ABB drives

Sécurité fonctionnelle

Guide technique n°10

ABB

ABB drives
Sécurité fonctionnelle

Guide technique n°10

3AUA0000048753 REV C
APPLICABLE LE : 09/04/2010

Table des matières

Limitation de responsabilité

Ce document est un guide informatif à destination des utilisateurs, prescripteurs, fabricants de machines et autres personnes concernées pour les aider à mieux comprendre les exigences de la Directive Machine de l'UE, et les mesures nécessaires au respect de la directive et des normes harmonisées sur lesquelles elle est basée.

Ce document n'est pas destiné à une utilisation mot à mot, mais doit être considéré comme une aide informative.

Les informations et exemples présentés dans ce guide sont destinés à une utilisation générale uniquement et n'offrent pas tous les détails nécessaires à la mise en œuvre d'un système de sécurité.

ABB Oy Drives ne saurait être tenu pour responsable de quelque blessure ou dommage directs ou indirects résultant de l'utilisation des informations contenues dans ce document. Le fabricant de la machine demeure toujours, en fin de compte, responsable de la sécurité du produit et de son adéquation au regard des lois applicables. ABB décline par la présente toute responsabilité quant à l'utilisation de ce document.

Au sujet de ce document

Ce document présente la Directive Machine et les normes à prendre en compte lors de la conception d'une machine, afin de garantir la sécurité fonctionnelle.

Le but de ce document est d'expliquer, en termes généraux, le processus permettant de respecter les exigences de la Directive Machine, et les critères d'obtention du marquage CE. Le marquage CE indique que la machine est conforme aux exigences de la Directive.

Remarque :
Ce document ne constitue qu'une présentation générale du processus permettant de répondre aux exigences essentielles de la Directive Machine. Le fabricant de la machine demeure toujours, en fin de compte, responsable de la sécurité et de la conformité du produit.

Le document comporte trois parties :

- Partie 1 - Théorie et contexte - présente l'idée sous-jacente à la sécurité fonctionnelle et comment respecter la Directive Machine. Elle présente aussi les changements à venir de la nouvelle Directive Machine et explique la hiérarchie du système européen de normes harmonisées.
- Partie 2 - Nouvelle approche - présente les normes relatives à la nouvelle Directive Machine qui remplacent les anciennes normes. Elle présente aussi les deux systèmes de normes et donne une liste de normes et de fonctions de sécurité pertinentes.
- Partie 3 - Les étapes nécessaires au respect de la Directive Machine - présente neufs étapes utiles dans le processus permettant de répondre aux exigences essentielles de la Directive Machine.

Partie 1 - Théorie et contexte

Les lois nationales de l'Union Européenne stipulent que les machines doivent satisfaire aux Exigences essentielles de santé et de sécurité (EESS) définies dans la Directive Machine et dans les normes harmonisées sur lesquelles elle est basée. Ceci signifie que toutes les nouvelles machines doivent respecter les mêmes exigences légales dans toute l'UE quel que soit le pays où elles sont installées. Ces mêmes normes sont aussi reconnues dans de nombreuses parties du monde en dehors de l'Europe, par exemple au travers de chartes d'équivalence, qui facilitent le commerce des machines et les livraisons de machines entre pays à l'intérieur et même à l'extérieur de l'UE.

Pourquoi les machines doivent-elles répondre à ces exigences ? Parce que la conformité contribue à la prévention des accidents et des blessures qui en résultent. De plus, en se conformant à la Directive machine et aux normes harmonisées correspondantes, les fabricants de machines sont sûrs d'avoir remplis leurs obligations en matière de conception et de fourniture de machines sûres respectant les lois nationales.

Pour les fabricants, des stratégies de sécurité nouvelles et meilleures deviennent un moyen d'améliorer leur productivité et leur compétitivité sur le marché. Le but des systèmes de sécurité traditionnels était d'assurer une sécurité fonctionnelle complète et de respecter les obligations légales. Ceci a été réalisé en utilisant des dispositifs électriques et mécaniques supplémentaires, même au prix de la productivité. Les opérateurs peuvent, dans certains cas, contourner ces systèmes pour essayer d'améliorer la productivité, ce qui peut conduire à des accidents.

Avec les systèmes de sécurité modernes, la sécurité des processus et de l'opérateur peut être prise en compte tout en maintenant la productivité. Par exemple, il est possible de laisser la machine en marche mais à vitesse réduite pour conserver la sûreté du fonctionnement. Avec les solutions de sécurité modernes, la sécurité peut être une composante intégrée de la fonctionnalité de la machine, et les solutions de sécurité ne sont plus ajoutées après coup pour respecter les règlementations.

Les systèmes de sécurité peuvent être mis en œuvre efficacement au travers de processus définis, pour obtenir des performances de sécurité spécifiques, et utiliser des sous-systèmes certifiés tels que les modules pour systèmes de sécurité. Le respect des normes de sécurité est une des règles du monde industriel, et les sous-systèmes certifiés comme les entraînements deviennent indispensables sur le marché. La sécurité des machines est l'un des secteurs dont la croissance est la plus rapide en automatisation industrielle.

Sécurité et sécurité fonctionnelle

Le but de la sécurité est de protéger les personnes et l'environnement des accidents, et dans le cas présent, des machines. Les systèmes de sécurité fonctionnelle atteignent cet objectif en diminuant la probabilité des évènements indésirables, de sorte que les accidents soient réduits lors de l'utilisation des machines. Les normes de sécurité définissent la sécurité comme l'absence de risque inacceptable.

Ce qui est acceptable est défini par la société. Les fabricants de machines devraient toujours utiliser les mêmes critères d'acceptabilité (les plus draconiens) pour tous les secteurs du marché, indépendamment des différences régionales.

Le moyen le plus efficace d'éliminer les risques est de le faire dès la conception. Mais si la réduction du risque au niveau de la conception n'est pas possible ou pratique, l'utilisation de protections statiques ou de systèmes de sécurité fonctionnelle est souvent la meilleure option. Lorsque les machines sont arrêtées rapidement et de façon sûre, ou utilisées à vitesse réduite pendant des périodes spécifiques afin de réduire le risque, il est possible d'obtenir une meilleure productivité machine, un temps d'utilisation plus important et un comportement du système de sécurité moins brusque. Les obligations légales sont par la même occasion respectées et la sécurité des personnes et de l'environnement est assurée.

La sécurité fonctionnelle des machines signifie habituellement des systèmes qui surveillent de façon sûre les applications de la machine, et, lorsque c'est nécessaire, prennent le contrôle de ces applications pour garantir un fonctionnement sûr. Un système relatif à la sécurité est un système qui met en œuvre les fonctions de sécurité requises et nécessaires. Les systèmes de sécurité fonctionnelle sont conçus pour détecter les situations dangereuses et faire repasser la machine dans un état sûr, ou pour garantir que l'action souhaitée, par exemple un arrêt sûr, ait bien lieu.

La surveillance peut concerner la vitesse, l'arrêt, le sens de rotation et l'immobilisation. Lorsque le système de sécurité exécute une fonction de sécurité active, par exemple la surveillance d'une vitesse de ralenti, et que le comportement du système dévie de ce qui est attendu (une vitesse trop élevée par exemple), le système de sécurité détecte la déviation et fait repasser de façon active le fonctionnement de la machine à un état sûr. Ceci peut être obtenu, par exemple, en arrêtant la machine de façon sûre (arrêt sûr) et en diminuant le couple de l'arbre moteur.

Un système de sécurité ne fait pas partie du fonctionnement standard de la machine, mais toute défaillance du système de sécurité augmente immédiatement les risques relatifs au fonctionnement de la machine.

Directive Machine

La Directive Machine, ainsi que les normes harmonisées listées ci-dessous, définissent les Exigences essentielles de santé et de sécurité (EESS) pour les machines au niveau de l'Union Européenne. La liste des EESS figure à l'Annexe I de la Directive Machine.

L'idée sous-jacente à la Directive machine est de garantir qu'une machine est sûre et qu'elle est conçue et construite de façon à pouvoir être utilisée, configurée et entretenue tout au long des phases de sa vie en représentant un risque minimal pour les personnes et l'environnement.

Les EESS affirment que lors de la recherche de solutions pour concevoir et construire des machines sûres, les fabricants de machines doivent appliquer les principes suivants dans l'ordre ci-dessous :

- Éliminer ou minimiser les dangers autant que possible en prenant en compte les aspects sécurité dans les phases de conception et de construction de la machine .
- Appliquer les mesures de protection nécessaires contre les dangers qui ne peuvent pas être éliminés.
- Informer les utilisateurs sur les risques résiduels, c'est-à-dire les risques qui demeurent bien que toutes les mesures de protection aient été prises, tout en spécifiant les exigences en matière de formation ou d'équipements de protection individuels.

La conformité avec les EESS de la Directive Machine permet au fabricant de machines d'apposer le marquage CE sur la machine. Avec le marquage CE, le fabricant garantit que le produit est conforme à toutes les règlementations sur la libre circulation des biens, ainsi qu'aux exigences essentielles des Directives européennes correspondantes, dans le cas présent, la Directive Machine.

Remarque :
Conformément à la Directive Machine, le marquage CE est apposé uniquement sur la machine complète, et non sur les composants de la machine. Ainsi, le fabricant du produit - ou son représentant - est responsable du marquage CE, et non le fabricant du composant inclus dans le produit final.

Le fabricant de la machine est responsable de la réalisation de l'analyse de risques concernée, telle que décrite dans les différentes étapes de la Partie 3, et de la conformité aux exigences. Le fabricant du composant est responsable des performances de sécurité (niveau SIL/PL) de la fonction de sécurité dudit composant, lorsque le composant est utilisé de façon appropriée. Dans ce cas présent, un composant peut être un relais de sécurité, ou un variateur de fréquence à fonctionnalité de sécurité intégrée.

