Institut National de Recherche et de Sécurité

Sécurité des machines

Principes de conception des systèmes de commande

L'Institut national de recherche et de sécurité (INRS)

Dans le domaine de la prévention des risques professionnels, l'INRS est un organisme scientifique et technique qui travaille, au plan institutionnel, avec la CNAM, les Carsat, Cramif, CGSS et plus ponctuellement pour les services de l'État ainsi que pour tout autre organisme s'occupant de prévention des risques professionnels.

Il développe un ensemble de savoir-faire pluridisciplinaires qu'il met à la disposition de tous ceux qui, en entreprise, sont chargés de la prévention : chef d'entreprise, médecin du travail, instances représentatives du personnel, salariés. Face à la complexité des problèmes, l'Institut dispose de compétences scientifiques, techniques et médicales couvrant une très grande variété de disciplines, toutes au service de la maîtrise des risques professionnels.

Ainsi, l'INRS élabore et diffuse des documents intéressant l'hygiène et la sécurité du travail : publications (périodiques ou non), affiches, audiovisuels, sites Internet... Les publications de l'INRS sont diffusées par les Carsat. Pour les obtenir, adressez-vous au service Prévention de la caisse régionale ou de la caisse générale de votre circonscription, dont l'adresse est mentionnée en fin de brochure.

L'INRS est une association sans but lucratif (loi 1901) constituée sous l'égide de la CNAM et soumise au contrôle financier de l'État. Géré par un conseil d'administration constitué à parité d'un collège représentant les employeurs et d'un collège représentant les salariés, il est présidé alternativement par un représentant de chacun des deux collèges. Son financement est assuré en quasi-totalité par la CNAM sur le Fonds national de prévention des accidents du travail et des maladies professionnelles.

Les caisses d'assurance retraite et de la santé au travail (Carsat), la caisse régionale d'assurance maladie d'Île-de-France (Cramif) et les caisses générales de sécurité sociale (CGSS)

Les caisses d'assurance retraite et de la santé au travail, la caisse régionale d'assurance maladie d'Île-de-France et les caisses générales de sécurité sociale disposent, pour participer à la diminution des risques professionnels dans leur région, d'un service Prévention composé d'ingénieurs-conseils et de contrôleurs de sécurité. Spécifiquement formés aux disciplines de la prévention des risques professionnels et s'appuyant sur l'expérience quotidienne de l'entreprise, ils sont en mesure de conseiller et, sous certaines conditions, de soutenir les acteurs de l'entreprise (direction, médecin du travail, instances représentatives du personnel, etc.) dans la mise en œuvre des démarches et outils de prévention les mieux adaptés à chaque situation. Ils assurent la mise à disposition de tous les documents édités par l'INRS.

Conception graphique et mise en pages : Patricia Fichou. Illustrations : Sophie Boulet. Photos : © 123rf

Sécurité des machines

Principes de conception des systèmes de commande

ED 6310
février 2019

SOMMAIRE

Ce document a été réalisé par un groupe de travail INRS piloté par James Baudoin et composé de :
Jean Paul Bello, Jean Christophe Blaise, Sandrine Hardy et Jean Louis Poyard

Afin de réduire le nombre d'accidents du travail de façon pérenne, la sécurité doit être intégrée dès la conception des machines. Cela se traduit par la mise en œuvre de mesures de prévention pour supprimer ou réduire les risques pouvant potentiellement survenir. Certaines d'entre elles, pour assurer leur rôle, sont dépendantes d'un système de commande.

Cette brochure traite des principes de conception des systèmes de commande de machines, concernant les parties relatives à la sécurité.
Elle s'adresse dans un premier temps à ceux qui désirent comprendre la démarche globale à appliquer pour leur conception. Elle fournit des informations pour permettre l'assimilation et l'application des référentiels normatifs correspondants et rappelle notamment les notions relatives à l'appréciation du risque et à sa réduction. La problématique des systèmes de commande relatifs à la sécurité est resituée dans le processus global de réduction du risque.

Après avoir souligné la nécessité de déterminer, pour chaque fonction de sécurité, ses spécifications et son niveau minimum de sécurité, cette brochure fournit des repères pour traiter de ces points. Pour ceux qui veulent aller plus loin dans la démarche, elle traite plus particulièrement de la mise en œuvre de la norme NF EN ISO 13849-1 [1] et des principales phases de conception préconisées. Certains points particuliers sont précisés à l'aide d'exemples.
Un exemple d'application de la démarche globale de conception d'un système de commande est présenté au chapitre B.

