

Sécurité des machines : sécurité fonctionnelle et mise en œuvre de la nouvelle Directive Machines

Résumé

Ce document traite des modifications apportées aux normes relatives à la conception des systèmes de contrôle de la sécurité. Les normes EN 62061 et EN ISO 13849-1 traitent toutes deux de la sécurité fonctionnelle des systèmes de commande des machines, mais utilisent des techniques et des termes légèrement différents pour déterminer les performances. De nombreux utilisateurs sont déroutés par les conseils contradictoires des fournisseurs, qui peuvent préférer une norme plutôt qu'une autre. Ce document clarifie les différences entre les normes EN ISO 13849-1 et EN 62061 et traite les points principaux que les constructeurs de machines doivent garder à l'esprit pour chacune d'elles.

Sommaire

Nouvelle Directive Européenne Machines	3
La nouvelle Directive Européenne Machines 2006/42/CE, publiée en 2010, remplace l'ancienne Directive Machines 98/37/CE. Dans le même temps, les normes disponibles pour la conception des systèmes de commande relatifs à la sécurité ont changé.	
Approche de la sécurité fonctionnelle	4
Les nouvelles normes de sécurité fonctionnelle visent à encourager les concepteurs à se concentrer davantage sur les fonctions requises pour réduire chaque risque individuel, ainsi que sur les performances nécessaires pour chaque fonction, plutôt que de compter simplement sur des composants en particulier. Ces normes permettent d'atteindre des niveaux de sécurité plus élevés tout au long du cycle de vie de la machine.	
Quelle norme ?	7
Les normes EN 62061 et EN ISO 13849-1 traitent toutes deux de la sécurité fonctionnelle des systèmes de commande des machines, mais utilisent des techniques et des termes légèrement différents pour déterminer les performances. Beaucoup d'utilisateurs sont déroutés par les conseils contradictoires des fournisseurs, qui peuvent préférer une norme à une autre.	
La sécurité fonctionnelle dans son contexte	9
La sécurité fonctionnelle fait partie intégrante de la conception des systèmes de commande relatifs à la sécurité. D'autres facteurs sont toutefois à prendre en compte lors de leur conception.	

Nouvelle Directive Européenne Machines

La nouvelle Directive Européenne Machines 2006/42/CE, publiée en 2010, remplace l'ancienne Directive Machines 98/37/CE.

Les utilisateurs de la norme EN 954-1 seront familiers avec l'ancien « graphe des risques » utilisé pour la conception de parties des circuits de commande électriques relatives à la sécurité dans les catégories B, 1, 2, 3 ou 4. Les utilisateurs devaient subjectivement évaluer la gravité des blessures, la fréquence d'exposition et la possibilité d'évitement afin de déterminer la catégorie requise pour chaque partie relative à la sécurité. Cette catégorie spécifiait alors le comportement requis du circuit de sécurité lorsqu'il faisait face à une erreur, mais elle ne traitait pas la probabilité qu'une erreur se produise.

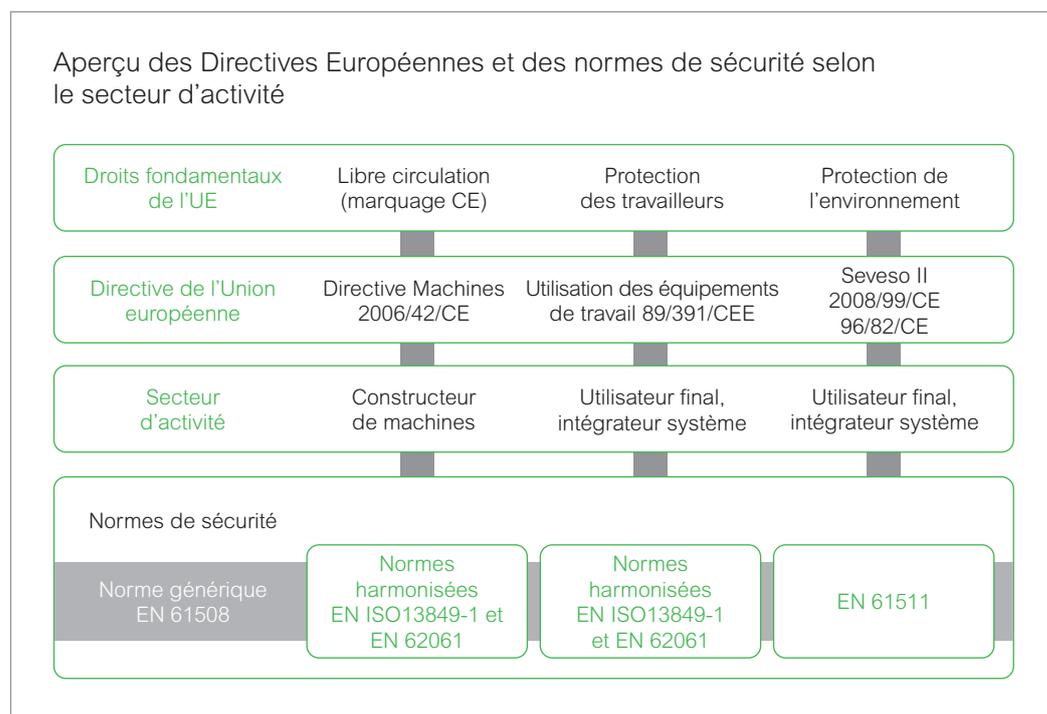
Avec l'utilisation croissante d'électronique programmable et non programmable dans ces systèmes, la sécurité ne peut plus être mesurée uniquement en termes de catégories. De plus, la norme précédente ne fournit aucune information sur la probabilité de défaillance (EN ISO 13849-1).