Modifications introduites par la nouvelle Directive Machine

Une nouvelle Directive Machine (2006/42/CE) remplacera l'ancienne Directive (98/37/CE) à compter du 29 décembre 2009. La nouvelle Directive sera applicable aux machines mises sur le marché après cette date.

Les différences entre l'ancienne Directive et la nouvelle Directive révisée ne sont pas très importantes. L'objectif de la nouvelle Directive est de renforcer les résultats obtenus par l'ancienne Directive Machine sur la libre circulation et la sûreté des machines et d'améliorer son application.

Les principales modifications introduites par la nouvelle Directive Machine sont les suivantes :

- *Modifications relatives au mode d'évaluation de la conformité pour les machines dangereuses figurant dans la liste de l'Annexe IV de la Directive Machine.*
  Avec la nouvelle Directive, le fabricant peut réaliser une auto-certification sans faire appel à un organisme notifié. À cette fin, le fabricant doit disposer d'une procédure d'assurance qualité mise en œuvre conformément aux exigences décrites à l'Annexe X de la Directive Machine.

- *Modifications relatives aux Exigences essentielles de santé et de sécurité décrites à l'Annexe I de la Directive Machine.*
  Le fabricant doit maintenant réaliser une appréciation du risque relative aux EESS.

- *Modifications relatives à la preuve de la sécurité de différents produits.*
  Les réglementations relatives aux machines s'appliqueront de la même façon aux machines, aux équipements interchangeables, aux composants de sécurité etc. Les produits doivent être accompagnés de l'évaluation de la conformité CE, de la déclaration de conformité et des informations utilisateur requises.

- *Modification des exigences relatives aux quasi-machines.*
  Une quasi-machine est un composant ou un ensemble de composants qui ne peut assurer à lui seul une fonction définie.
  La quasi-machine est assemblée à d'autres machines ou à d'autres quasi-machines ou équipements en vue de constituer une machine à laquelle la présente directive s'applique.

  En plus de la déclaration du fabricant, le fabricant doit maintenant aussi fournir une déclaration d'incorporation précisant celles des exigences essentielles de la directive qui sont appliquées à la quasi-machine, et celles qui sont satisfaites. La documentation technique doit aussi comporter les instructions relatives à l'installation.

- *Modifications relatives à la Directive Basse tension.*
  Le champ d'application de la Directive Basse tension concerne maintenant un produit au lieu d'un risque. La distinction entre la Directive Machine et la Directive Basse tension a été clarifiée.

- *Modifications relatives à l'analyse de danger.*
  L'analyse de danger est remplacée par une appréciation et une évaluation des risques obligatoires.

- *Modifications relatives au contrôle de la fabrication.*
  Les machines de série font maintenant l'objet d'un contrôle interne de fabrication, précisé dans l'Annexe VIII de la Directive Machine.

- *Modifications relatives à la validité de l'attestation d'examen CE de type.*
  Un organisme notifié doit réexaminer la validité de l'attestation d'examen CE de type tous les cinq (5) ans. Le fabricant et l'organisme notifié conservent les documents techniques pertinents pendant une durée de 15 ans.

Hiérarchie du système européen de normes harmonisées

Le Comité européen de normalisation (CEN) et le Comité européen pour la normalisation électrotechnique (CENELEC) sont chargés d'établir les normes harmonisées. Toutes les normes harmonisées portent le préfix "EN".

Une liste des normes harmonisées est disponible sur le site internet de la Commission européenne à l'adresse http://ec.europa.eu.

La majorité des normes harmonisées sont utilisées comme référence par une ou plusieurs Directives. Pour garantir que les exigences essentielles de la Directive machine sont satisfaites, il est conseillé d'appliquer les normes harmonisées européennes appropriées.
En concevant leurs machines conformément à ces normes, les fabricants peuvent démontrer qu'ils répondent aux exigences de la Directive machine, et de façon générale, qu'ils n'ont pas besoin de certification indépendante.

Remarque :
Les exceptions concernant les machines visées à l'Annexe IV de la Directive Machine sont à noter.

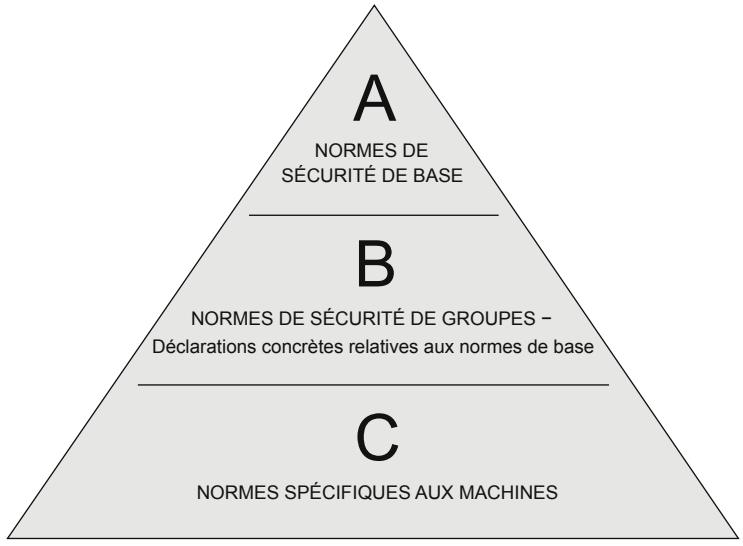


Figure 1-1 Hiérarchie des normes européennes harmonisées

- Les normes de type C sont spécifiques à une machine ou à une catégorie de machine. Si une machine est concernée par une norme de type C, les normes associées de type B et éventuellement de type A deviennent secondaires. Lors de la conception des fonctions de sécurité, les normes de type C définissent des exigences supplémentaires et obligatoires pour les machines concernées. Toutefois, si aucune norme de type C ne s'applique à une machine donnée, les normes de type B et A fournissent une aide à la conception et à la fabrication de machines conformes aux exigences de la Directive Machine.
- Les normes de type B concernent les exigences de sécurité communes à la conception de la plupart des machines. Ces normes fournissent des informations sur les risques potentiels et sur la façon de les gérer à l'aide d'un processus de réduction des risques. Les normes de type B peuvent être classées en deux groupes, B1 et B2. Les normes de type B1 concernent les aspects spécifiques à la sécurité et les normes de type B2, les équipements relatifs à la sécurité en général. Parmi les normes de type B1 se trouvent par exemple les normes EN 62061:2005 et EN ISO 13849-1:2008. Les normes de type B2 comprennent les normes relatives aux boutons d'arrêt d'urgence, comme la norme EN ISO 13850:2008.
- Les normes de type A concernent les principes de conception et les notions fondamentales relatives aux machines. Un exemple de norme de type A est la norme de sécurité de base EN ISO 12100-1.

Remarque :
L'application de ces normes n'est pas obligatoire, mais elles fournissent des lignes directrices et une aide pour répondre aux exigences de la Directive Machine, qui elles, sont obligatoires.

Partie 2 – Nouvelle approche

Remarque :
L'ancienne norme EN 954-1 a été supplantée par les normes EN ISO 13849-1 et EN 62061 en 2006. Toutefois, l'ancienne norme conserve encore la présomption de conformité, en parallèle avec les nouvelles normes pendant une période de transition, qui se termine le 31 décembre 2011 (la période de transition originelle de 2006 à 2009 a été prolongée de deux ans, jusque fin 2011).

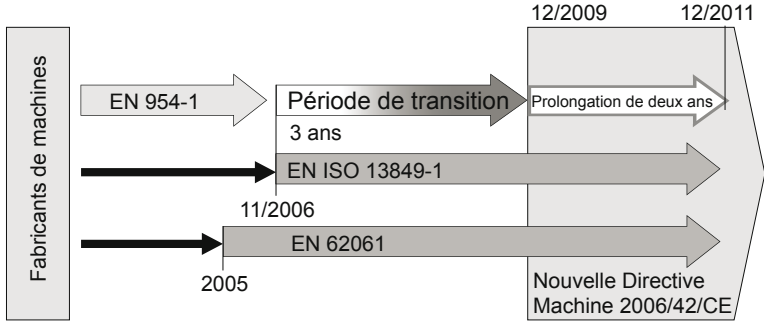


Figure 2-1 Période de transition entre l'ancienne et les nouvelles normes

Le remplacement de la norme EN 954-1 par les normes EN ISO 13849-1 et EN 62061 (qui n'est applicable qu'aux systèmes de commande électrique) représente un passage d'une approche déterministe, où les relations de cause à effet étaient bien connues, à une approche probabiliste ou fiabiliste des systèmes relatifs à la sécurité.
Les nouvelles normes prennent en compte la probabilité de défaillance de l'ensemble de la fonction de sécurité, et pas seulement de ses composants. Contrairement à l'ancienne norme EN 954-1, ces nouvelles normes permettent aussi d'utiliser des systèmes de sécurité programmables.

La nouvelle approche continue à utiliser le concept d'architectures désignées (catégories) de la norme EN 954-1, et introduit en plus de nouveaux concepts, comme le cycle de vie, la quantification - fiabilité des composants et qualité du test - et l'analyse des défaillances de cause commune.

Remarque :
La norme EN ISO 13849-1 a conservé les catégories introduites par la norme EN 954-1. Elle fournit des méthodes pour la conception et la vérification basées sur ces catégories. La norme EN 62061 comprend des architectures désignées et une méthodologie similaires.