Pour faciliter la compréhension de la brochure, il est conseillé, en cours de lecture, de se référer au chapitre B et aux parties concernées.

→ ***Avertissement***

Ce document ne se substitue en aucun cas à la norme, dont la lecture préalable et l'utilisation en cours de conception restent indispensables. En effet, il n'intègre pas et ne rappelle pas l'ensemble de ses préconisations.

CHAPITRE

A

DÉMARCHE GLOBALE DE CONCEPTION DES SYSTÈMES DE COMMANDE

1 LE RISQUE

1.1. Notions

Les machines et plus généralement les installations automatisées utilisées dans l'industrie, peuvent, si aucune mesure de prévention n'est prise, présenter des risques pour les opérateurs et tierces personnes amenés à les côtoyer.

Les risques existent par exemple lorsque des éléments mobiles de travail ou de transmission d'énergie génèrent des phénomènes dangereux, et que les opérateurs ou des tierces personnes sont susceptibles de les atteindre lorsqu'ils sont en mouvement.

Conformément aux dispositions de la Directive machines [2], transposée en droit national dans le Code du travail, les fabricants doivent réduire les risques dès la conception et respecter des exigences essentielles de sécurité et de santé (EESS), listées dans son annexe I.

Pour les aider concrètement dans leur démarche, les fabricants ont à leur disposition la norme NF EN ISO 12100 [3] qui décrit des principes généraux de conception des machines.

1.2. Origine

La figure 1 illustre les différents éléments générateurs d'un risque, qui peuvent conduire à un accident générant un dommage pour une personne exposée. Rappelons que pour qu'un accident se produise, il faut la conjonction :

- d'un phénomène dangereux et d'une présence humaine : ce qui constitue une situation dangereuse par exemple, la présence des mains d'un opérateur entre les outils d'une presse à découper les métaux ;
- de l'apparition d'un événement dangereux : par exemple, le démarrage intempestif d'un élément mobile dangereux ;
- de la non-possibilité d'éviter le dommage : par exemple, une impossibilité d'échapper à un élément mobile dangereux qui se déplace rapidement.

Ces différents éléments doivent être pris en compte pour l'estimation du risque.

