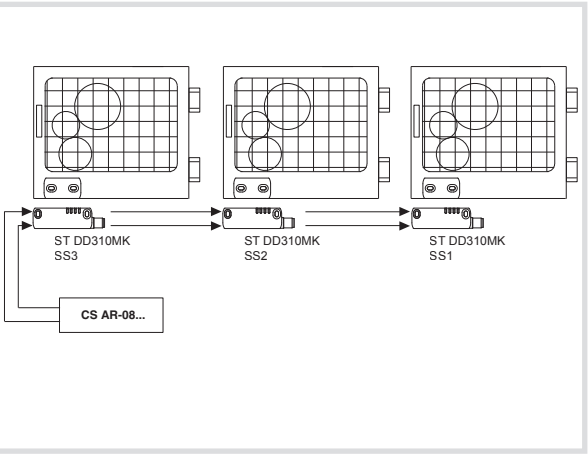


Toutes les informations et les exemples d'application, y compris les schémas de raccordement, illustrés dans cette documentation sont de nature purement descriptive.
C'est l'utilisateur qui a la responsabilité de s'assurer que les produits choisis et appliqués sont utilisés comme il est prescrit dans les normes afin qu'ils ne puissent porter préjudice ni aux biens ni aux personnes.

EXEMPLE 5
Application : Contrôle des protecteurs

Norme de référence EN ISO 13849-1	
Catégorie de sécurité	**4**
Niveau de performance	**PL e**

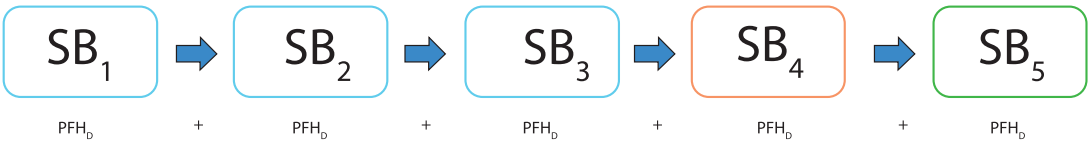




Description de la fonction de sécurité
L'ouverture des protecteurs provoque l'intervention des capteurs SS1 sur le premier protecteur, de SS2 sur le second et de SS3 sur le troisième ; les capteurs activent le module de sécurité CS AR-08 et les deux contacteurs KM1 et KM2. Les contacteurs KM1 et KM2 (avec contacts forcés) sont contrôlés par CS AR-08 via le circuit de rétroaction.

Données des dispositifs
SS1, SS2, SS3 sont des capteurs de la série ST avec technologie RFID codifiés. PFH_D = 1,20E-11, PL = e
CS AR-08 est un module de sécurité. PFH_D = 9,73E-11, PL = e
KM1, KM2 sont des contacteurs utilisés à charge nominale. B_{10D} = 1.300.000 (voir tableau C.1 d'EN ISO 13849-1)

Hypothèse de fréquence d'utilisation
Chaque porte est ouverte toutes les 2 minutes, 16 heures par jour et 365 jours par an, donc n_{op} = 175.200
Définition du SRP/CS et des sous-systèmes
La SRP/CS est constituée de 5 sous-systèmes (SB) :
SB1, 2, 3 représentent trois capteurs RFID de la série ST
SB4 représente le module de sécurité CS AR-08
SB5 représente deux télérupteurs KM1 et KM2 en architecture redondante (cat. 4)



Calcul de PFH_D pour SB5
$MTTF_D$ KM1,KM2 = 74,2 ans.
DC = 99%, les contacts de KM1 et KM2 sont contrôlés par le module de sécurité via le circuit de rétroaction.
On suppose une valeur supérieure à 65 pour le paramètre CCF (selon l'annexe F de l'EN ISO 13849-1).
Un circuit de catégorie 4 avec $MTTF_D$ = 74,2 ans (élevée) et une couverture élevée du diagnostic (DC = 99%) correspond à une probabilité de défaillance PFH_D = 3,4E-08 et à un PL e.

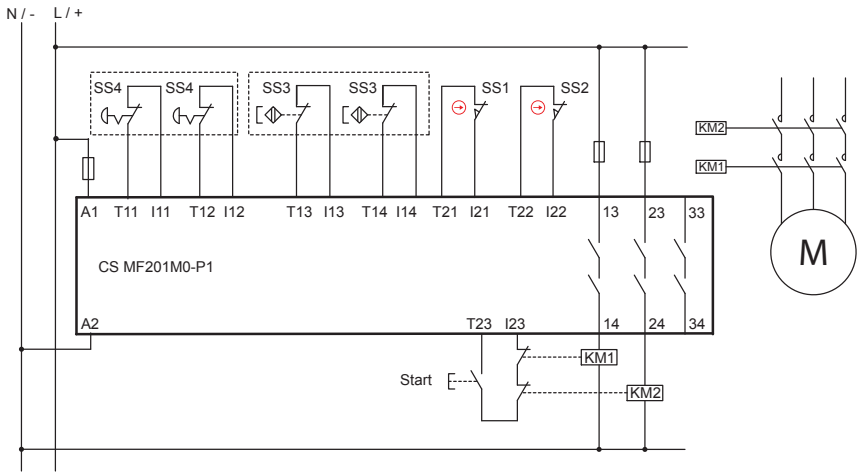
Calcul de la PFH_D totale du SRP/CS
$PFH_{DTOT} = PFH_{DSB1} + PFH_{DSB2} + PFH_{DSB3} + PFH_{DSB4} + PFH_{DSB5}$ = 3,5E-08
Cela correspond à un PL e.