La norme EN 954-1 était une norme relativement simple, qui offrait un procédé clair et rapide de détermination de la catégorie de sécurité d'une machine. Le processus de la norme EN ISO 13849-1 est similaire, mais

un peu plus complexe, car en plus de la détermination de la catégorie ou de l'architecture du système, le fabricant de la machine doit aussi maintenant garantir la sécurité de la machine en réalisant des évaluations et des calculs. L'utilisation de sous-systèmes certifiés pour réaliser les systèmes de sécurité est recommandée, puisqu'elle accélère le processus de spécification et nécessite moins de calculs.

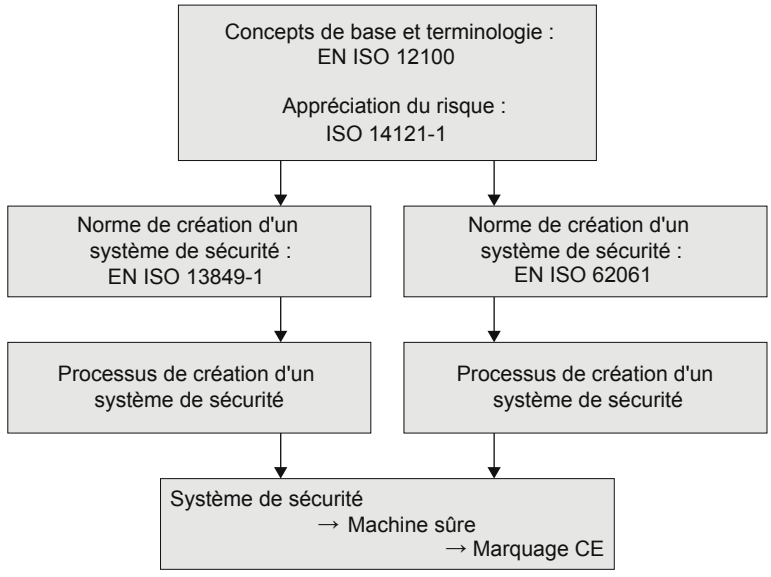


Figure 2-2 Présentation des normes

Deux normes - CEI et ISO

Deux normes différentes peuvent être utilisées pour la mise en œuvre de systèmes de sécurité fonctionnelle conformément à la Directive Machine : La norme de la Commission Électrotechnique Internationale (CEI) et la norme de l'Organisation internationale de normalisation (ISO).

Suivre l'une ou l'autre de ces normes donne des résultats très similaires, et les niveaux d'intégrité de sécurité (Safety Integrity Level, SIL) et de performance (Performance Level, PL) obtenus sont en fait comparables. Pour plus d'informations, référez-vous au tableau de comparaison dans la Partie 3, Étape 6.

Un tableau expliquant l'adéquation des deux nouvelles normes à la conception de systèmes utilisant des technologies particulières est disponible dans les normes EN ISO 13849-1 et EN 62061.

Remarque :
Il appartient au fabricant de la machine de décider - le cas échéant - quelle norme de création de système de sécurité doit être utilisée (EN ISO 13849-1 ou EN 62061), et il doit alors suivre cette norme du début jusqu'à la fin pour garantir la congruence avec ladite norme.

Les normes CEN sont basées sur les normes ISO et sont généralement prévues pour les équipements mécaniques - les numéros des nouvelles normes font partie de la série des 10 000 - alors que les normes CENELEC sont basées sur les normes CEI - les numéros des nouvelles normes font partie de la série des 60 000.

Remarque :
Dans ce document, les normes EN ISO sont désignées en utilisant le sigle "ISO". Toutefois, les normes EN CEI sont désignées sans utiliser le sigle "CEI", conformément à la convention utilisée dans la liste des normes harmonisées.

Normes relatives à la réduction des risques

Les normes de sécurité de base pour la réduction des risques comprennent :

- **EN ISO 12100-1:2003**
  (Sécurité des machines - Concepts de base, principes généraux de conception)
- **EN ISO 14121-1:2007**
  (Sécurité des machines – Appréciation des risques).

La norme EN ISO 12100 donne aux concepteurs un cadre de travail général et des lignes directrices, et propose une stratégie de réduction des risques (la méthode en trois étapes). La norme EN ISO 12100-1 définit la terminologie de base utilisée et la méthodologie appliquée pour réaliser la sécurité des machines.

La norme EN ISO 14121-1 est une nouvelle norme d'appréciation du risque utilisée dans le processus de réduction des risques, qui est décrit dans la norme EN ISO 12100. La norme EN ISO 14121-1 a remplacé la norme EN 1050:1996, qui a expiré le 24 juin 2008.

Remarque :
Toutes les autres références à ces normes dans le présent document s'appliquent toujours aux versions mentionnées ci-dessus.

Normes relatives aux systèmes de sécurité électroniques

Les normes relatives aux systèmes de sécurité électroniques sont les suivantes :

- **EN ISO 13849-1:2008** (Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Principes généraux de conception).
- **EN 62061:2005** (Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité).
- **CEI 61508:1998-2000** (Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité).

- **EN 60204-1:2006** (Sécurité des machines – Équipement électrique des machines – Règles générales).

Remarque :
Toutes les autres références à ces normes dans le présent document s'appliquent toujours aux versions mentionnées ci-dessus.

La norme EN ISO 13849-1 fournit des instructions pour concevoir des machines sûres. Ces instructions comprennent des recommandations relatives à la conception, à l'intégration et à la validation des systèmes. Elle peut être utilisée pour les parties relatives à la sécurité des systèmes de commande et différents types de machine, indépendamment de la technologie et de l'énergie utilisées. La norme comprend aussi des exigences particulières pour les parties relatives à la sécurité comportant des systèmes électroniques programmables. Cette norme couvre l'ensemble de la fonction de sécurité pour tous les dispositifs inclus (une chaîne de sécurité complète, par exemple capteur - fonction logique - actionneur).

La norme définit comment le niveau de performance (PL) est déterminé et comment le PL obtenu est vérifié au sein d'un système. Le PL spécifie la capacité d'un système de sécurité à exécuter une fonction de sécurité en conditions prévisibles. Il existe 5 niveaux de performances : a, b, c, d et e. Le PL “e” correspond à la fiabilité en matière de sécurité la plus élevée, alors que le PL “a” correspond à la plus faible.

La norme EN 62061 est destinée à la conception des systèmes de sécurité électriques. Il s'agit d'une norme spécifique au secteur des machines, dans le cadre de la norme CEI 61508. La norme EN 62061 comprend des recommandations pour la conception, l'intégration et la validation des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité des machines. L'ensemble de la chaîne de sécurité (par exemple capteur - fonction logique - actionneur) est couverte par cette norme. Les sous-systèmes individuels n'ont pas besoin d'être certifiés, du moment que l'ensemble de la fonction de sécurité répond aux exigences définies. Toutefois, l'utilisation de sous-systèmes certifiés tels que les modules est fortement recommandée, car elle peut réduire considérablement les efforts nécessaires à la conception.

Remarque :
Contrairement à la norme EN ISO 13849-1, la norme EN 62061 ne couvre pas les exigences relatives aux équipements de commande non-électrique relatifs à la sécurité des machines.

Cette norme définit comment le niveau d'intégrité de sécurité (Safety Integrity Level, SIL) est déterminé. Le SIL représente la fiabilité des fonctions de sécurité. Il existe quatre niveaux d'intégrité de sécurité : 1, 2, 3 et 4. “SIL 4” est le niveau d'intégrité de sécurité le plus élevé et “SIL 1” le plus faible. Seuls les niveaux 1 à 3 sont utilisés pour les machines.

La norme CEI 61508 est une norme de sécurité fonctionnelle de base. Elle couvre le cycle de vie des systèmes comprenant des composants électriques et/ou électroniques et/ou électroniques programmables utilisés pour réaliser des fonctions de sécurité. La norme CEI 61508 n'est pas une norme harmonisée, mais elle constitue la principale norme exposant les exigences et les méthodes de conception des systèmes de commande relatifs à la sécurité avec du matériel et des logiciels complexes. La norme CEI 61508 est généralement utilisée pour la conception de sous-systèmes de sécurité certifiables. Les normes EN ISO 13849-1 et EN 62061 sont basées sur les principes définis dans la norme CEI 61508.

La norme EN 60204-1 fournit des lignes directrices et des exigences pour les équipements électriques des machines afin d'améliorer la sécurité et la facilité d'utilisation.

Normes de sécurité spécifiques aux produits (type C)

Les normes de sécurité spécifiques aux produits, appelées normes de type C, concernent une machine ou une classe de machine spécifique et sont basées sur la présomption de conformité aux EESS couvertes par la norme.

Il est à noter que :

- Les exigences spécifiées dans les normes de type annulent en général les exigences définies par les normes de sécurité générales (EN 62061, EN ISO 13849-1, etc.).
- Les normes de type C peuvent comporter des exigences en matière de SIL/PL pour certaines fonctions de sécurité. Il est obligatoire de satisfaire à ces exigences, indépendamment des résultats de l'analyse de risques.

Remarque :
Même si la liste des dangers potentiels associés à la machine, élaborée lors de l'appréciation des risques, et celle de la norme de type C sont identiques, il est possible que la norme ne tienne pas compte de toutes les EESS pertinentes. Il est nécessaire de passer soigneusement la norme en revue afin de déterminer quels dangers peuvent avoir été exclus de la liste.

Normes spécifiques aux systèmes d'entraînement relatifs à la sécurité

La norme suivante est une norme spécifique aux systèmes d'entraînement relatifs à la sécurité :

- **EN 61800-5-2:2007** (Entraînements électriques de puissance à vitesse variable - Exigences de sécurité fonctionnelle).