Ces dernières années, le concept de *sécurité fonctionnelle* a fait son apparition. Ce concept fait référence à la sécurité globale de l'équipement sous contrôle (EUC) et du système de commande de l'EUC. La sécurité fonctionnelle dépend du fonctionnement correct ou de l'exploitation correcte des systèmes électriques, électroniques, électroniques programmables et d'autres systèmes technologiques liés à la sécurité, ainsi que des possibilités de réduction des risques externes. Il ne s'agit pas de l'attribut d'un composant en particulier ou d'un type spécifique d'appareil, mais plutôt de l'ensemble de l'EUC et de son système de commande. La sécurité fonctionnelle s'applique à toutes les parties qui contribuent à l'exécution d'une fonction de sécurité, comme par exemple les « dispositifs » d'entrée, tels que les interrupteurs ou les capteurs de sécurité, les solveurs logiques tels que les modules de sécurité, les contrôleurs de sécurité et les automates programmables de sécurité (y compris leurs logiciels et firmwares), ainsi que les dispositifs de sortie tels que les contacteurs, les variateurs de vitesse ou les servomoteurs.

Le terme *fonctionnement correct* ne signifie pas uniquement que l'opération correspond à celle qui était prévue, il signifie surtout que son fonctionnement est correct. Par conséquent, une sélection appropriée des fonctions est primordiale. Dans le passé, les concepteurs avaient tendance à choisir des composants dans la catégorie la plus élevée de la norme EN 954-1, au lieu de choisir des composants dans une catégorie inférieure qui pourraient finalement offrir des fonctions plus appropriées. Cela était souvent dû à l'idée fautive que les catégories de la norme EN 954-1 étaient hiérarchisées, par exemple la catégorie 3 serait « meilleure » que la catégorie 2.



Les nouvelles normes EN ISO 13849-1 et EN 62061 permettent de remédier aux défauts de la norme EN 954-1. Bien qu'elles exigent toujours la considération de l'architecture du circuit comme dans la norme 954-1, elles prennent également en compte la fiabilité des composants du circuit de sécurité et la capacité du circuit à détecter ou diagnostiquer des erreurs ainsi que la probabilité de défaillances de causes communes (EN ISO 13849-1). La performance de chaque fonction de sécurité est spécifiée soit en SIL (Safety Integrity Level ou niveau d'intégrité de sécurité 1, 2 ou 3) selon la norme EN 62061, soit en PL (Performance Level ou niveau de performance a, b, c, d ou e) selon la norme EN ISO 13849-1.