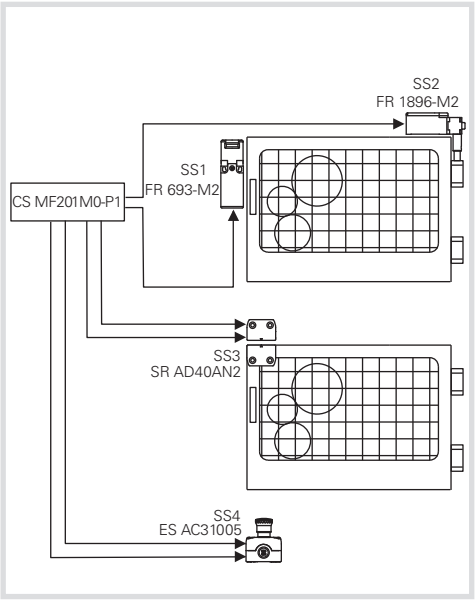
Exemple de calcul effectué avec le logiciel SISTEMA, téléchargeable gratuitement sur le site www.pizzato.com

Toutes les informations et les exemples d'application, y compris les schémas de raccordement, illustrés dans cette documentation sont de nature purement descriptive.
C'est l'utilisateur qui a la responsabilité de s'assurer que les produits choisis et appliqués sont utilisés comme il est prescrit dans les normes afin qu'ils ne puissent porter préjudice ni aux biens ni aux personnes.

EXEMPLE 6
Application : Contrôle des protecteurs

Norme de référence EN ISO 13849-1	
Catégorie de sécurité	4
Niveau de performance	PL e





Description de la fonction de sécurité
L'ouverture d'un protecteur provoque l'intervention des interrupteurs SS1, SS2 dans la première protection et du capteur SS3 dans la deuxième ; les interrupteurs actionnent le module de sécurité et les deux contacteurs KM1 et KM2.
Les signaux des dispositifs SS1, SS2 et SS3 sont contrôlés de façon redondante par le module de sécurité CS MF.
Il y a aussi un bouton d'arrêt d'urgence qui est également relié au module de sécurité par un double canal.
Les contacteurs KM1 et KM2 (avec contacts forcés) sont aussi contrôlés par CS MF via le circuit de rétroaction.

Données des dispositifs :
- SS1 (FR 693-M2) est un interrupteur à ouverture forcée. B_{10D} = 2.000.000
- SS3 (FR 1896-M2) est un interrupteur pour charnières à ouverture forcée. B_{10D} = 5.000.000
- SS3 (SR AD40AN2) est un capteur magnétique de sécurité. B_{10D} = 20.000.000
- SS4 (ES AC31005) est un boîtier avec bouton d'arrêt d'urgence (E2 1PERZ4531) avec 2 contacts NC. B_{10D} = 600.000
- KM1, KM2 sont des contacteurs utilisés à charge nominale. B_{10D} = 1.300.000 (voir tableau C.1 d'EN ISO 13849-1)
- CS MF201M0-P1 est un module de sécurité avec $MTTF_D$ = 842 ans et DC = 99%

Hypothèse de fréquence d'utilisation
- Chaque porte est ouverte 2 fois par heure, 16 heures/jour et 365 jours/an, donc n_{op}/an = 11.680
- On suppose que le bouton d'arrêt d'urgence est actionné au plus 1 fois par jour, n_{op}/an = 365
- Les contacteurs interviennent pour un nombre double d'opérations = 23.725

Calcul de $MTTF_D$

Protecteur SS1/SS2
- $MTTF_{D\ SS1,SS3}$ = 1.712 ans
- $MTTF_{D\ SS2,SS4}$ = 4.281 ans
- $MTTF_{D\ KM1,KM2}$ = 548 ans
- $MTTF_{D\ CS}$ = 842 ans
- $MTTF_{D\ CH1}$ = 278 ans (SS1, CS, KM1)
- $MTTF_{D\ CH2}$ = 308 ans (SS2, CS, KM2)
- $MTTF_D$: en symétrisant les deux canaux, on obtient $MTTF_D$ = 293 ans

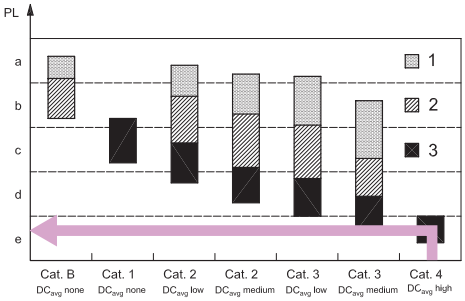
Protecteur SS3
- $MTTF_{D\ SS3}$ = 17.123 ans
- $MTTF_{D\ KM1,KM2}$ = 548 ans
- $MTTF_{D\ CS}$ = 842 ans
- $MTTF_D$ = 325 ans

Bouton d'arrêt d'urgence SS4
- $MTTF_{D\ SS4}$ = 16.438 ans
- $MTTF_{D\ KM1,KM2}$ = 548 ans
- $MTTF_{D\ CS}$ = 842 ans
- $MTTF_D$ = 325 ans

Couverture du diagnostic DC_{avg}
- Les contacts de KM1 et KM2 sont contrôlés par CS MF via le circuit de rétroaction. DC = 99%
- Il est possible de détecter toutes les défaillances dans la série des dispositifs SS1, SS2 et SS3. DC = 99%
- Le module CS MF201M0-P1 a une DC = 99%
- On suppose une couverture du diagnostic de 99% (High)