1.3. Estimation

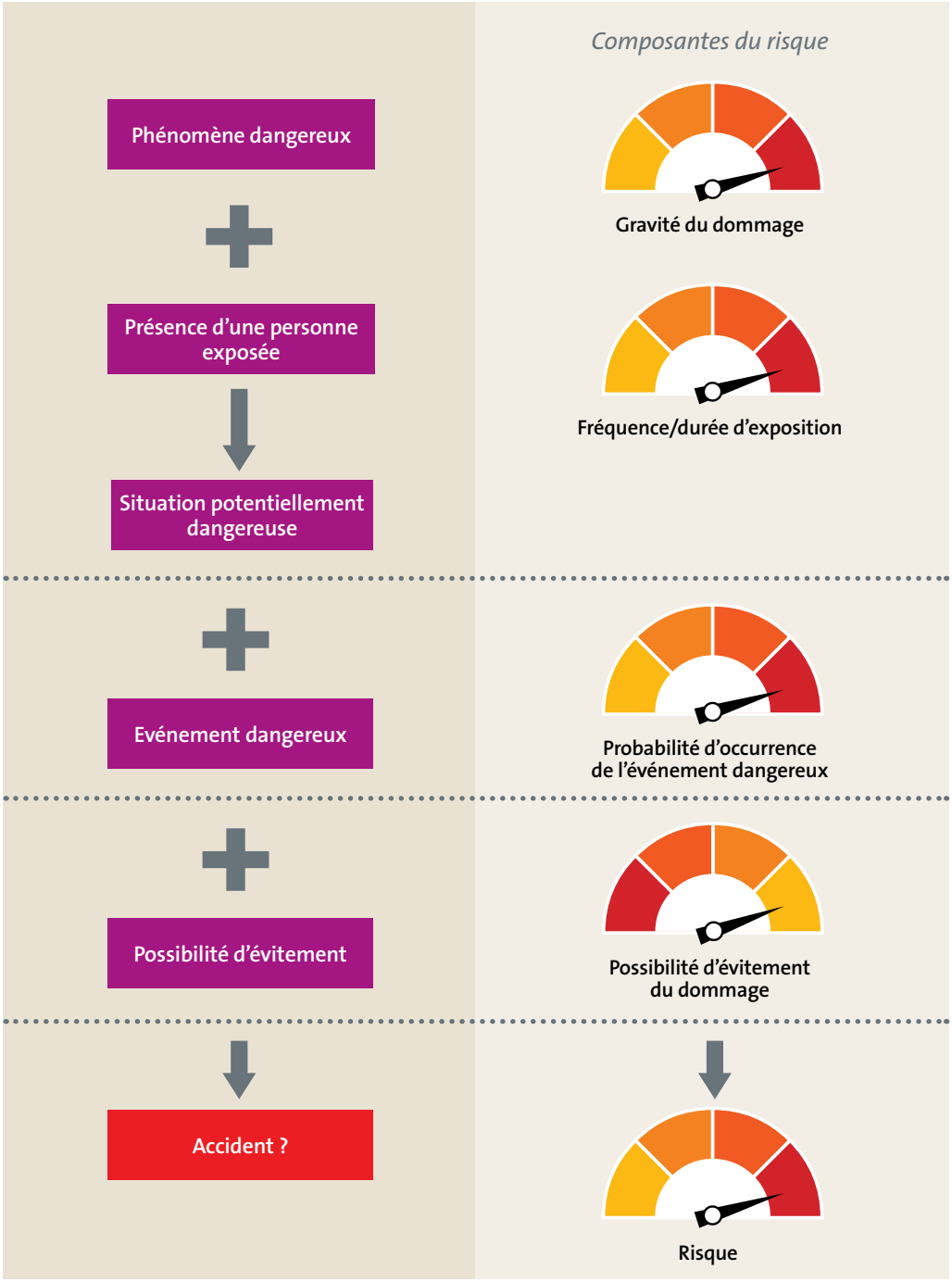
Pour estimer le niveau d'un risque, il faut tenir compte de ses différentes composantes que sont la gravité et la probabilité d'occurrence du dommage. La gravité est fonction des dommages provoqués sur la personne. La probabilité d'occurrence du dommage dépend de trois paramètres :

- la fréquence et/ou la durée d'exposition,
- la probabilité d'occurrence de l'événement dangereux. Cette probabilité d'occurrence peut d'être d'origine humaine (manœuvre inappropriée par exemple) ou technique (défaillance de composant, erreur logicielle, etc.),
- la possibilité d'éviter ou de limiter le dommage.

La figure 1 montre l'évolution du niveau de risque en fonction de la variation de ses différentes composantes. On peut noter, par exemple, qu'un risque est plus élevé lorsque la fréquence/durée d'exposition ou la probabilité d'occurrence ou la gravité augmentent, ou que la possibilité d'évitement diminue.

→ La norme NF EN ISO 12100 définit le risque comme étant une combinaison de la probabilité d'occurrence d'un dommage et de la gravité de ce dommage.
→ La plupart des composantes de l'estimation du risque sont également nécessaires pour déterminer le niveau de sécurité des fonctions assurées par les systèmes de commande relatifs à la sécurité lors de leur conception.

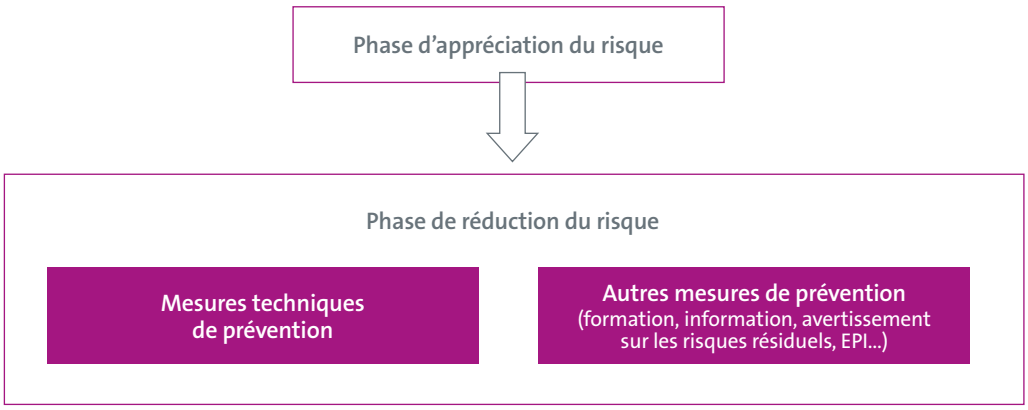
Figure 1. Causes d'un accident et composantes du risque



1.4. Appréciation et réduction

Après l'estimation du risque, il convient d'appliquer un processus itératif pour son appréciation et sa réduction, tel qu'illustré de manière synthétique dans la figure 2.