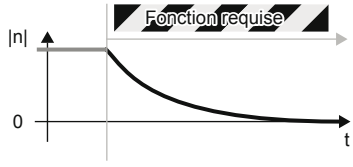
Remarque :
Toutes les autres références à cette norme dans le présent document s'appliquent uniquement à la version mentionnée ci-dessus.

La norme EN 61800-5-2 donne des spécifications et des lignes directrices concernant les entraînements électriques de puissance utilisés dans des applications relatives à la sécurité. Il s'agit d'une norme de produit qui présente des aspects relatifs à la sécurité au regard du cadre de la norme CEI 61508, et qui introduit des exigences pour les entraînements électriques de puissance lorsqu'ils sont utilisés comme sous-systèmes dans des systèmes de sécurité.

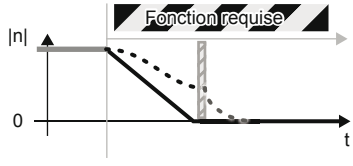
Fonctions de sécurité normalisées

La norme EN 61800-5-2 comprend des définitions pour de nombreuses fonctions de sécurité. Un entraînement peut offrir une ou plusieurs de ces fonctions. Quelques exemples :

Safe torque-off (STO)
Cette fonction permet de mettre la machine hors couple et/ou interdit le redémarrage intempestif.



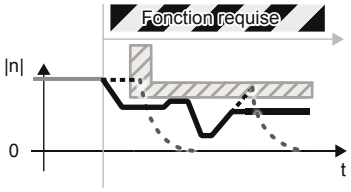
Safe stop 1 (SS1)
Cette fonction arrête le moteur en sécurité, et active la fonction STO en dessous d'une vitesse spécifiée ou après un temps défini.



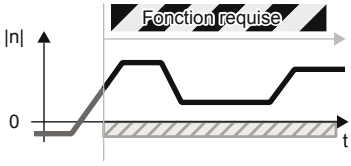
Safe stop 2 (SS2)
Cette fonction arrête le moteur en sécurité, et active la fonction SOS en dessous d'une vitesse spécifiée ou après un temps défini.

Safe operating stop (SOS)
Cette fonction maintient le moteur immobilisé en sécurité tout en conservant le couple moteur actif.

Safely-limited speed (SLS)
Cette fonction empêche le moteur de dépasser la limite de vitesse spécifiée.

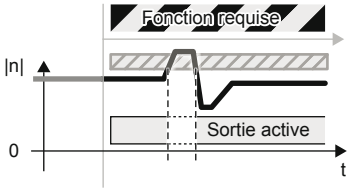


Safe direction (SDI)
Cette fonction empêche l'arbre moteur de tourner dans le sens non désiré.



Safe brake control (SBC)
Cette fonction génère un signal de sortie sécurisé pour la commande d'un dispositif externe de freinage (mécanique) de sécurité.

Safe speed monitor (SSM)
Cette fonction génère un signal de retour sûr lorsque la vitesse du moteur se situe en dessous d'une limite de vitesse spécifiée.



Référez-vous à la norme EN 61800-5-2 pour plus d'exemples de fonctions de sécurité.

Opérations d'urgence
La norme EN 60204-1 introduit deux opérations d'urgence, l'interrupteur d'arrêt d'urgence et l'arrêt d'urgence.

Coupure d'urgence
La fonction de coupure d'urgence coupe l'alimentation du système ou d'une partie de ce système en cas de risque d'électrocution.

Cette fonction nécessite des interrupteurs externes, et ne peut pas être réalisée avec des fonctions basées sur les entraînements comme la fonction safe torque-off (STO).

Arrêt d'urgence
Un arrêt d'urgence doit fonctionner de telle sorte que, lorsque celui-ci est activé, le mouvement dangereux de la machine est arrêté et la machine ne peut en aucun cas redémarrer de façon inopinée, même après annulation de l'arrêt d'urgence. Seule l'annulation de l'arrêt d'urgence permet de redémarrer la machine.

L'arrêt d'urgence peut arrêter des mouvements dangereux au moyen des actions suivantes :
- taux de décélération optimal jusqu'à l'arrêt de la machine,
- utilisation de l'une des deux catégories d'arrêt d'urgence, 0 ou 1, ou
- utilisation d'une séquence d'arrêt prédéfinie.

Un arrêt d'urgence de catégorie 0 signifie que l'alimentation du moteur est immédiatement coupée. L'arrêt d'urgence de catégorie 0 est équivalent à la fonction *safe torque-off (STO)* telle que définie par la norme 61800-5-2.

Un arrêt d'urgence de catégorie 1 signifie que la décélération et l'arrêt de la machine sont contrôlés, puis l'alimentation coupée. L'arrêt de catégorie 1 est équivalent à la fonction *Safe Stop 1 (SS1)* telle que définie par la norme 61800-5-2.

Lorsqu'elle est activée, la fonction d'arrêt d'urgence ne doit pas créer de dangers supplémentaires ni nécessiter une intervention plus poussée de l'opérateur.

Remarque :
Les principes de conception d'une fonction d'arrêt d'urgence sont présentées dans la norme EN ISO 13850:2008.

Prévention des démarrages intempestifs
Garantir qu'une machine demeure à l'arrêt lorsque des personnes se trouvent dans la zone à risque est l'une des conditions les plus importantes pour la sécurité des machines.

La fonction *safe torque-off (STO)* peut être utilisée pour empêcher efficacement tout redémarrage inopiné, ce qui rend l'arrêt sûr en empêchant que le moteur ne soit alimenté et en maintenant l'alimentation des circuits de commande de l'entraînement principal.

Les principes et exigences concernant la prévention des démarrages intempestifs sont décrits dans la norme EN 1037:1995+A1.

Partie 3 – Les étapes nécessaires au respect de la Directive Machine

La Directive Machine exige des machines qu'elles soient sûres. Toutefois, le risque zéro n'existe pas. L'objectif est de réduire les risques.

La conformité à la Directive Machine peut être obtenue :

- en satisfaisant aux exigences définies par les normes harmonisées ou
- en faisant réaliser un contrôle d'acceptation de la machine par un tiers autorisé.

Le processus pour répondre aux EESS de la Directive Machine en utilisant les normes harmonisées peut être décomposé en neuf étapes :

- **Étape 1 : Gestion de la sécurité fonctionnelle** - gérer la sécurité fonctionnelle tout au long du cycle de vie de la machine.
- **Étape 2 : Appréciation du risque** - analyser et évaluer les risques.
- **Étape 3 : Réduction des risques** - éliminer ou réduire les risques au moyen de la conception et de la documentation.
- **Étape 4 : Détermination des exigences de sécurité** - définir ce qui est nécessaire (fonctionnalité, performance de sécurité) pour éliminer le risque ou le réduire à un niveau acceptable.
- **Étape 5 : Mise en œuvre du système de sécurité fonctionnelle** - concevoir et créer les fonctions de sécurité.
- **Étape 6 : Vérification du système de sécurité fonctionnelle** - garantir que le système de sécurité satisfait aux exigences définies.
- **Étape 7 : Validation du système de sécurité fonctionnelle** - réitérer le processus d'appréciation du risque et vérifier que le système de sécurité a réellement réduit les risques conformément à la Directive.
- **Étape 8 : Documentation** - documenter la conception, élaborer la documentation destinée à l'utilisateur.
- **Étape 9 : Conformité** - apporter la preuve de la conformité de la machine aux EESS de la Directive Machine au moyen d'une évaluation de conformité et d'un dossier technique.

Chacune de ces étapes est détaillée dans les chapitres suivants.

Mise à jour pour les machines existantes

Les questions suivantes doivent être prises en compte lors de la mise à jour des exigences de sécurité pour des machines existantes :

- Pour les machines disposant déjà du marquage CE - les nouveaux composants ajoutés à la machine doivent aussi avoir le marquage CE. La façon dont les nouveaux composants sont appliqués à l'ancien système conformément à la Directive Machine doit être définie au cas par cas.
- Pour les machines qui n'ont pas de marquage CE - le niveau de sécurité de la machine peut être conservé en remplaçant les composants existants par de nouveaux qui ont le marquage CE. Dans ce cas, la déclaration d'incorporation n'est pas fournie avec la machine. Il est nécessaire de se conformer à la Directive 89/655/CEE et à la Directive 95/63/CE la modifiant.

En dernier ressort, c'est aux autorités compétentes de décider si la modification est assez importante pour nécessiter une mise à jour du niveau de sécurité.

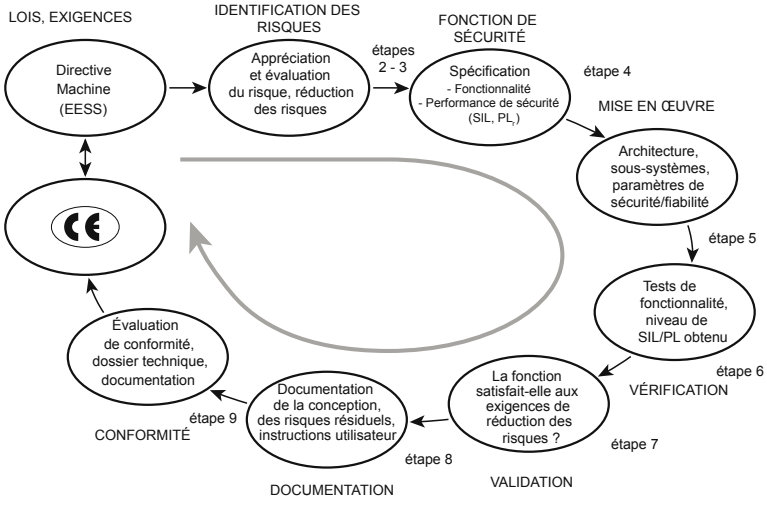


Figure 3-1 Organigramme du processus permettant de répondre aux exigences de la Directive Machine

ÉTAPE 1 : Gestion de la sécurité fonctionnelle

Pour obtenir la sécurité fonctionnelle requise, il est nécessaire de mettre en œuvre un système de gestion de projet et de gestion de la qualité comparable à ceux décrits dans les normes CEI 61508 ou ISO 9001 par exemple. Ce système de gestion peut être spécifié sous la forme d'un plan de sécurité.