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

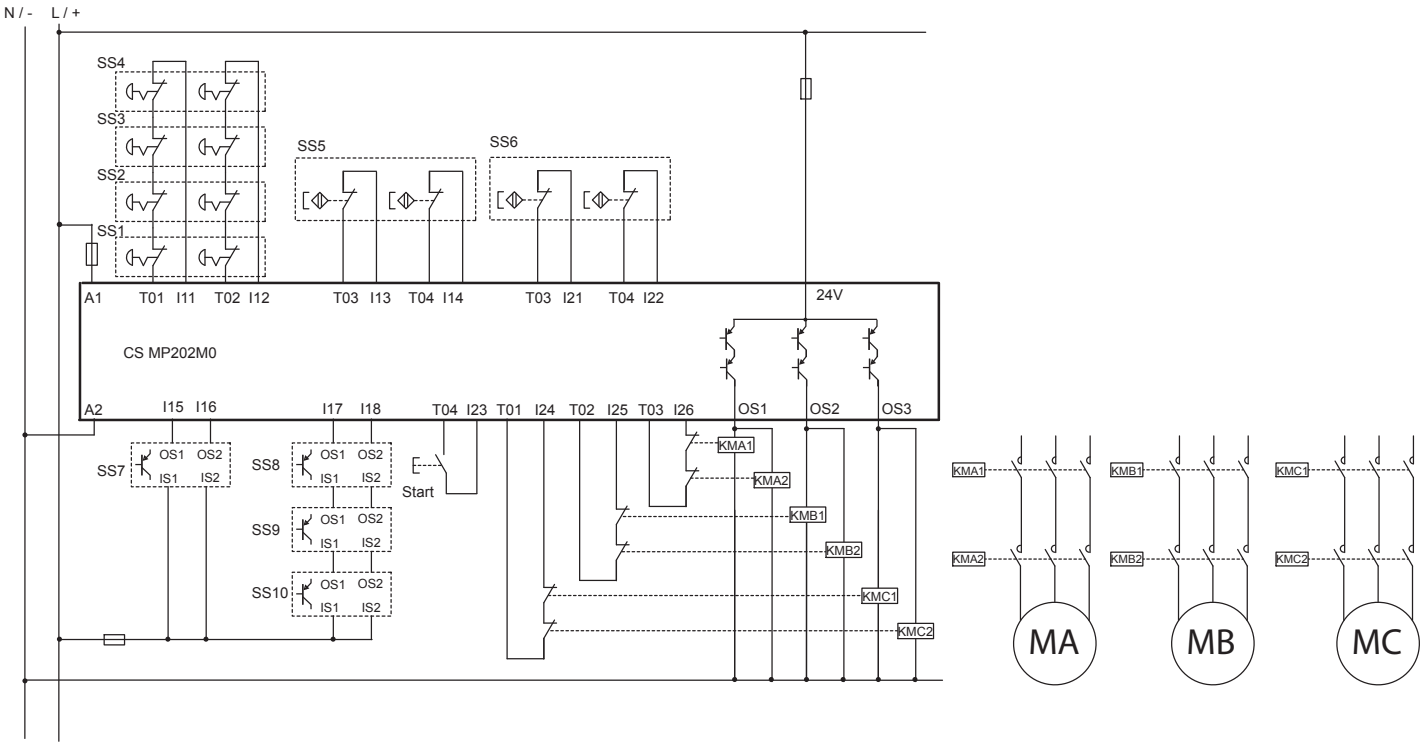
Vérification du PL
- Un circuit de catégorie 4 avec $MTTF_D \geq 30$ ans (High) et DC_{avg} = High correspond à un PL e.
- Les fonctions de sécurité liées aux protecteurs SS1/SS2, SS3 et au bouton d'arrêt d'urgence sont de PL e.