Figure 2. Représentation synthétique du processus d'appréciation et de réduction du risque



Appréciation du risque

Elle comprend une analyse précise des limites de la machine, une identification des phénomènes dangereux, une estimation et une évaluation du risque, en tenant compte de l'usage normal et du mauvais usage raisonnablement prévisible. Des exemples de ces éléments appliqués à une machine, suivant la norme NF EN ISO 1200, sont donnés dans le chapitre B (partie 2). La machine est, quant à elle, décrite dans ce même chapitre (partie 1).

Réduction du risque

Elle consiste à mettre en œuvre prioritairement des mesures « techniques » de prévention. Ces dernières doivent privilégier des mesures de prévention intrinsèques et à défaut d'autres mesures telles que des protecteurs fixes ou mobiles, ou des dispositifs de protection. Des exemples de « mesures techniques de prévention » sont donnés dans le chapitre B (partie 2, tableau 2).

> *Note*
> *La représentation synthétique du processus ne montre pas les différentes itérations menant au choix des mesures de prévention. Dans la réalité, lorsque le concepteur décide d'arrêter les itérations, c'est qu'il a estimé que le risque « initial » a été éliminé ou réduit de manière adéquate par les mesures de prévention qu'il a retenues et qu'aucun nouveau risque n'a été généré par ces mesures.*
> *Les autres mesures de prévention identifiées dans la représentation synthétique du processus ne sont pas abordées dans ce document.*

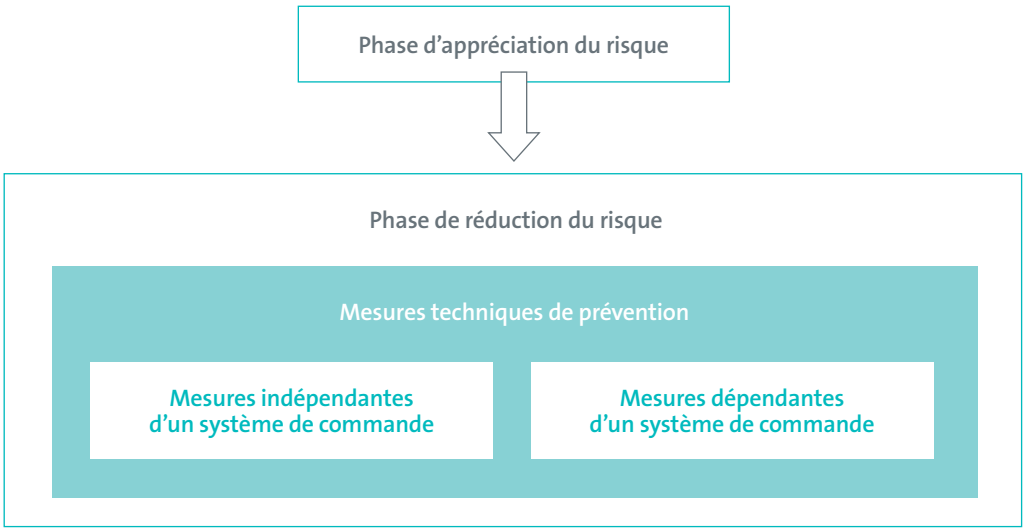
→ Les résultats de l'appréciation du risque seront plus réalistes et plus probants si celle-ci est effectuée de façon collective et consensuelle par l'ensemble des acteurs concernés : fabricant, opérateurs de maintenance, opérateurs de production...

2

MESURES TECHNIQUES DE PRÉVENTION ET SYSTÈME DE COMMANDE

Parmi les mesures techniques de prévention pouvant être retenues, suite au déroulement du processus d'appréciation et de réduction du risque, deux cas se présentent comme le montre la figure 3.