Plan de sécurité
La norme EN 62061 définit un plan de sécurité pour le processus permettant de répondre aux exigences de la Directive Machine. Ce plan doit être conçu et documenté pour chaque système de sécurité et mis à jour lorsque nécessaire.

Plan de sécurité :

- identifie toutes les activités pertinentes,
- décrit la politique et la stratégie pour satisfaire aux exigences de sécurité fonctionnelle,
- identifie les responsabilités,
- identifie ou élabore les procédures et les ressources documentaires,
- décrit la stratégie pour la gestion de la configuration,
- inclut les plans de vérification et de validation.

Remarque :
Bien que les activités ci-dessus ne soient pas spécifiquement définies dans la norme EN ISO 13849-1:2008, des activités similaires sont nécessaires pour satisfaire aux exigences de la Directive Machine.

Une fois que le plan de sécurité (selon la norme EN 62061) a été élaboré, l'appréciation du risque commence.

ÉTAPE 2 : Appréciation du risque

L'appréciation du risque est un processus lors duquel les risques sont analysés et évalués. Un risque est une combinaison de la conséquence d'un dommage et de la probabilité d'occurrence du dommage lors de l'exposition à un danger.

Remarque :
L'appréciation du risque pour une machine est devenue obligatoire avec la nouvelle Directive Machine 2006/42/CE.

La Directive Machine 2006/42/CE exige que les fabricants réalisent des appréciations du risque et prennent en compte les résultats lors de la conception d'une machine. Tout risque considéré comme «élevé» doit être réduit à un niveau acceptable en modifiant la conception ou en utilisant les techniques de protection appropriées.

L'appréciation du risque fournit au concepteur de la machine les exigences nécessaires à la conception de sécurité intrinsèque. Il est très important d'apprécier les risques lors de la phase de conception, car cette méthode est en général beaucoup plus efficace que de fournir des instructions destinées à l'utilisateur sur la manière d'utiliser l'équipement de façon sûre.

Le processus d'appréciation du risque, selon la norme EN ISO 12100-1, se décompose en deux parties : une analyse des risques et une évaluation des risques. L'analyse des risques implique d'identifier et estimer les risques, et l'évaluation des risques implique de décider si le risque est acceptable ou si une réduction des risques est nécessaire.

L'évaluation des risques est réalisée à partir des résultats de l'analyse des risques. Les décisions concernant la nécessité de la réduction des risques se prennent conformément à la procédure d'évaluation des risques.

Remarque :
L'évaluation des risques doit être réalisée pour chaque danger.

Étapes de l'analyse des risques :

1. Détermination des limites et de l'utilisation prévue de la machine. Ces limites comprennent
   - limites d'utilisation,
   - limites dans l'espace,
   - limites ambiantes ou environnementales,
   - limites de durée de vie.
2. Identification des dangers potentiels générés par la machine.
3. Estimation des risques identifiés un par un.
   - Sévérité du risque (conséquences potentielles)
   - Probabilité du risque (fréquence, probabilité, évitement)

- Évaluation du risque : la réduction du risque est-elle nécessaire ?
  - OUI : Application de mesures de réduction des risques et retour à l'étape 2 de l'analyse des risques.

La méthode en 3 étapes de réduction des risques selon la norme EN ISO 12100-1 est décrite dans le chapitre suivant.

  - NON : L'objectif de réduction des risques est atteint et le processus d'appréciation du risque est terminé.

Documentation du processus d'appréciation du risque et de ses résultats séparément pour chaque danger.

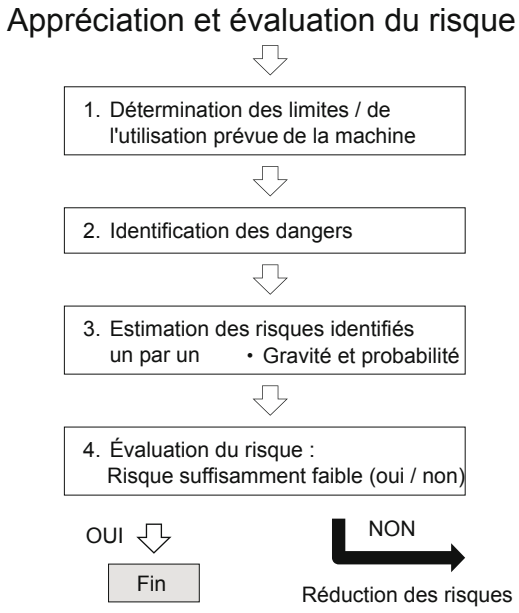


Figure 3-2 Appréciation et évaluation des risques selon la norme EN ISO 14121-1

Après avoir réalisé l'appréciation du risque, deux options sont possibles, en fonction du résultat de l'appréciation :

- Si la conclusion de l'appréciation est que la réduction des risques n'est pas nécessaire, la machine a atteint le niveau de sécurité approprié exigé par la Directive Machine.

Remarque :
Pour que la machine soit approuvée et le marquage CE apposé, les risques résiduels doivent être documentés dans les manuels d'utilisation et d'entretien appropriés. Il existe toujours des risques résiduels.

- Si l'appréciation révèle que le risque demeure inacceptable, le processus de réduction des risques commence.

ÉTAPE 3 : Réduction des risques

Le moyen le plus efficace pour réduire les risques est de les éliminer lors de la phase de conception, par exemple en modifiant la conception ou le processus de travail de la machine. Si c'est impossible, l'un des moyens de réaliser le processus de réduction des risques et de garantir la conformité aux exigences est d'appliquer les normes harmonisées adaptées sur lesquelles est basée la Directive machine.

Si le processus d'appréciation des risques conclut que la réduction des risques est nécessaire, une stratégie de réduction des risques est élaborée. Selon la norme EN ISO 12100-1, la réduction des risques peut être décomposée en trois étapes (la méthode en trois étapes) :

1. **Mesures de conception de sécurité intrinsèque - conception plus sûre, modification du processus.**
2. **Moyens de protection et mesures de protection complémentaires - fonctions de sécurité, protections statiques.**
3. **Information sur l'utilisation (gestion des risques résiduels) :**
   - **sur la machine - plaques d'avertissement, signaux et dispositifs d'avertissement**
   - **dans les instructions d'utilisation.**

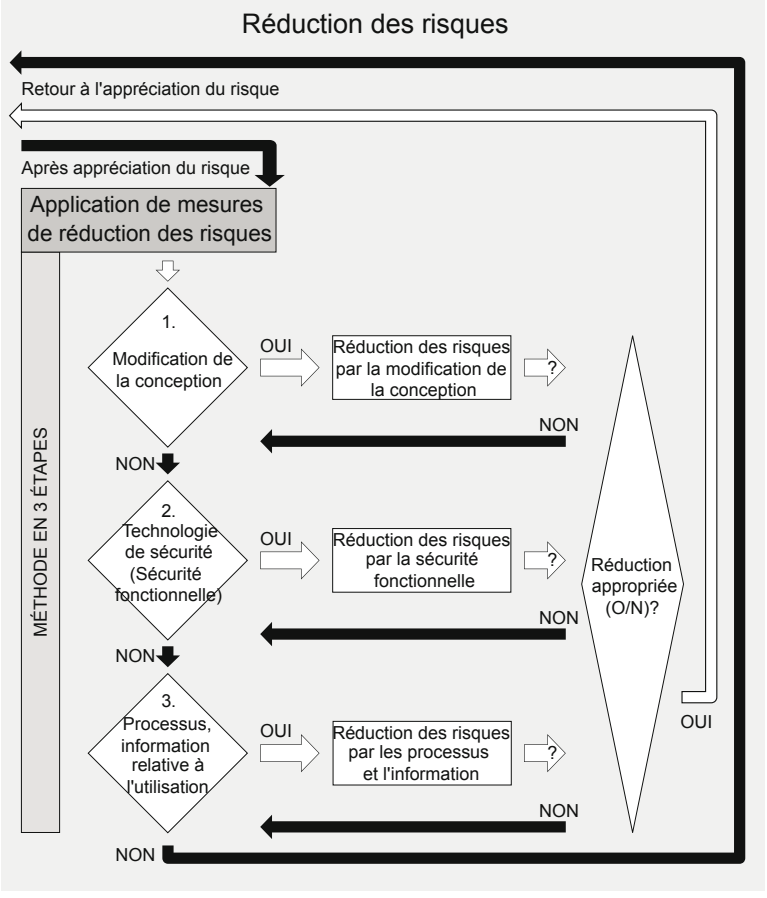


Figure 3-3 La méthode en 3 étapes de réduction des risques selon la norme EN ISO 12100-1

Le risque résiduel est le risque qui demeure lorsque toutes les mesures de protection ont été prises en compte et mises en œuvre. La technologie ne permet pas d'atteindre le risque zéro, car il existe toujours des risques résiduels.

Tous les risques résiduels doivent être documentés dans les instructions d'utilisation.