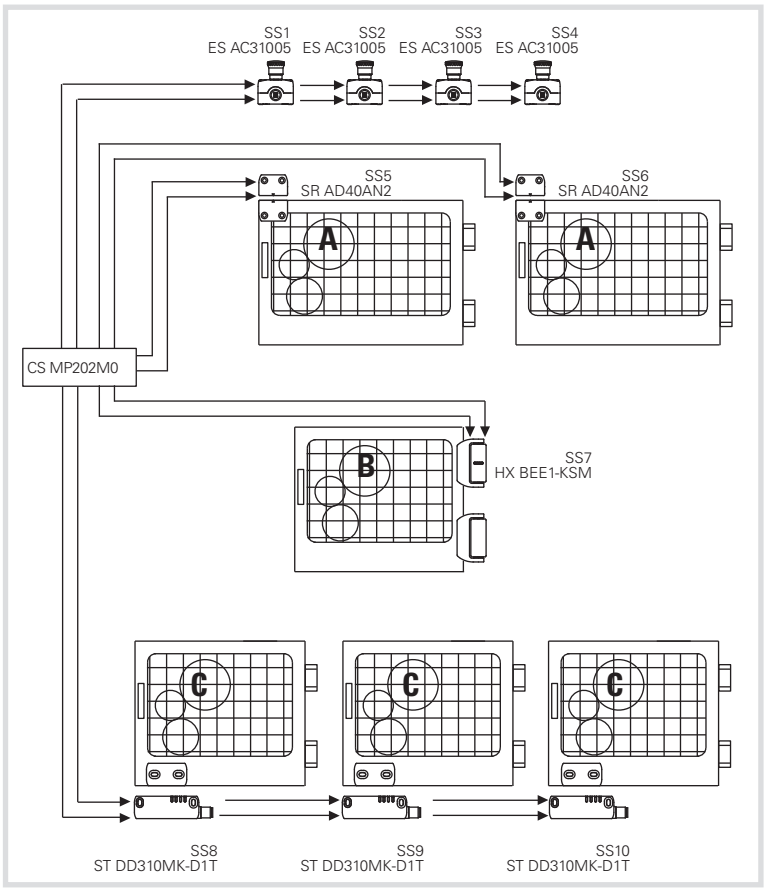


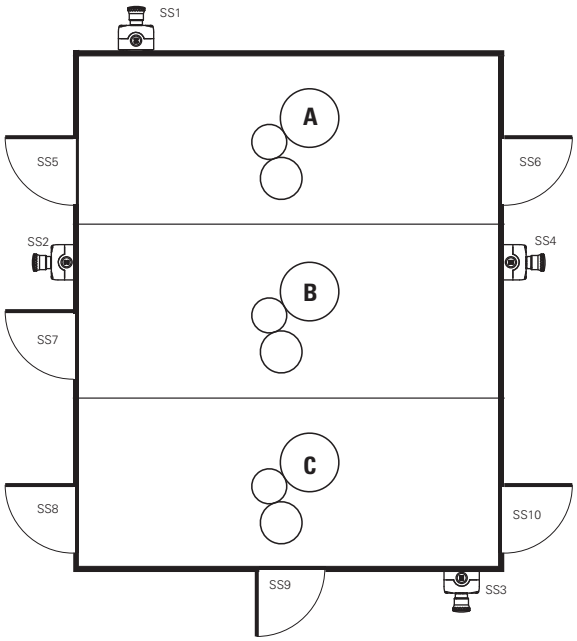
Toutes les informations et les exemples d'application, y compris les schémas de raccordement, illustrés dans cette documentation sont de nature purement descriptive.
C'est l'utilisateur qui a la responsabilité de s'assurer que les produits choisis et appliqués sont utilisés comme il est prescrit dans les normes afin qu'ils ne puissent porter préjudice ni aux biens ni aux personnes.

EXEMPLE 7
Application : Contrôle des protecteurs

Norme de référence EN ISO 13849-1	
Catégorie de sécurité	**4**
Niveau de performance	**PL e**







Description de la fonction de sécurité

Une machine est divisée en 3 zones distinctes. L'accès à chaque zone est contrôlé par des protecteurs et une série de 4 boutons d'arrêts d'urgence est présente.
L'action d'un bouton d'arrêt d'urgence provoque l'intervention du module de sécurité CS MP et des contacteurs forcés KMA1/2, KMB1/2, KMC1/2, en arrêtant tous les moteurs.
L'ouverture d'un protecteur dans la zone A provoque l'intervention des dispositifs SS5 ou SS6 qui actionnent le module de sécurité CS MP et les contacteurs KMA1 et KMA2, en arrêtant ainsi le moteur MA. Les dispositifs SS5, SS6 sont connectés de façon séparée et par un double canal au module de sécurité CS MP.
L'ouverture du protecteur dans la zone B provoque l'intervention du dispositif SS7 qui actionne le module de sécurité CS MP et les deux contacteurs KMB1 et KMB2, en arrêtant ainsi le moteur MB. La charnière SS7 a deux sorties OSSD et est contrôlée de façon redondante par le module de sécurité CS MP.
L'ouverture d'un protecteur dans la zone C provoque l'intervention des dispositifs SS8, SS9 ou SS10 ; les dispositifs actionnent le module de sécurité et les deux contacteurs KMC1 et KMC2, en arrêtant ainsi le moteur MC. Les capteurs SS8, SS9 et SS10 sont reliés les uns aux autres par les sorties OSSD et sont contrôlés de façon redondante par le module de sécurité CS MP.

Données des dispositifs

- SS1, SS2, SS3 et SS4 (ES AC31005) sont des boutons d'arrêt d'urgence (E2 1PERZ4531) avec 2 contacts NC. B_{10D} = 600.000
- SS5 et SS6 (SR AD40AN2) sont des capteurs magnétiques de sécurité. B_{10D} = 20.000.000
- SS7 (HX BEE1-KSM) est une charnière de sécurité avec sorties OSSD. $MTTF_D$ = 4077 ans / DC = 99%
- SS8, SS9 et SS10 (ST DD310MK-D1T) sont des capteurs de sécurité avec technologie RFID et sorties OSSD. $MTTF_D$= 4077 ans / DC=99%
- KMA, KMB et KMC sont des contacteurs utilisés à charge nominale. B_{10D} = 1.300.000 (voir tableau C.1 d'EN ISO 13849-1)
- CS MP202M0 est un module de sécurité avec $MTTF_D$ = 2035 ans / DC = 99%

Hypothèse de fréquence d'utilisation

- Chaque porte de la zone A est ouverte 2 fois par heure, 16 heures/jour et 365 jours/an, donc n_{op}/an = 11.680. Les contacteurs interviennent pour un nombre double d'opérations = 23.360
- La porte de la zone B est ouverte 4 fois par heure, 16 heures/jour et 365 jours/an, donc n_{op}/an = 23.360. Les contacteurs interviennent pour un nombre d'opérations = 23.360
- Chaque porte de la zone C est ouverte 1 fois par heure, 16 heures/jour et 365 jours/an, donc n_{op}/an = 5.840. Les contacteurs interviennent pour un nombre d'opérations = 17.520
- On suppose que le bouton d'arrêt d'urgence est actionné au plus une fois par semaine, n_{op}/an = 52
- Exclusion de défaillances : on exclut la possibilité de court-circuit entre +24V et les contacteurs, car on suppose que les paires de contacteurs, qui sont connectées en parallèle aux sorties de sécurité respectives, sont câblées en permanence à l'intérieur du tableau électrique (voir tableau D.4, D.5.2 d'EN ISO 13849-2).