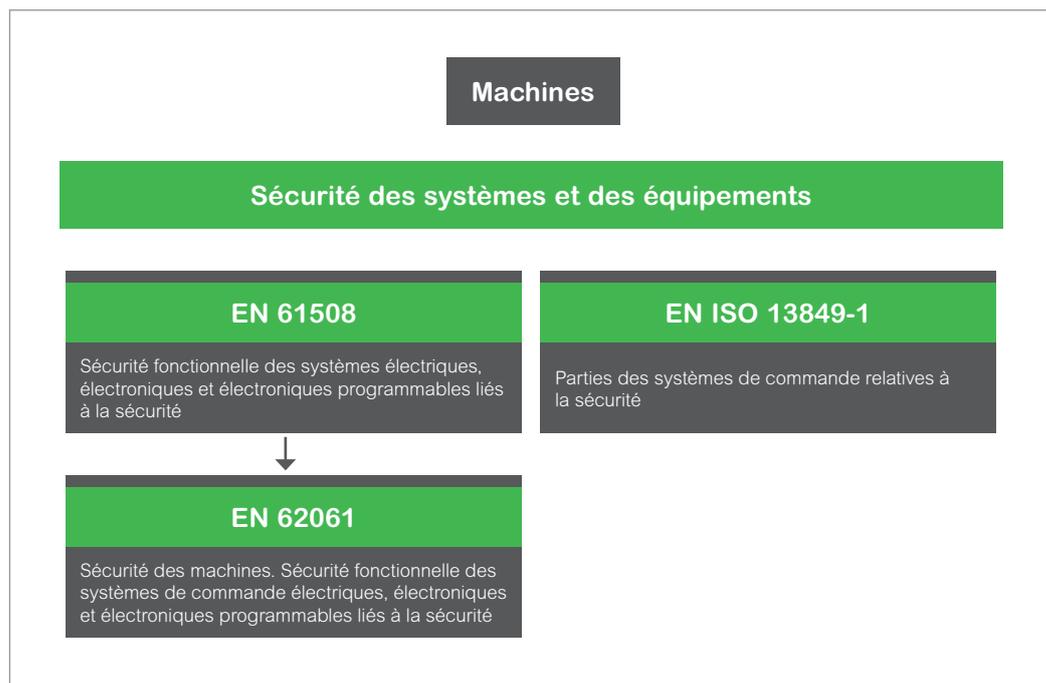


Approche de la sécurité fonctionnelle

Les nouvelles normes de sécurité fonctionnelle visent à encourager les concepteurs à se concentrer davantage sur les fonctions requises pour réduire chaque risque individuel, ainsi que sur les performances nécessaires pour chaque fonction, plutôt que de compter simplement sur des composants en particulier. Ces normes permettent d'atteindre des niveaux de sécurité plus élevés tout au long du cycle de vie de la machine.

Dans l'ancienne norme EN 954-1, les catégories (B, 1, 2, 3 et 4) déterminaient comment un circuit de commande électrique de sécurité devait se comporter en cas d'erreur. Les concepteurs peuvent suivre aussi bien la norme EN ISO 13849-1 que la norme EN 62061 pour démontrer la conformité avec la Directive Machines. Ces deux normes tiennent compte non seulement de la possibilité qu'une erreur se produise, mais aussi de la probabilité qu'elle puisse se produire.

Cela signifie qu'il y a un élément de conformité quantifiable et probabiliste : les constructeurs de machines doivent être en mesure de déterminer si leur circuit de sécurité répond aux niveaux requis d'intégrité de sécurité (SIL) ou de performance (PL). Les tableaux et les concepteurs doivent savoir que les fabricants des composants utilisés dans les circuits de sécurité (tels que les composants de détection, les solveurs logiques de sécurité et les dispositifs de sortie comme les contacteurs) doivent fournir des données détaillées sur leurs produits.



Ces données peuvent être assez complexes et les nouvelles normes ont des exigences différentes, il peut donc être difficile de comprendre la signification de tous les chiffres et acronymes.

Voici les points principaux que les constructeurs de machines doivent garder à l'esprit pour la norme EN ISO 13849-1 :