Côté utilisateur, la réduction des risques comprend les informations fournies par le concepteur (fabricant). Les mesures de réduction des risques pour l'utilisateur de la machine / l'organisation sont les suivantes :

- Mesures de réduction des risques classiques prises par l'organisation :
    - mise en place de procédures de travail sûres,
    - surveillance du travail,
    - systèmes d'autorisation de travail.
- Fourniture et utilisation de protections supplémentaires.
- Utilisation d'équipement de protection individuel.
- Formation des utilisateurs.
- Lecture et respect des instructions d'utilisation et de sécurité.

Les concepteurs devraient aussi consulter les utilisateurs, dont les informations peuvent être précieuses, lors de la définition des mesures de protection.

Lorsque la réduction des risques a été réalisée, elle doit être examinée pour garantir que les mesures prises sont adéquates et permettent de réduire le risque à un niveau approprié. Cet examen peut se faire en répétant le processus d'appréciation du risque.

Les étapes restantes ci-dessous décrivent l'option 2 de la méthode en 3 étapes : protection au moyen d'une solution de sécurité fonctionnelle.

ÉTAPE 4 : Détermination des exigences de sécurité

Une fois que toutes les mesures de réduction des risques possibles ont été intégrées au niveau de la conception, il est nécessaire de définir les protections supplémentaires. Il est possible d'utiliser des solutions de sécurité fonctionnelle comme mesures de réduction des risques vis à vis des risques résiduels.

Fonctions de sécurité
Une fonction de sécurité est une fonction de la machine dont la défaillance peut entraîner une augmentation immédiate du risque. En bref, il s'agit des mesures qui doivent être prises pour réduire la probabilité d'occurrence d'un évènement intempestif lors de l'exposition à un

danger. Une fonction de sécurité ne fait pas partie du fonctionnement de la machine elle-même. Cela signifie qu'en cas de défaillance de la fonction de sécurité, la machine peut fonctionner normalement, mais le risque de blessure lié au fonctionnement de la machine augmente.

Une fonction de sécurité est toujours définie par deux composants :

- *action* (ce qui doit être fait pour réduire le risque).
- *performance de sécurité* (niveau d'intégrité de sécurité - SIL ou niveau de performance - PL).

Remarque :
Une fonction de sécurité doit être définie, vérifiée (fonctionnalité et performance de sécurité) et validée de façon séparée pour chaque danger identifié.

Exemple de fonction de sécurité :
Exigence : Un arbre rotatif apparent présente un risque de blessure pour les personnes qui s'en approchent trop.

Action : Afin d'éviter des blessures causées par l'arbre, le moteur doit s'arrêter une (1) seconde après ouverture du portillon de sécurité.

Après que la fonction de sécurité qui exécute l'action a été définie, le niveau de sécurité requis pour cette fonction est déterminé.

Performance de sécurité / intégrité
L'intégrité de sécurité mesure la performance d'une fonction de sécurité. Elle correspond à la probabilité d'exécution sur demande de la fonction de sécurité. L'intégrité de sécurité requise pour une fonction est déterminée lors de l'appréciation du risque et est représentée par le niveau d'intégrité de sécurité (SIL) ou le niveau de performance (PL), en fonction de la norme utilisée.

Les deux normes utilisent des techniques d'évaluation différentes, mais leurs résultats sont comparables. Les termes et les définitions sont similaires pour les deux normes.

Détermination du SIL requis (EN 62061)
Le processus de détermination du niveau d'intégrité de sécurité (SIL) est le suivant :

1. Détermination de la gravité des conséquences d'un évènement dangereux.
2. Détermination du nombre de points correspondant à la fréquence et à la durée de l'exposition d'une personne au dommage.
3. Détermination du nombre de points correspondant à la probabilité d'occurrence de l'évènement dangereux lors de l'exposition à cet évènement.
4. Détermination du nombre de points correspondant à la possibilité d'éviter ou de limiter l'étendue du dommage.

Exemple :
Les paramètres utilisés pour déterminer le nombre de points sont présentés dans l'exemple suivant de tableau d'affectation de SIL.

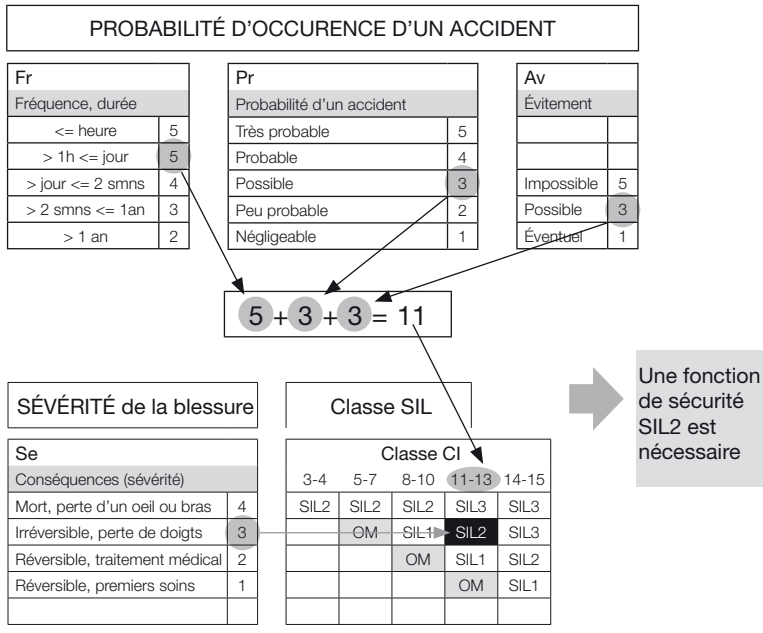


Figure 3-4 Exemple de tableau d'affectation de SIL

Dans cet exemple, l'analyse de danger concerne un arbre rotatif apparent.

- **La conséquence du danger est une blessure irréversible, et éventuellement la perte des doigts. Sévérité (Se) = 3.**
- **Une personne est exposée au danger plusieurs fois par jour. Fréquence (Fr) = 5.**
- **Il est possible que l'évènement dangereux se produise. Probabilité (Pr) = 3.**
- **Le danger peut être évité. Évitement (Av) = 3.**
- **5 + 3 + 3 = 11, et en tenant compte de la conséquence du danger, cela donne SIL 2.**

Les tableaux utilisés pour déterminer le nombre de points sont présentés dans la norme.

Après que le SIL requis a été défini, la mise en œuvre du système de sécurité peut commencer.

Détermination du PL requis (EN ISO 13849-1)
Pour déterminer le PL requis, sélectionnez l'une des possibilités dans les catégories suivantes et créez un "chemin" dans le tableau suivant.

1. Détermination de la gravité du dommage.
   Les paramètres de gravité sont les suivants :
   S1 Blessure légère, généralement réversible
   S2 Blessure grave généralement irréversible, décès inclus

2. Détermination de la fréquence et de la durée d'exposition au danger.
   Les paramètres de fréquence et de durée sont les suivants :
   F1 Exposition rare à peu fréquente et/ou de courte durée
   F2 Exposition fréquente à permanente et/ou de longue durée

3. Détermination de la possibilité d'éviter le danger ou de limiter les dommages causés par le danger.
   Les paramètres d'évitement et de limitation du danger sont les suivants :
   P1 Possibilité sous certaines conditions
   P2 Quasi-impossibilité

Exemple :
Le niveau de performance résultant est représenté par a, b, c, d et e dans l'exemple suivant de graphique des risques utilisé pour la détermination du PL.

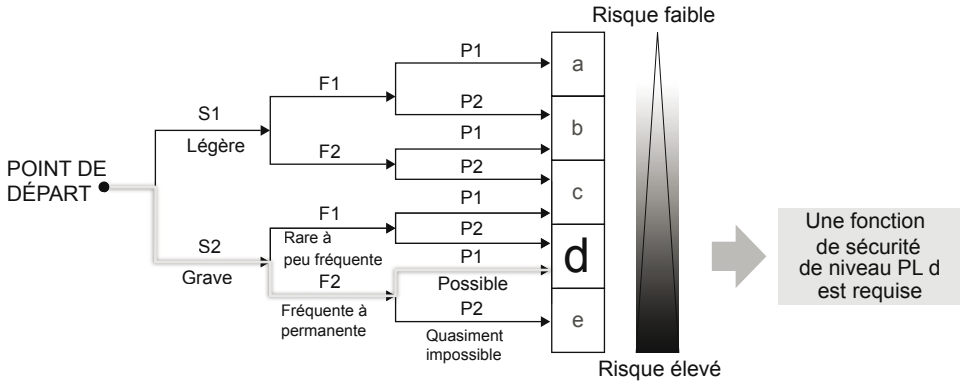


Figure 3-5 Exemple de graphique des risques utilisé pour la détermination du PL

Dans cet exemple, l'analyse de danger concerne un arbre rotatif apparent.

- La conséquence du danger est une blessure grave, irréversible. Gravité = S2.
- Une personne est exposée au danger plusieurs fois par jour. Fréquence = F2.
- Il est possible d'éviter le danger ou de limiter les dommages causés. Possibilité = P2.

Le chemin mène à une valeur de PL_r égale à d. Les tableaux utilisés pour déterminer les valeurs des paramètres sont présentés dans la norme. Après que le PL_r a été défini, la mise en œuvre du système de sécurité peut commencer.

ÉTAPE 5 : Mise en œuvre du système de sécurité fonctionnelle

Lors de la conception et de la construction d'une fonction de sécurité, l'idée est d'élaborer et de construire cette fonction de façon à obtenir les SIL/PL requis déterminés dans le chapitre précédent. L'utilisation de sous-systèmes certifiés dans les systèmes de sécurité fonctionnelle peut réduire considérablement le travail du concepteur du système de sécurité. La mise en œuvre des fonctions de sécurité est plus facile si une partie des calculs de sécurité et de fiabilité est déjà faite et si les sous-systèmes sont certifiés.