Calcul de $MTTF_D$

Boutons d'arrêt d'urgence
- $MTTF_D$ SS1/SS2/SS3/SS4 = 115.384 ans
- $MTTF_D$ CS = 2035 ans
- $MTTF_D$ KMC1,KMC2 = 742 ans
- $MTTF_D$ e-stop = 541 ans

Protecteurs zone A
- $MTTF_D$ SS5/SS6 = 17.123 ans
- $MTTF_D$ CS = 2035 ans
- $MTTF_D$ KMA1,KMA2 = 556 ans
- $MTTF_D$ A = 425 ans (SS5/SS6,CS,KMA)

Protecteur zone B
- $MTTF_D$ SS7 = 4.077 ans
- $MTTF_D$ CS = 2035 ans
- $MTTF_D$ KMB1,KMB2 = 556 ans
- $MTTF_D$ B = 394 ans (SS7,CS,KMB)

Protecteurs zone C
- $MTTF_D$ SS8/SS9/SS10 = 4.077 ans
- $MTTF_D$ CS = 2035 ans
- $MTTF_D$ KMC1,KMC2 = 742 ans
- $MTTF_D$ C = 479 ans (SS8/SS9/SS10,CS,KMC)

Couverture du diagnostic DC_{avg}

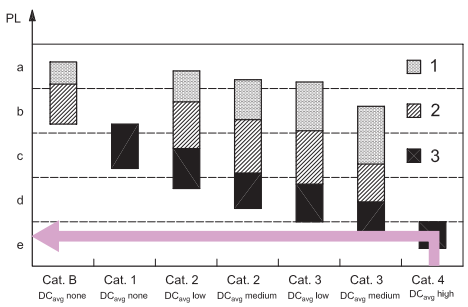
- Les contacts de KMA, KMB et KMC sont contrôlés par CS MP via le circuit de rétroaction. DC = 99%
- Il est possible de détecter toutes les défaillances des dispositifs. DC = 99%
- Le module CS MP202M0 a une DC = 99%
- On obtient une couverture du diagnostic de 99% (High) pour chaque fonction

Défaillance de cause commune CCF

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

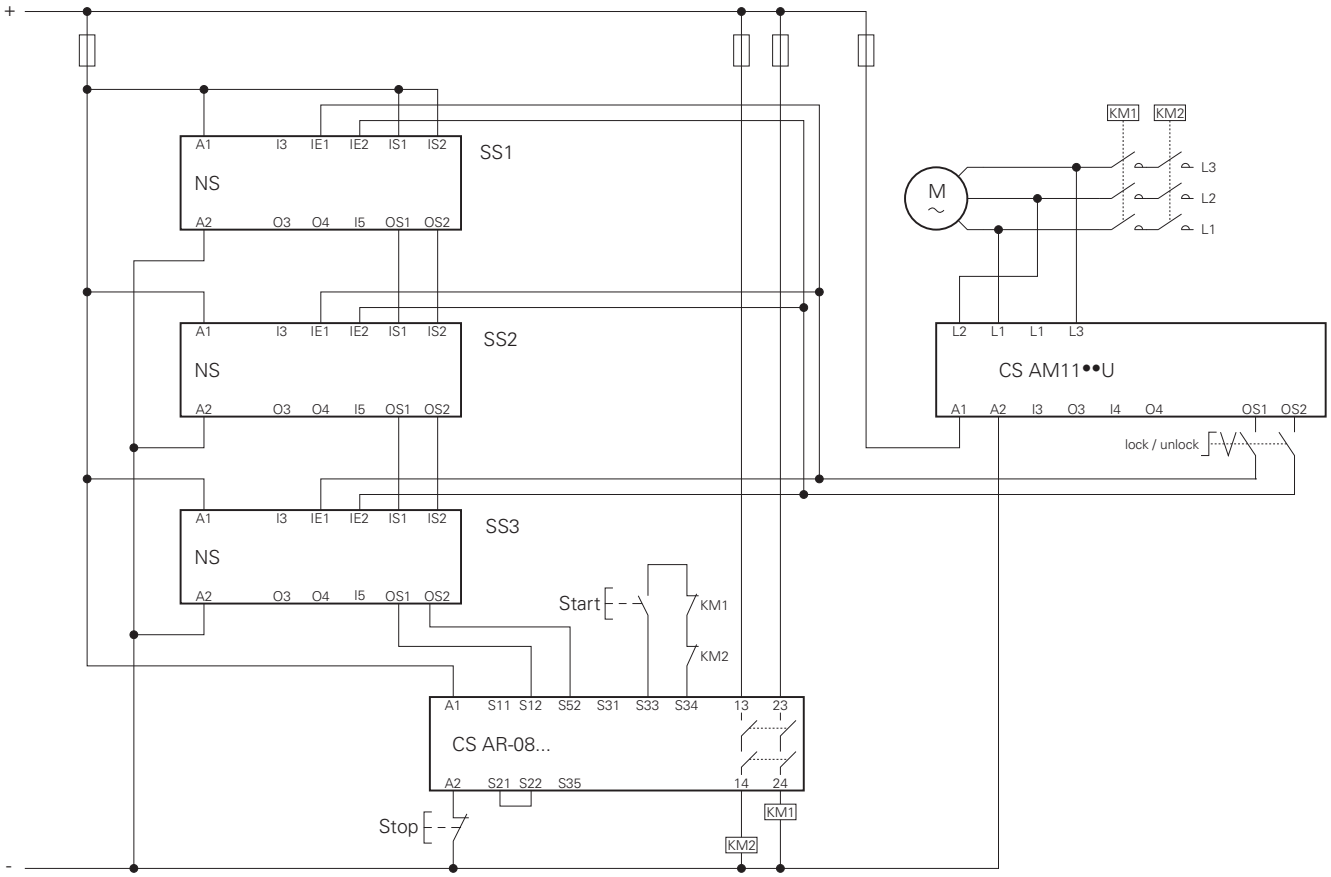
Vérification du PL

- Un circuit de catégorie 4 avec $MTTF_D \geq 30$ ans (High) et DC_{avg} = High correspond à un PL e.
- Toutes les fonctions de sécurité liées aux protecteurs et aux boutons d'arrêt d'urgence sont de PL e.