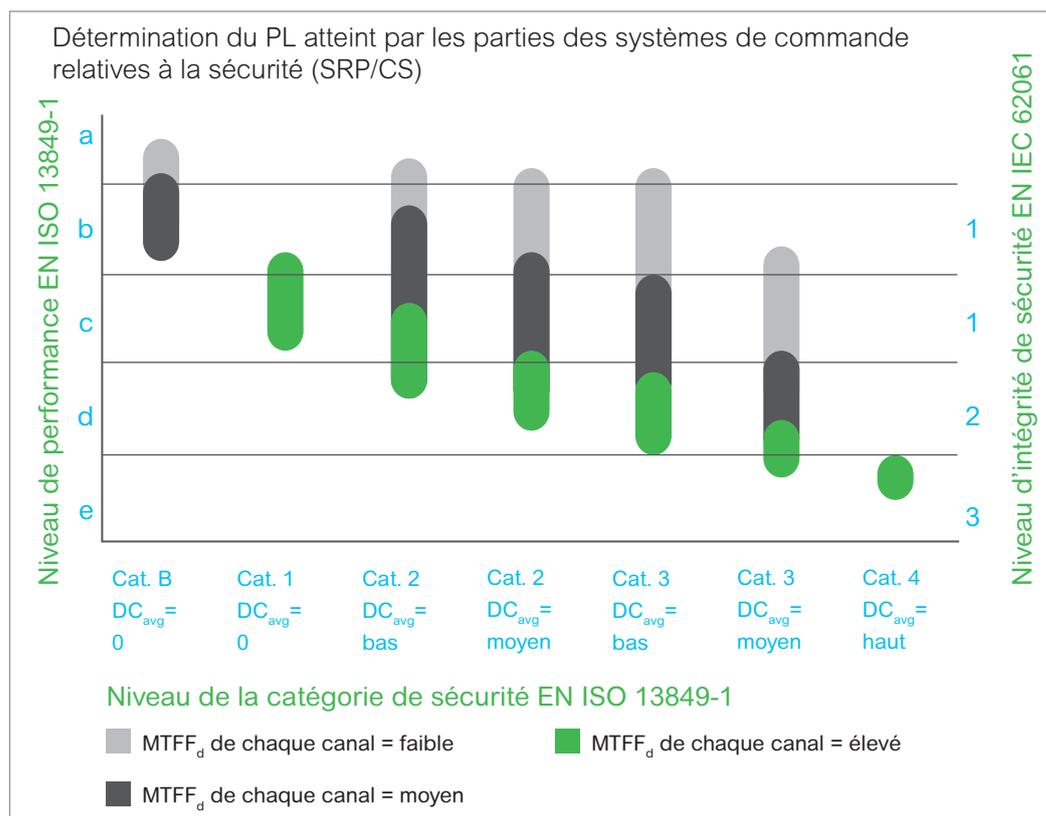
- **Le niveau de performance (Performance Level - PL)** est déterminé par l'architecture du circuit (similaire aux catégories B, 1, 2, 3, et 4 de l'EN 954-1) ainsi que par les valeurs MTTFd et DC. La norme ISO définit cinq niveaux de performance allant de PL a (probabilité d'erreur la plus élevée) à PL e (probabilité d'erreur la plus faible) Si un constructeur indique un PL spécifique pour un composant (tel qu'un module de sécurité), cela signifie que pour un circuit incorporant ce composant, ce PL est le niveau le plus élevé qu'il puisse atteindre.
- **Le temps moyen avant une défaillance dangereuse (Mean Time To Dangerous Failure - MTTFd) (EN ISO 13849-1)** correspond au délai moyen avant que la défaillance d'un composant n'entraîne la défaillance d'une fonction de sécurité. Le MTTFd est classé en trois niveaux : élevé (30-100 ans), moyen (10-30 ans) ou faible (3-10 ans). Remarque : si le MTTFd du composant est de 100 ans, cela ne garantit pas qu'il ne puisse pas rencontrer d'erreur avant.
- **La couverture de diagnostic (Diagnostic Coverage - DC)** est la capacité d'un composant ou d'un circuit à détecter ou diagnostiquer une erreur le concernant (un court-circuit, par exemple). Plus le DC est élevé et plus la probabilité d'erreurs matérielles non identifiées et potentiellement dangereuses est faible.
- **Les défaillances de causes communes (Common Cause Failures - DCC) (EN ISO 13849-1)** correspondent à des problèmes dans l'architecture à double canal dus à une erreur similaire dans les deux canaux (comme un court-circuit). Des mesures peuvent être prises pour éviter les défaillances de causes communes. Le concepteur peut par exemple utiliser des composants différents fonctionnant dans des modes différents dans les systèmes à deux canaux.

Points clés de la norme EN 62061 :

- **Le niveau d'intégrité de sécurité (Safety Integrity Level - SIL)** est le niveau discret permettant de déterminer les exigences d'intégrité de sécurité du système de commande relatif à la sécurité. Cette norme définit trois niveaux, allant de un (niveau bas) à trois (niveau élevé). Si un fabricant revendique un SIL spécifique pour un composant (tel qu'un automate de sécurité), il s'agit alors du SIL maximal pouvant être revendiqué pour tout système utilisant ce composant comme un sous-système.
- **La limite de revendication de SIL (SIL Claim Limit - SILCL)** s'applique aux sous-systèmes au sein d'un système de sécurité. Un sous-système est défini comme une partie d'un système ou circuit de sécurité, dont une erreur entraînerait une défaillance de la fonction de sécurité. Le SILCL est le SIL le plus élevé pouvant être revendiqué en ce qui concerne les contraintes architecturales et l'intégrité de sécurité systématique.
- **La probabilité de défaillance par heure (Probability of dangerous Failure per Hour - PFH) (EN 62061)** est une mesure de la fiabilité d'un composant, d'un sous-système ou d'un système ou circuit de sécurité complet. Elle correspond au MTTFd de la norme EN ISO 13849-1.
- **Taux de défaillances non dangereuses (Safe Failure Fraction - SFF) (EN 62061)** d'un sous-système correspond au ratio entre d'une part le taux moyen d'erreurs non dangereuses additionnées aux erreurs dangereuses détectées du sous-système et d'autre part le taux d'erreurs moyen total du sous-système.

Les valeurs B10 et B10d, utilisées pour évaluer la conformité, sont des caractéristiques de fiabilité pour les composants électromécaniques. B10 correspond au nombre d'opérations pour lesquelles 10 % de la population va connaître des défaillances et B10d correspond au nombre de cycles après lesquels 10 % de la population aura fait face à une défaillance dangereuse.

Normalement, il n'existe pas de valeurs MTTFd ou PFHd publiées pour les composants électromécaniques, car les taux d'erreurs dépendent du taux d'activation par heure, qui est spécifique à l'application. Toutefois, les concepteurs peuvent utiliser B10 ou B10d avec des données connues sur les machines (par exemple, les interrupteurs de protection peuvent s'activer un nombre de fois connu par heure lors du chargement d'une machine), afin de calculer le MTTFd ou le PFHd des sous-systèmes contenant ces composants.



Quelle norme ?