Remarque :
Dans le cas où les sous-systèmes utilisés ne sont pas certifiés, il peut être nécessaire de réaliser des calculs de sécurité pour chacun d'entre eux. Les normes EN 62061 et EN ISO 13849-1 comprennent des informations sur le processus et les paramètres de calcul nécessaires.

Les processus de mise en œuvre et de vérification sont itératifs et réalisés en parallèle. L'idée est d'utiliser la vérification en tant qu'outil pendant la mise en œuvre pour garantir que le niveau de sécurité défini est atteint par le système mis en œuvre. Pour plus d'informations sur les processus de vérification, référez-vous à l'étape suivante.

Remarque :
La solidité du système est celle de son maillon faible. Ceci signifie qu'afin de satisfaire aux EESS définies par la Directive Machine, tous les sous-systèmes du système de sécurité fonctionnelle doivent atteindre au moins la valeur SIL/PL requise pour le système.

Il existe de nombreux logiciels de calcul sur le marché qui sont conçus pour la vérification des systèmes de sécurité fonctionnelle. Ces programmes facilitent l'ensemble du processus de création et de vérification du système.

Les étapes générales de mise en œuvre d'un système de sécurité fonctionnelle sont les suivantes :

1. *Définition des exigences de sécurité* sous la forme de SIL et PL, selon les normes EN 62061 ou EN ISO 13849-1.

2. *Sélection de l'architecture de système* à utiliser pour le système de sécurité.
   Les normes EN ISO 13849-1 et EN 62061 fournissent des architectures de base et des formules de calcul.

3. Détermination de :

- la catégorie B, 1, 2, 3 ou 4, telle que décrite dans la norme EN ISO 13849-1, ou
- l'architecture désignée A, B, C ou D, telle que décrite dans la norme EN 62061 pour les sous-systèmes et l'ensemble du système.

Pour plus d'informations sur les architectures désignées, référez-vous aux normes respectives.

1. *Construction du système à partir de sous-systèmes relatifs à la sécurité* - capteur/interrupteur, entrée, fonction logique, sortie et actionneur.

   Soit :
   - en utilisant des sous-systèmes certifiés (recommandé) ou
   - en réalisant des calculs de sécurité pour chaque sous-système.

   Le niveau de sécurité du système complet est établi en additionnant les niveaux de sécurité des sous-systèmes.

2. *Installation du système de sécurité.*

   Le système doit être installé correctement pour éviter les risques courants de défaillance liés à un câblage incorrect, à l'environnement ou à d'autres facteurs du même type. Un système de sécurité qui ne fonctionne pas correctement en raison d'une installation bâclée n'est que peu ou pas utile, voire source de risque.

3. *Vérification de la fonctionnalité du système.*

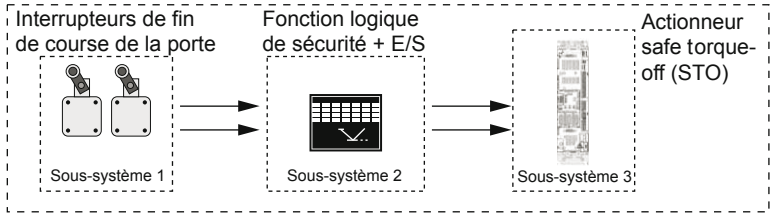


Figure 3-6 Structure d'une fonction de sécurité

ÉTAPE 6 : Vérification d'un système de sécurité fonctionnelle

La vérification du système de sécurité fonctionnelle prouve et garantit que le système de sécurité mis en œuvre satisfait aux exigences spécifiées pour le système lors de la phase de détermination des exigences de sécurité, et permet d'établir si la fonction de sécurité est viable.

La vérification ne devrait pas être réalisée après le processus de mise en œuvre, mais en même temps, de sorte que le résultat de la mise en œuvre soit en fait un système qui réponde aux exigences définies.

En plus de la vérification du SIL ou du PL du système, il est absolument nécessaire de vérifier la sécurité du système en réalisant des test de fonctionnalité.

Vérification du SIL du système de sécurité (EN 62061)
Pour vérifier les niveaux d'intégrité de sécurité, il faut montrer que la performance de sécurité, en d'autres termes la fiabilité de la fonction de sécurité créée est supérieure ou égale à l'objectif de performance requis défini pendant l'évaluation des risques. L'utilisation de sous-systèmes certifiés est recommandée, car le fabricant dispose déjà de valeurs définies pour la détermination de l'intégrité de sécurité systématique (SILCL) et de l'intégrité de sécurité du matériel (PFH_d) pour ceux-ci.

Étapes de la vérification du SIL d'un système de sécurité comprenant des sous-systèmes certifiés :

1. Détermination de l'intégrité de sécurité systématique pour le système en utilisant les valeurs de SILCL (SIL Claim Limit, limite de revendication de SIL) définies pour les sous-systèmes.

   Le SILCL représente la valeur de SIL maximum pour lequel le sous-système est structurellement adapté. Le SILCL est utilisé comme indicateur pour déterminer le SIL obtenu : le SILCL de l'ensemble du système ne peut pas être plus élevé que le SILCL le plus faible de tous les sous-systèmes.

2. Calcul de l'intégrité de sécurité du matériel pour le système en utilisant la PFH_d *(Probability of a dangerous Failure per Hour, Probabilité de défaillance dangereuse par heure)* définie pour les sous-systèmes. Les fabricants de sous-systèmes certifiés fournissent généralement les valeurs de PFH_d pour leurs équipements.

   La PFH_d est la valeur de la probabilité de défaillance du matériel utilisée pour déterminer le SIL.

3. Utilisation de la liste de contrôle de *CCF (Common Cause Failure, Défaillance de cause commune)* pour garantir que tous les aspects nécessaires de la création des systèmes de sécurité ont été pris en compte.

   La liste de contrôle des CCF est disponible dans la norme EN 62061 standard, Annexe F.

Calcul du nombre de points selon la liste et comparaison du résultat général avec les valeurs figurant dans la liste de la norme EN 62061, Annexe F, Tableau F.2 Estimation du facteur de CCF (β). Cette valeur est utilisée pour estimer la valeur de la probabilité PFH_d.

1. Détermination du SIL obtenu à partir du tableau correspondant.

Exemple de vérification du SIL :
Vérification du système de sécurité fonctionnelle de l'arbre rotatif :

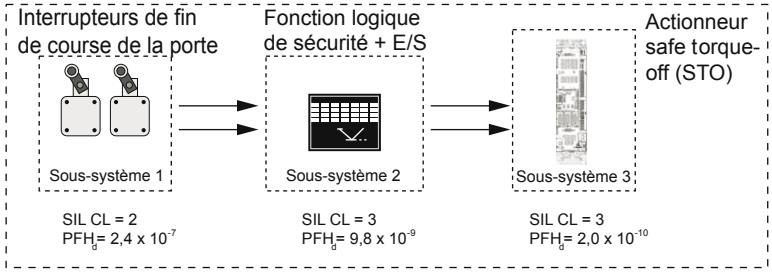


Figure 3-7 Exemple de vérification de SIL

Intégrité de sécurité systématique :
$SIL\ CL_{sys} \leq (SIL\ CL_{sous\text{-}système})_{le\ plus\ faible}$ -> SIL Claim Limit 2

Intégrité de sécurité du matériel :
$PFH_d = PFH_{d1}+PFH_{d2}+PFH_{d3} = 2{,}5 \times 10^{-7} < 10^{-6}$

Le système répond aux exigences de SIL2.

Tableau de détermination du SIL en fonction de la valeur de PFH_d obtenue pour l'ensemble du système de sécurité :

SIL	Probabilité de défaillance dangereuse par heure (1/h)
SIL 1	$\geq 10^{-6}$ jusqu'à $< 10^{-5}$
SIL 2	$\geq 10^{-7}$ jusqu'à $< 10^{-6}$
SIL 3	$\geq 10^{-8}$ jusqu'à $< 10^{-7}$

Tableau 3-1 Tableau de détermination du SIL

Verification du PL du système de sécurité (EN ISO 13849-1)
Pour vérifier le niveau de performance, il faut établir que le PL de la fonction de sécurité correspond au PL_r requis. Si plusieurs sous-systèmes forment une fonction de sécurité, leur niveau de performance doit être supérieur ou égal au niveau de performance requis pour ladite fonction de sécurité. L'utilisation de sous-systèmes certifiés est recommandée, car leur valeur de performance de sécurité a déjà été définie.

Étapes de la vérification du PL d'un système de sécurité comprenant des sous-systèmes certifiés :

1. Détermination de la susceptibilité du système aux CCF (défaillance de cause commune) au moyen de la liste de contrôle des CCF.

   Les tableaux de liste de contrôle des CCF figurent dans la norme EN ISO 13849-1:2008, Annexe 1. Le résultat minimum exigé est de 65 points.

2. Détermination du PL obtenu avec le graphique à barre en utilisant les paramètres déterminés :

   - catégorie,
   - $MTTF_d$ (Mean Time To dangerous Failure, Temps moyen avant défaillance dangereuse),
   - DC (Diagnostic Coverage, Couverture du diagnostic).

   Le $MTTF_d$ est le temps moyen s'écoulant avant une défaillance dangereuse. DC représente le nombre de défaillances dangereuses pouvant être détectées au moyen de diagnostics.

   Pour plus d'informations sur le détail des calculs, référez-vous à la norme EN ISO 13849-1.