Figure 3. Mesures techniques de prévention dépendantes ou non d'un système de commande



2.1. Mesures indépendantes d'un système de commande

Il s'agit :

- de mesures de prévention intrinsèques consistant à supprimer le risque, par conception et sans faire appel à des protecteurs ou des dispositifs de protection : par exemple, supprimer les angles vifs et les parties saillantes des éléments mécaniques,
- de protecteurs fixes pour empêcher, par exemple, l'accès à un système de transmission par chaîne.

Des exemples de mesure intrinsèque et de protecteurs fixes, avec description de leurs rôles, sont donnés dans le chapitre B (partie 2, tableau 2).

Note
Comme ces mesures de prévention sont indépendantes d'un système de commande, elles ne sont plus abordées dans la suite de ce document.

2.2. Mesures dépendantes d'un système de commande

Il s'agit par exemple :
- d'un protecteur mobile avec dispositif de verrouillage qui commande l'arrêt d'un mouvement potentiellement dangereux,
- de la limitation sûre de la vitesse de déplacement d'un élément mobile de travail,
- d'un dispositif de validation qui commande l'arrêt d'un mouvement potentiellement dangereux.

Des exemples de telles mesures sont donnés dans le chapitre B (partie 2,tableau 2).
Un système de commande est nécessaire pour que ce type de mesure puisse accomplir l'action attendue.

→ Jusqu'à ce stade de la conception, la norme NF EN ISO 12100 sert de référence. C'est seulement à partir de ce qui suit que les normes spécifiques à la réalisation de systèmes de commande sont utiles.

2.3. Fonctions de sécurité

La réduction du risque par un moyen de protection tel qu'un protecteur mobile ou un dispositif de protection nécessite le recours à un système de commande. Ce dernier assure une fonction de sécurité car lorsqu'elle est défaillante, le moyen de protection peut devenir inopérant. Par exemple, si le contact électrique du dispositif de verrouillage d'un protecteur reste bloqué fermé suite à une défaillance, l'ouverture du protecteur ne commande plus l'arrêt du mouvement dangereux pour lequel il a été mis en place.

La définition d'une fonction de sécurité, est la suivante : « *Fonction d'une machine dont la défaillance peut provoquer un accroissement immédiat du ou des risques* » (NF EN ISO 12100, § 3.30).

Note
Une liste d'exemples de défaillances de diverses origines, pouvant affecter une fonction de sécurité, est donnée chapitre B (partie 3).

Pour chaque fonction de sécurité, il est nécessaire de décrire précisément son comportement attendu, avec par exemple les éléments suivants :
- Le rappel du moyen de protection prévu (par exemple une barrière immatérielle, un protecteur mobile avec dispositif de verrouillage), ainsi que sa localisation (par exemple un protecteur de la face avant).
- Les modes de marche ou les phases de cycle dans lesquels le moyen de protection est actif.
- Le phénomène dangereux ou l'élément mobile dangereux (les citer précisément) ainsi que le ou les actionneur(s) concerné(s) et le cas échéant, d'autres précisions telles que le sens du mouvement dangereux.
- Le fonctionnement attendu de la fonction de sécurité, en fonction des informations d'entrée. Par exemple, arrêt de l'élément mobile dangereux à l'ouverture du protecteur mobile verrouillé et maintien à l'arrêt de cet élément tant que le protecteur n'est pas fermé.

Des exemples de fonctions de sécurité sont donnés dans le chapitre B (partie 2, tableau 2).

3

NOTIONS DE SYSTÈME DE COMMANDE RELATIF À LA SÉCURITÉ

Le système de commande d'une machine (figure 4) se décompose en deux parties qui sont amenées à échanger :