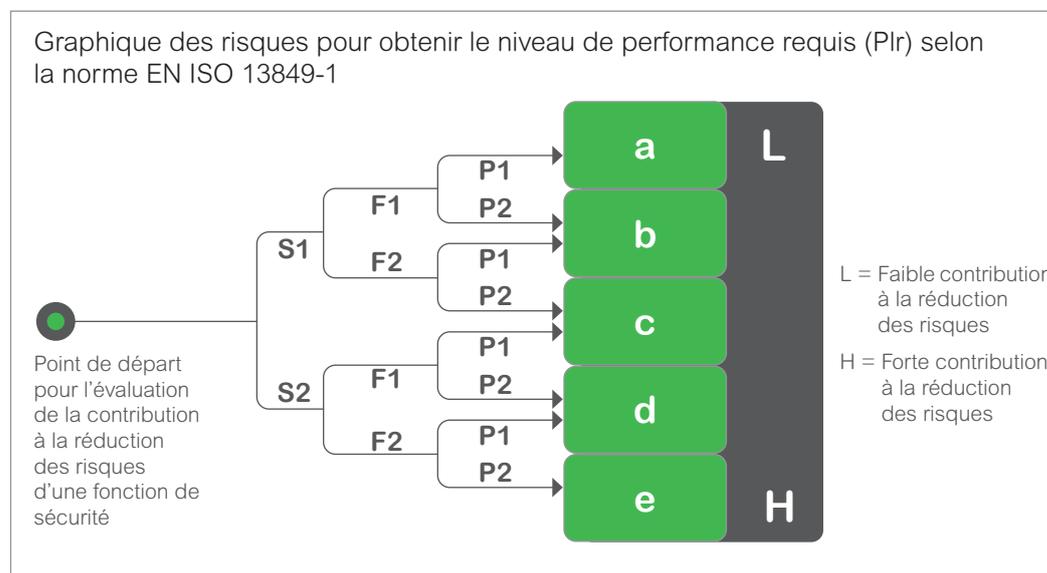
Les normes EN 62061 et EN ISO 13849-1 traitent toutes deux de la sécurité fonctionnelle des systèmes de commande des machines, mais utilisent des techniques et des termes légèrement différents pour déterminer les performances. Beaucoup d'utilisateurs sont déroutés par les conseils contradictoires des fournisseurs, qui peuvent préférer une norme à une autre.

Avoir deux normes parmi lesquelles choisir n'est pas idéal. Cela peut entraîner des problèmes d'intégration entre les composants et affecter les relations entre les fabricants, les constructeurs de machines et les utilisateurs finaux. Cependant, le Comité Européen de Normalisation Electrotechnique (CENELEC) et le Comité Européen de Normalisation (CEN) ont tous deux des idées claires sur la manière de réglementer la sécurité fonctionnelle lors de la construction de machines. À ce titre, ils ont tous deux établi des normes pouvant fournir une présomption de conformité aux exigences appropriées de la Directive Machines.

Les normes EN 62061 (publiée par le CENELEC) et EN ISO 13849-1 (publiée par le CEN) ont toutes deux le même objectif : minimiser l'attention sur le comportement des composants individuels pour se concentrer davantage sur la sécurité fonctionnelle de l'ensemble de la machine. Ces deux normes visent à réduire la possibilité de blessure. Utilisées correctement, elles réduisent ainsi souvent la probabilité d'erreur de la machine. Si ces normes peuvent permettre d'atteindre des niveaux similaires de réduction des risques, elles atteignent cet objectif de manières très différentes.

Ces normes utilisent des termes différents pour désigner les niveaux de sécurité fonctionnelle des circuits : la norme EN 62061 définit trois niveaux d'intégrité de sécurité (SIL), tandis que la norme EN ISO 13849-1 spécifie cinq niveaux de performance (PL). Malgré ces différences terminologiques, certaines exigences (telles que la probabilité de défaillance dangereuse par heure (EN 62061)) sont faciles à comparer. Les normes adoptent toutefois des approches différentes.

Les normes EN 62061 et EN ISO 13849-1 présentent toutes deux des points forts et des faiblesses, et il existe des arguments pour et contre l'utilisation de l'une ou l'autre, selon l'application et les préférences individuelles du fabricant. À moins qu'une norme de type C spécifique à une machine ne définisse un SIL ou un PL, les concepteurs sont libres de choisir la norme à utiliser. Quelle que soit la norme, elle doit cependant être utilisée dans son intégralité et les deux normes ne peuvent pas être mélangées dans une même fonction de sécurité.



Les concepteurs familiers avec les anciennes catégories de l'EN 954-1 peuvent trouver la norme EN ISO 13849-1 plus facile à utiliser. Comme sa prédécesseur, la norme applique un « graphe des risques » facile à lire, afin de déterminer le niveau de performance (PL) requis pour les fonctions de sécurité individuelle après qu'une évaluation des risques ait été effectuée conformément à la norme EN ISO 12100. Cela signifie que les fonctions de sécurité peuvent être attribuées à la performance appropriée afin de traiter chaque risque individuel. Cependant, utiliser uniquement le graphe des risques n'est pas suffisant, le concepteur du système doit également faire d'autres choix.