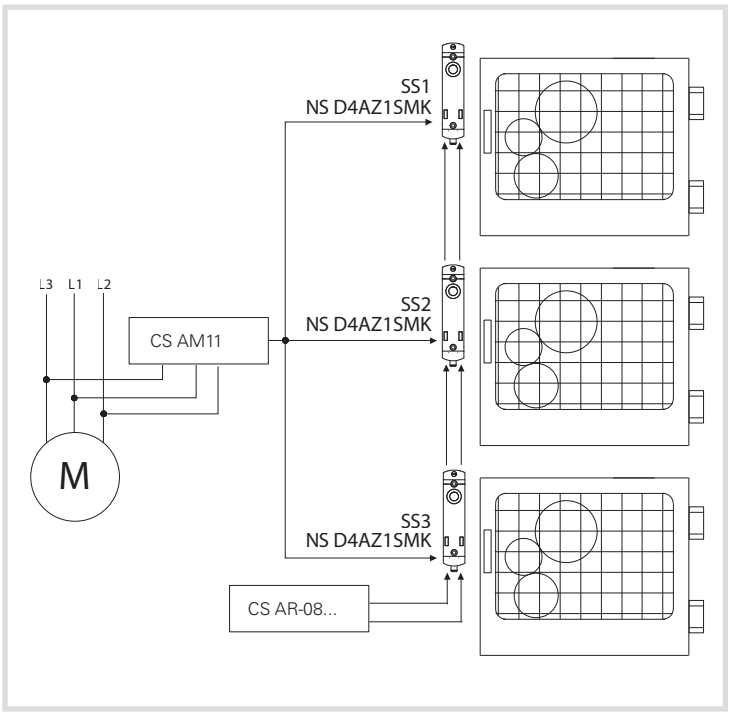


Toutes les informations et les exemples d'application, y compris les schémas de raccordement, illustrés dans cette documentation sont de nature purement descriptive.
C'est l'utilisateur qui a la responsabilité de s'assurer que les produits choisis et appliqués sont utilisés comme il est prescrit dans les normes afin qu'ils ne puissent porter préjudice ni aux biens ni aux personnes.

EXEMPLE 8
Application : Contrôle des protecteurs



Norme de référence EN ISO 13849-1	
Niveau de performance fonction de sécurité 1	**PL e**
Niveau de performance fonction de sécurité 2	**PL e**

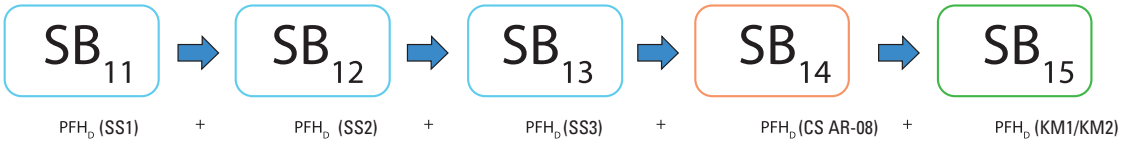


Description de la fonction de sécurité
Les dispositifs d'interverrouillage SS1, SS2 et SS3 réalisent deux fonctions de sécurité : surveillance de l'état « protecteur verrouillé » et verrouillage du protecteur.
Une fois les protecteurs déverrouillés, les trois capteurs font intervenir le module de sécurité et les deux contacteurs KM1 et KM2. Les contacteurs KM1 et KM2 (avec contacts forcés) sont contrôlés par CS AR-08 via le circuit de rétroaction.
La commande de verrouillage dans les trois dispositifs SS1, SS2 et SS3 est maintenue jusqu'au moment où le module de détection du moteur arrêté CS AM11 détecte l'arrêt effectif du mouvement.

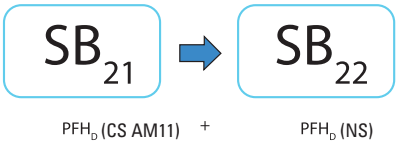
Données des dispositifs
SS1, SS2, SS3 sont des dispositifs d'interverrouillage codifiés de la série NS avec technologie RFID et avec un dispositif de verrouillage du protecteur. Fonction de détection de la protection verrouillée PFH_D = 1,23E-09 PL =e, fonction de commande de retenue PFH_D = 2,04E-10 PL = e.
CS AR-08 est un module de sécurité, PFH_D = 9,73E-11, PL = e.
CS AM11 est un module de sécurité pour la détection d'arrêt moteur, PFH_D = 1,00E-09, PL e.
KM1, KM2 sont des contacteurs utilisés à charge nominale. B_{10D} = 1.300.000 (voir tableau C.1 d'EN ISO 13849-1)

Hypothèse de fréquence d'utilisation
Chaque porte est ouverte toutes les 10 minutes, 16 heures par jour et 365 jours par an, donc n_{op}/an = 35.040

Définition du SRP/CS et des sous-systèmes
Cet exemple d'application est caractérisé par deux fonctions de sécurité :
1. Fonction d'arrêt liée à la sécurité activée par une mesure de protection
2. Fonction de maintien du protecteur verrouillé avec moteur M en mouvement
La fonction de sécurité 1 est réalisée par un SRP/CS composé de 5 sous-systèmes (SB) :
- SB11, 12, 13 représentent trois dispositifs d'interverrouillage RFID des séries NS, SS1, SS2 et SS3
- SB14 représente le module de sécurité CS AR-08
- SB15 représente deux télérupteurs KM1 et KM2 en architecture redondante (cat. 4)



La fonction de sécurité 2 est réalisée par 2 sous-systèmes (SB) :
- SB21 représente le module de sécurité de détection d'arrêt moteur CS AM11
- SB22 représente trois dispositifs d'interverrouillage RFID de la série NS