3. Introduction du résultat dans le graphe PL, qui permet de déterminer le PL résultat.

Exemple de vérification du PL :
Vérification du système de sécurité fonctionnelle de l'arbre rotatif :

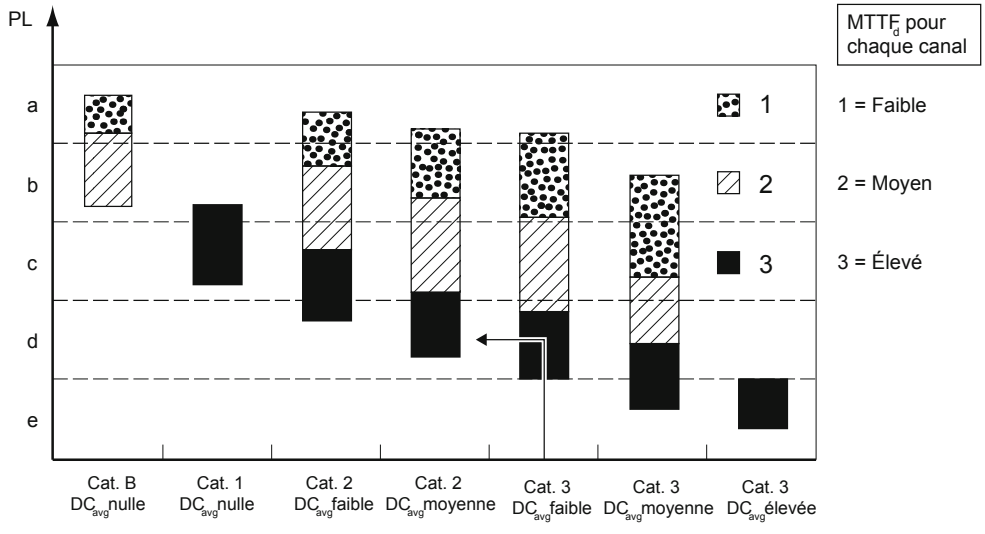


Figure 3-8 Exemple de vérification de PL

Pour atteindre le PL_r défini dans l'exemple précédent :

- architecture désignée de catégorie 3,
- valeur du $MTTF_d$ élevée,
- valeur de DC average (DC moyen) faible.

Le système obtient une valeur de PL égale à d.

Tableau de détermination du PL en fonction de la valeur de PFH_d obtenue pour l'ensemble du système de sécurité :

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

Tableau 3-2 Tableau de détermination du PL

Comparaison des valeurs de SIL et PL
Bien que les méthodes d'évaluation soient différentes dans les deux normes, les résultats d'évaluation peuvent être comparés sur la base de la défaillance du matériel :

Niveau d'intégrité de sécurité SIL	Niveau de performance PL
Pas de correspondance	a
1	b
1	c
2	d
3	e

Tableau 3-3 Tableau de comparaison de SIL et PL

ÉTAPE 7 : Validation du système de sécurité fonctionnelle

Chaque fonction de sécurité doit être validée afin de garantir qu'elle réduit le risque conformément aux exigences établies lors de la phase de l'appréciation du risque.

Afin de déterminer la validité du système de sécurité fonctionnelle, le système doit être examiné en fonction du processus d'appréciation du risque réalisé au début de la procédure destinée à répondre aux EESS de la Directive Machine. Le système est valide s'il réduit réellement les risques analysés et évalués lors du processus d'appréciation du risque.

ÉTAPE 8 : Documentation du système de sécurité fonctionnelle

La conception de la machine doit être documentée et la documentation pertinente destinée aux utilisateurs doit être élaborée afin que la machine réponde aux exigences définies dans la Directive Machine.

La documentation doit être soigneusement réalisée pour répondre à son objectif. Elle doit être précise et concise, et en même temps fournir les informations nécessaires et être facile à comprendre . Tous les risques résiduels doivent être documentés dans la documentation utilsateur, avec les instructions appropriées sur la manière d'utiliser la machine de façon sûre. La documentation doit être accessible et doit pouvoir être mise à jour. La documentation utilisateur est fournie avec la machine.

Pour plus d'informations sur la documentation requise et sur sa nature, référez-vous aux EESS dans l'Annexe 1 de la Directive Machine.

ÉTAPE 9 : Preuve de conformité

Avant qu'une machine ne puisse être mise sur le marché, le fabricant doit garantir que la machine est conforme aux normes harmonisées. Il faut aussi prouver que la combinaison des composants relatifs à la sécurité pour chaque fonction de sécurité satisfait aux exigences définies.

Pour prouver la conformité à la Directive Machine, il faut montrer que :

- La machine répond aux Exigences essentielles de santé et de sécurité (EESS) pertinentes décrites dans la Directive Machine.
- La machine répond aux exigences des autres Directives pouvant la concerner.
- La conformité à ces exigences peut être garantie en appliquant les normes harmonisées correspondantes.
- Le dossier technique est à jour et disponible.
  Le dossier technique démontre que la machine est conforme aux réglementations décrites dans la Directive Machine.

Remarque :
L'absence de dossier technique pourrait donner des raisons de douter de la conformité de la machine avec les EESS.

Le dossier technique doit couvrir la conception, la fabrication et le fonctionnement de la machine en tant que de besoin pour démontrer la conformité. Pour plus d'informations sur le contenu du dossier technique, référez-vous à l'Annexe VI de la Directive Machine 98/37/CE ou à l'Annexe de la nouvelle Directive Machine 2006/42/CE lorsque celle-ci sera devenue applicable.

- Les procédures d'évaluation de la conformité ont été appliquées. Les exigences spéciales pour les machines visées à l'Annexe IV de la Directive Machine sont respectées, lorsque c'est nécessaire.
- La déclaration de conformité CE a été faite et est fournie avec la machine.

Une fois que la conformité a été établie, un marquage CE est apposé.

Une machine portant un marquage CE et qui est accompagnée par une déclaration de conformité CE est supposée répondre aux exigences de la Directive Machine.

Glossaire

Marquage CE
Un marquage de conformité obligatoire apposé sur les machines et de nombreux autres types de produit mis sur le marché unique de l'Espace Économique Européen (EEE).
En apposant le marquage CE sur le produit, le fabricant garantit que le produit est conforme à toutes les exigences essentielles des Directives européennes correspondantes.

CCF, Défaillance de cause commune
Une situation dans laquelle plusieurs sous-systèmes tombent en panne en raison d'un unique évènement. Toutes les défaillances sont causées par l'évènement lui-même et ne sont pas des conséquences l'une de l'autre.

DC, Couverture du diagnostic
La couverture du diagnostic (DC) est l'efficacité de la surveillance des défaillances d'un système ou d'un sous système. C'est le rapport entre le taux d'apparition des défaillances dangereuses détectées et le taux d'apparition des défaillances dangereuses totales.

EESS, Exigences essentielles de santé et de sécurité
Les exigences auxquelles la machine doit satisfaire pour être en conformité avec la Directive Machine de l'Union européenne et obtenir la marquage CE. La liste de ces exigences se trouve dans l'Annexe I de la Directive Machine.

EN
Signifie «Euronorm». Ce préfixe est utilisé pour les normes harmonisées.

Dommage
Blessure physique ou atteinte à la santé.

Norme harmonisée
Une norme européenne qui a été préparée sous le mandat de la Commission européenne ou du Secrétariat de l'AELE dans le but d'apporter un soutien aux exigences essentielles d'une directive et qui est obligatoire au regard de la législation de l'UE.

Danger
Source potentielle de dommage.

CEI, Commission Electrotechnique internationale
Une organisation internationale de normalisation qui rassemble tous les comités électrotechniques nationaux.
www.iec.ch

ISO, Organisation internationale de normalisation
Une fédération internationale d'organismes nationaux de normalisation.
www.iso.org

$MTTF_d$, Temps moyen avant défaillance dangereuse
Durée moyenne statistique de fonctionnement avant défaillance dangereuse.

PFH_d, Probabilité de défaillance dangereuse par heure
Probabilité moyenne de l'occurence d'une défaillance dangereuse par heure. La **PFH_d,est la valeur utilisée pour déterminer le SIL ou le PL d'une fonction de sécurité.**

PL, Niveau de performance
Niveaux (a, b, c, d, e) spécifiant la capacité d'un système de sécurité à exécuter une fonction de sécurité en conditions prévisibles.

PL_r
Niveau de performance requis (basé sur l'évaluation des risques).

Risque
Une combinaison de la probabilité d'un dommage et de sa gravité.

Fonctions de sécurité
Une fonction conçue pour améliorer la sécurité d'une machine et dont la défaillance peut entraîner une augmentation du risque immédiate.

SIL, Niveau d'intégrité de sécurité
Niveaux (1, 2, 3, 4) spécifiant la capacité d'un système de sécurité électrique à exécuter une fonction de sécurité en conditions prévisibles. Seuls les niveaux 1 à 3 sont utilisés pour les machines.

SILCL, limite de revendication de SIL
Niveau d'intégrité de sécurité (SIL) maximum pouvant être revendiqué pour un système de sécurité électrique, compte tenu des contraintes architecturales et de l'intégrité de sécurité systématique.

Sous-système
Un composant d'une fonction de sécurité qui possède son propre niveau de sécurité (SIL/PL), qui affecte le niveau de sécurité de l'ensemble de la fonction. La défaillance de l'un des sous-systèmes entraîne la défaillance de l'ensemble de la fonction de sécurité.

Index

ABB France
Division DM
Activité Moteurs, Machines & Drives
465 avenue des Pré Seigneurs
La Boisse
01124 Montluel Cedex
France
Téléphone +33 (0)4 37 40 40 00
Télécopieur +33 (0)4 37 40 40 72

www.abb.fr/drives
www.abb.fr/drivespartners

3AUA0000079965 REV C FR 1.5.2010