Le PL n'est pas déterminé uniquement par l'architecture du système. Il se base aussi sur le temps moyen avant défaillance dangereuse (MTTFd) (EN ISO 13849-1) et sur la couverture de diagnostic (DC). L'un des avantages majeurs de cette approche est que les concepteurs peuvent utiliser des systèmes de circuits plus simples, à condition de choisir des composants à haute fiabilité ou des composants présentant des valeurs MTTFd plus élevées. Cela est dû au fait que les cinq niveaux de performance (PL) définis dans l'EN ISO 13849-1 sont des groupes de valeurs plutôt que des catégories discrètes.

L'avantage de la norme EN ISO 13849-1 par rapport à l'ancienne norme est qu'elle peut rendre la sécurité financièrement plus rentable pour les concepteurs, en leur permettant de concevoir des circuits de sécurité utilisant des composants plus fiables, et en plus petite quantité. Par exemple, avec la nouvelle norme, on peut obtenir un PL d, en utilisant soit une conception à canal unique de catégorie 2 avec des composants à haute fiabilité, soit une architecture à double canal de catégorie 3 avec des composants ayant une fiabilité plus faible. Le concepteur dispose donc d'un choix plus large.

Des outils (tels que SISTEMA, créé par l'Institut allemand de la sécurité et de la santé au travail), sont disponibles pour aider les développeurs et les testeurs à évaluer la sécurité des machines conformément à la norme EN ISO 13849-1.

Pour les applications présentant des exigences plus robustes en matière de gestion de la sécurité fonctionnelle, la norme EN 62061 peut être plus adaptée. Elle fournit plus de conseils sur les exigences organisationnelles pour garantir la mise en place et le maintien de la sécurité fonctionnelle. De plus, cette norme prend davantage en considération l'effet des modifications qui peuvent être apportées soit lors de la mise en service d'un nouvel équipement, soit pendant la durée de vie de la machine. Par exemple, les ingénieurs procédant à la mise en service doivent prendre en compte les effets probables de toute modification proposée, ainsi que la mesure maximale dans laquelle le système de commande peut être modifié avant qu'une revalidation ne soit nécessaire.

Un groupe de travail conjoint ISO et IEC a élaboré une comparaison des deux normes. Ce document a été publié par les deux organisations en tant que rapport technique – rapport n'ayant pas le même statut qu'un rapport standard mais qui est plus rapide à publier.



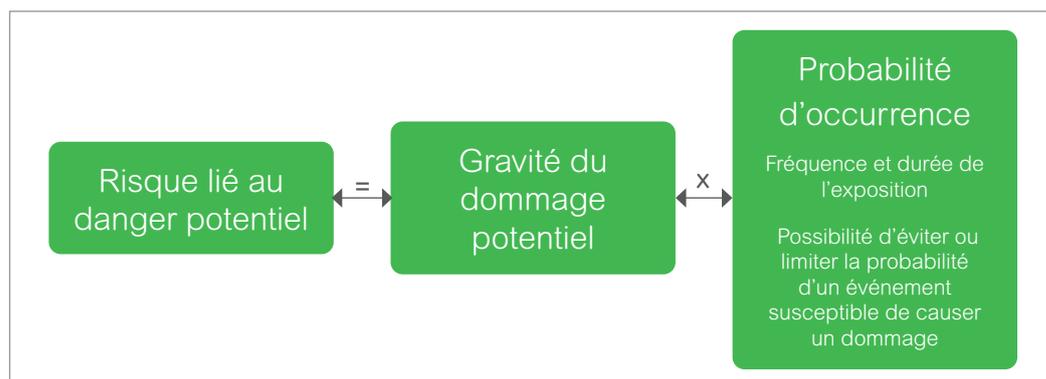
La sécurité fonctionnelle dans son contexte

La sécurité fonctionnelle fait partie intégrante de la conception de systèmes de commande sûrs. D'autres facteurs sont cependant à prendre en considération lors de la conception des systèmes de commande.

Bien que la sécurité fonctionnelle soit importante, elle n'est pertinente que lorsque d'autres facteurs ont été pris en compte afin de replacer le calcul de la sécurité fonctionnelle dans son contexte. Cela signifie qu'il faut analyser des aspects tels que la conception de base de la machine et son équipement électrique, ainsi que son équipement pneumatique et hydraulique.

De plus, les normes de sécurité fonctionnelle ne sont utiles que dans le contexte de normes plus fondamentales telles que l'EN ISO 12100 (Sécurité des machines – Principes généraux de conception – Évaluation et réduction des risques), et l'EN 60204-1 (Sécurité des machines – Équipement électrique des machines).