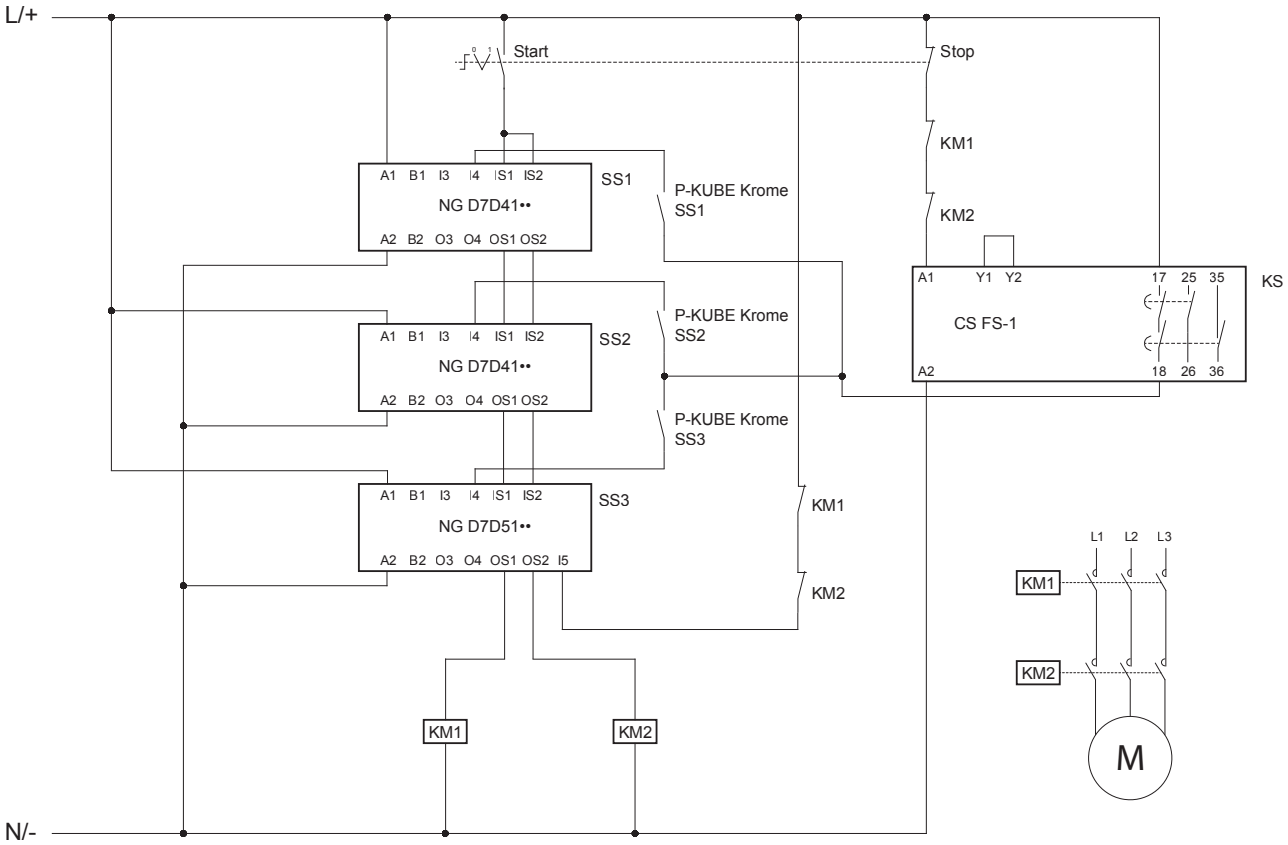
Calcul de PFH_D pour SB15
$MTTF_D$ KM1,KM2 = 371 ans.
DC = 99%, les contacts de KM1 et KM2 sont contrôlés par le module de sécurité via le circuit de rétroaction.
On suppose une valeur supérieure à 65 pour le paramètre CCF (selon l'annexe F de l'EN ISO 13849-1).
Un circuit de catégorie 4 avec $MTTF_D$ = 371 et une couverture élevée du diagnostic (DC = 99%) correspond à une probabilité de défaillance PFH_D = 6,3E-09 et à un PL e.

Calcul de la PFH_D totale du SRP/CS fonction de sécurité 1 (interverrouillage)
$PFH_{DTOT} = PFH_{DSB11} + PFH_{DSB12} + PFH_{DSB13} + PFH_{DSB14} + PFH_{DSB15}$ = 1E-08
cela correspond à un PL e.

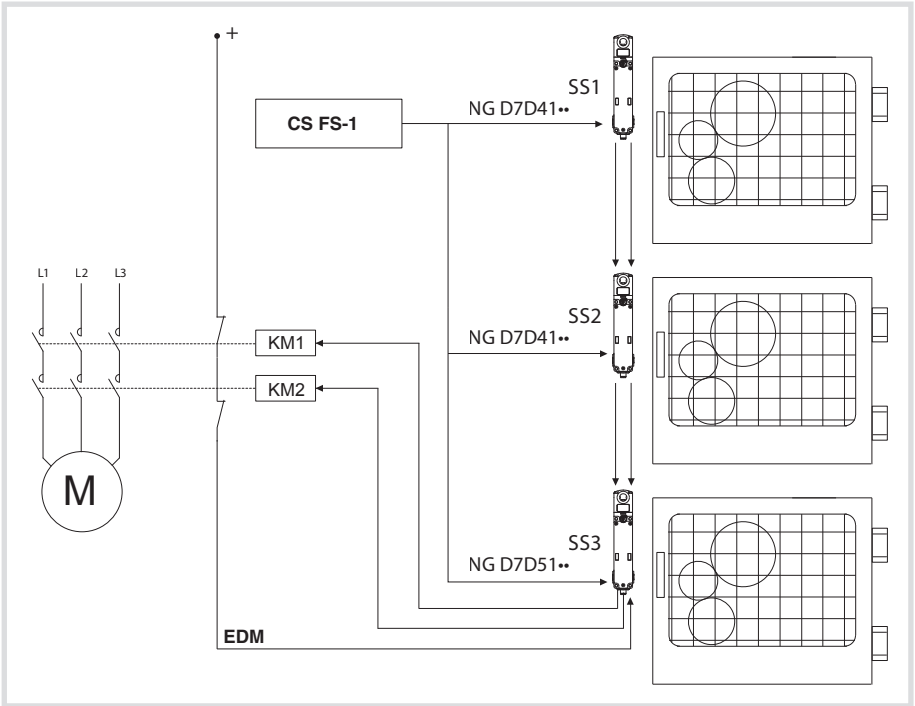
Calcul de la PFH_D totale du SRP/CS fonction de sécurité 2 (verrouillage)
$PFH_{DTOT} = PFH_{DSB21} + PFH_{DSB22}$ = 1,20E-09
cela correspond à un PL e.