Bien que les normes EN ISO 13849-1 et EN 62061 soient les normes de sécurité fonctionnelle privilégiées pour les systèmes de commande, elles ne remplacent pas la nécessité d'une évaluation et d'un plan de réduction des risques avant de concevoir des systèmes de commande relatifs à la sécurité. En outre, elles ne remplacent pas les bonnes pratiques d'ingénierie. Les niveaux de performance (PL) et les niveaux d'intégrité de sécurité (SIL) ne sont pas une science exacte mais plutôt des facteurs de qualité qui doivent être utilisés uniquement à titre indicatif.

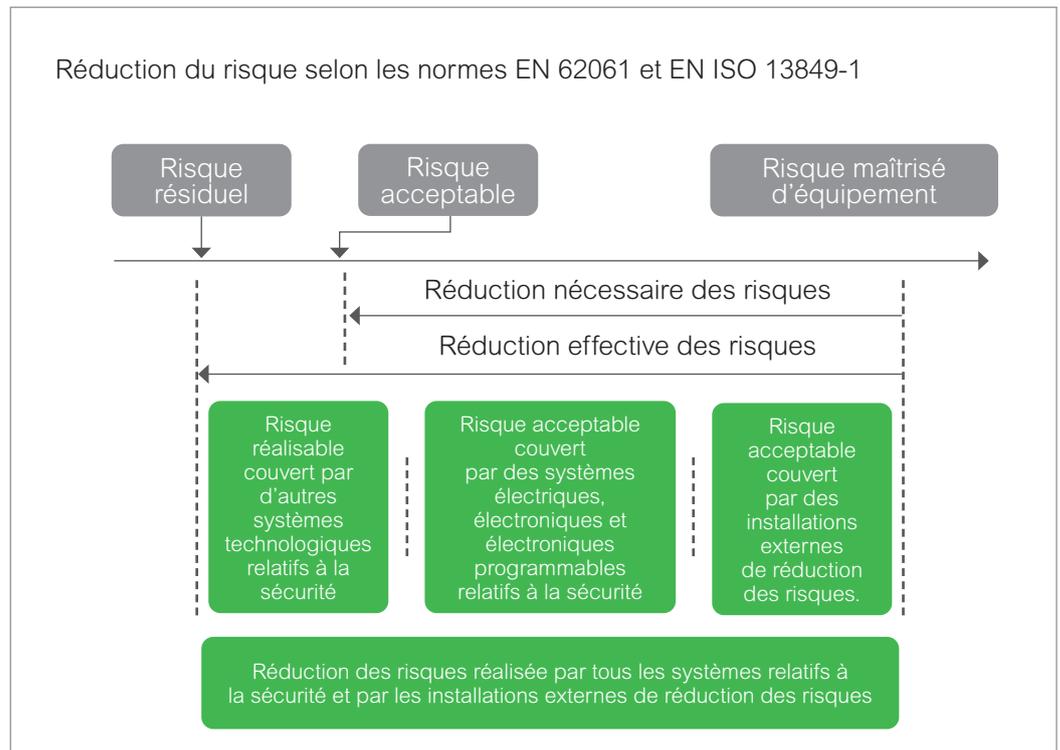


L'évaluation et la réduction des risques doivent être effectuées conformément à la norme EN ISO 12100. L'objectif principal est de réduire raisonnablement les risques autant que possible. La hiérarchie de la réduction des risques peut se décrire en trois étapes.