Exemple de calcul effectué avec le logiciel SISTEMA, téléchargeable gratuitement sur le site www.pizzato.com

EXEMPLE 9
Application : Contrôle des protecteurs



Norme de référence EN ISO 13849-1	
Niveau de performance fonction de sécurité 1	**PL e**
Niveau de performance fonction de sécurité 2	**PL d**

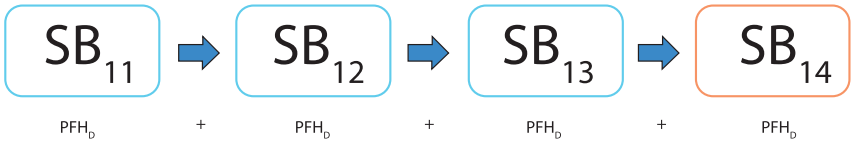


Description de la fonction de sécurité
Les dispositifs d'interverrouillage SS1, SS2 et SS3 réalisent deux fonctions de sécurité : surveillance de l'état « protecteur verrouillé » et verrouillage du protecteur.
Une fois les protecteurs déverrouillés, les trois capteurs agissent directement sur les deux contacteurs KM1 et KM2. Les contacteurs KM1 et KM2 (avec contacts forcés) sont commandés par le capteur SS3 via l'entrée I5 de l'EDM (External Device Monitoring).
La commande de verrouillage dans les trois dispositifs SS1, SS2 et SS3 est conditionnée par la fermeture du contact de sécurité d'un temporisateur de sécurité CS FS-1. Chaque appareil reçoit la commande de déverrouillage en appuyant sur le bouton de la poignée P-KUBE Krome.

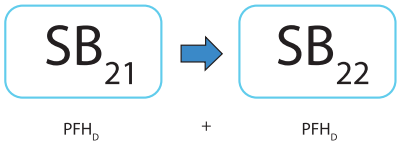
Données des dispositifs
SS1, SS2, SS3 sont des dispositifs d'interverrouillage codifiés avec technologie RFID et avec un dispositif de verrouillage du protecteur. Fonction de détection de la protection verrouillée PFH_d = 1,17E-09 PL = e, fonction de commande de retenue à canal unique PFH_d = 1,51E-10 PL = d.
CS FS-1 est un temporisateur de sécurité, PFH_d = 5,06E-10, PL = e.
KM1, KM2 sont des contacteurs utilisés à charge nominale. B_{10D} = 1.300.000 (voir tableau C.1 d'EN ISO 13849-1)

Hypothèse de fréquence d'utilisation
Chaque porte est ouverte toutes les 10 minutes, 16 heures par jour et 365 jours par an, donc n_{op} = 35.040

Définition du SRP/CS et des sous-systèmes
Cet exemple d'application est caractérisé par deux fonctions de sécurité :
1. Fonction d'arrêt liée à la sécurité activée par une mesure de protection
2. Fonction de maintien du protecteur verrouillé avec moteur M1 en mouvement
La fonction de sécurité 1 est réalisée par un SRP/CS composé de 4 sous-systèmes (SB) :
- SB11, 12, 13 représentent trois dispositifs d'interverrouillage RFID des séries NG SS1, SS2 et SS3
- SB14 représente deux télérupteurs KM1 et KM2 en architecture redondante (cat. 4)



La fonction de sécurité 2 est réalisée par 2 sous-systèmes (SB) :



- SB21 représente le temporisateur de sécurité CS FS-1
- SB22 représente le dispositif d'interverrouillage RFID de la série NG

Calcul de PFH_D pour SB14
$MTTF_D$ KM1,KM2 = 371 ans.
DC = 99%, les contacts de KM1 et KM2 sont contrôlés par le dernier dispositif NG de la série via l'entrée EDM.
On suppose une valeur supérieure à 65 pour le paramètre CCF (selon l'annexe F de l'EN ISO 13849-1).
Un circuit de catégorie 4 avec $MTTF_D$ = 371 et une couverture élevée du diagnostic (DC = 99%) correspond à une probabilité de défaillance PFH_D = 6,3E-09 et à un PL e.

Calcul de la PFH_D totale du SRP/CS fonction de sécurité 1
$PFH_{DTOT} = PFH_{DSB11} + PFH_{DSB12} + PFH_{DSB13} + PFH_{DSB14}$ = 9,8E-09
Cela correspond à un PL e.

Calcul de la PFH_D totale du SRP/CS fonction de sécurité 2
$PFH_{DTOT} = PFH_{DSB21} + PFH_{DSB22}$ = 6,6E-10
Cela correspondrait à un PL e. Toutefois, si l'on considère que le dispositif avec commande de verrouillage à canal unique NG est caractérisé par un PL d, l'ensemble SRP/CS est déclassé à cette valeur, PL d.