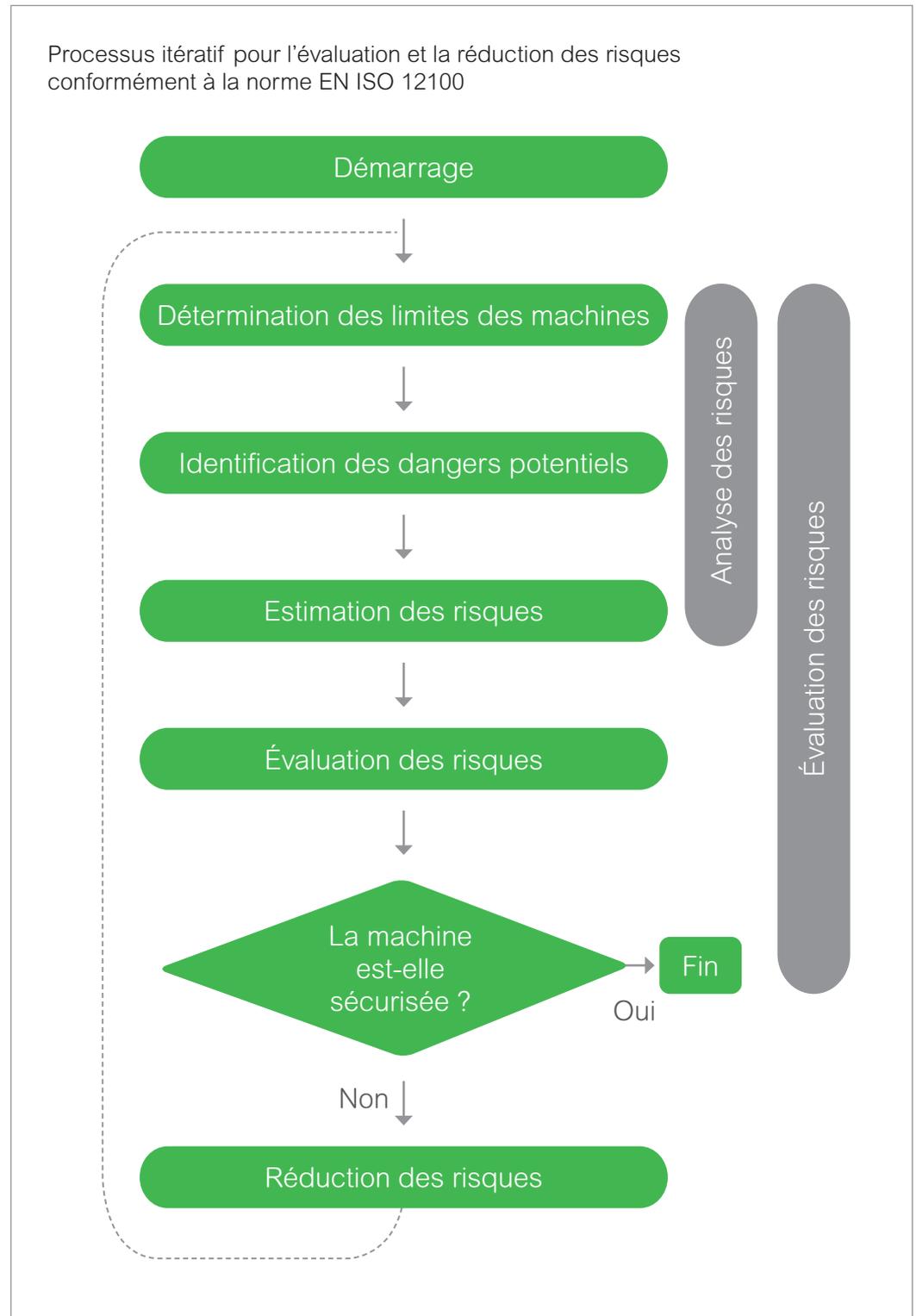
- **Étape 1** : éliminer si possible le danger potentiel (conception de sécurité intrinsèque) conformément à la norme EN ISO 12100. Exemple : placer une barrière de protection autour de la partie mobile dangereuse afin de protéger l'utilisateur.
- **Étape 2** : se prémunir contre les dangers potentiels lorsqu'une conception de sécurité intrinsèque n'est pas réalisable. Exemple : mettre en œuvre des mesures de protection par le biais de systèmes de commande relatifs à la sécurité tels que des protections avec des interrupteurs de verrouillage ou des zones d'accès libre protégées par une barrière lumineuse.
- **Étape 3** : appliquer des mesures de protection complémentaires. Exemple : fournir au personnel des formations, des panneaux d'avertissements, des conseils d'utilisation et des équipements de protection individuelle.

Les utilisateurs doivent répéter ce cycle d'évaluation des risques suivi d'une réduction des risques, afin de réduire les risques à un niveau acceptable et afin de s'assurer qu'un risque supplémentaire n'ait pas été introduit.

Le processus de réduction des risques peut nécessiter l'utilisation de systèmes de commande relatifs à la sécurité conçus selon les normes EN ISO 13849-1 et EN 62061. Cependant, la sécurité globale d'une machine dépendra aussi de sa conformité à d'autres normes telles que l'EN 60204-1 pour l'équipement électrique complet.



Un guide clair et concis détaillant les exigences de ces deux normes de sécurité fonctionnelle et proposant des exemples concrets est disponible en téléchargement sur la page Sécurité des machines du site web de Schneider Electric.



Pour plus d'informations, veuillez vous rendre sur :

www.se.com/fr/fr/work/campaign/smart-machines/safety.jsp

Life Is On



se.com/fr

Schneider Electric France

35 rue Joseph Monier
92500 Rueil-Malmaison, France
Conseils : 0 825 012 999*
Services : 0810 102 424**

* Services 0,15 €/appel + prix de l'appel
** Service gratuit + prix de l'appel

© 2020 Schneider Electric. Tous droits réservés. Life Is On Schneider Electric est une marque commerciale appartenant à Schneider Electric SE, ses filiales et ses sociétés affiliées.
En raison de l'évolution des normes et du matériel, les caractéristiques indiquées par les textes et les images de ce document ne nous engagent qu'après confirmation par nos services.
Life Is On : la vie s'illumine - Conception, réalisation : Schneider Electric, DMCF, @Laurent Gasm

ZZ7014 - 04/2021 (source 998-20499581)