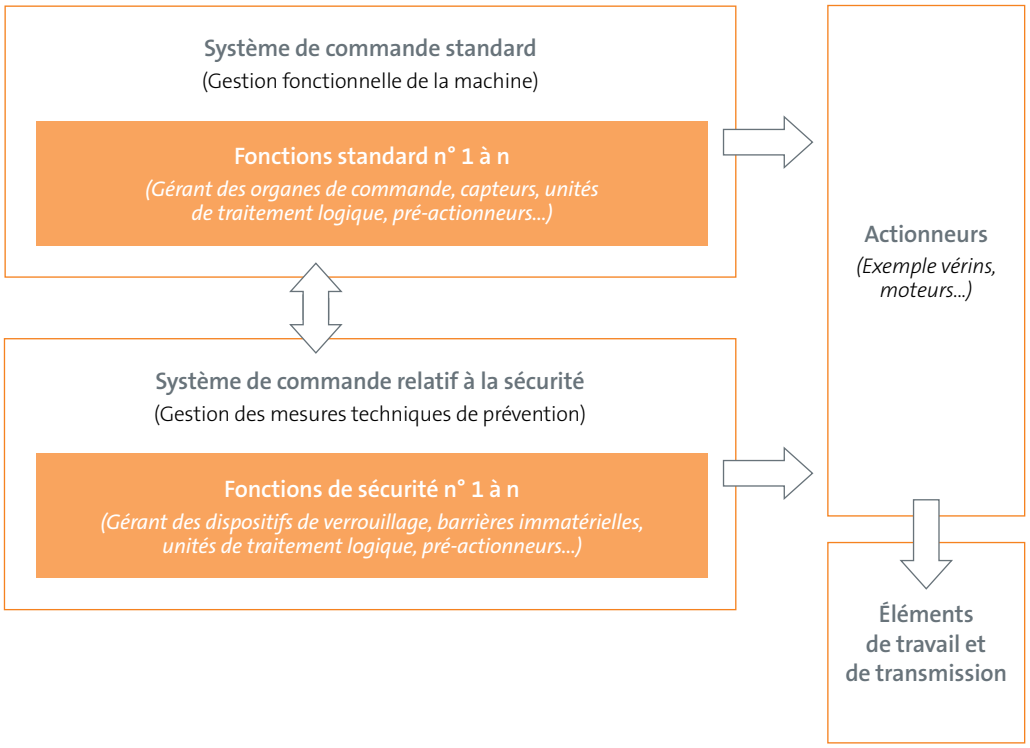
▶ L'une participe au fonctionnement de la machine pour assurer la production ou pour permettre son réglage, sans rapport avec la sécurité opérateur. Ces fonctions gèrent par exemple les mouvements des éléments mobiles d'une machine tels que montée, descente, avant, arrière, etc.

Il s'agit du système de commande « standard » qui gère les « fonctions standard ».

▶ L'autre gère les mesures techniques de prévention des risques. Cette partie est indispensable à la protection des personnes, par exemple pour commander un arrêt des éléments mobiles d'une machine lors de l'ouverture d'un protecteur.

Cette partie constitue le système de commande relatif à la sécurité qui gère les fonctions de sécurité.

Figure 4. Exemple de représentation simplifiée du système de commande d'une machine



→ Les échanges entre le système de commande « standard » et le système de commande relatif à la sécurité doivent être gérés de façon à ce que les fonctions de sécurité soient toujours assurées, quel que soit le comportement de la partie standard.

3.1. Exigences réglementaires

Les parties d'un système de commande relatives aux fonctions de sécurité doivent être conçues de telle sorte qu'elles soient sûres et fiables afin d'éviter toute situation dangereuse, et ce même en présence d'un défaut, d'une défaillance ou d'une détérioration. Les règles techniques de conception, également appelées dans la Directive machines « Exigences essentielles de santé et de sécurité », figurent dans le Code du travail à l'annexe I de l'article R. 4312-1. Le sous-paragraphe 1.2.1 de cette annexe « Sécurité et fiabilité des systèmes de commande » stipule notamment que :
« Les systèmes de commande doivent être conçus et construits de manière à éviter toute situation dangereuse. Ils doivent avant tout être conçus et construits de manière :
- à pouvoir résister aux contraintes de service et aux influences extérieures normales,
- à ce qu'une défaillance du matériel ou du logiciel du système de commande n'entraîne pas de situation dangereuse,
- à ce que des erreurs affectant la logique du système de commande n'entraînent pas de situation dangereuse,
- à ce qu'une erreur humaine raisonnablement prévisible au cours du fonctionnement n'entraîne pas de situation dangereuse.
... ».
Pour répondre à ces exigences réglementaires, les concepteurs ont à leur disposition des normes :

- décrivant des principes généraux à respecter, par exemple pour la sélection du matériel, la prise en compte des contraintes environnementales...,
- traitant plus spécifiquement de sûreté de fonctionnement, notamment NF EN ISO 13849-1 ou NF EN 62061 [4], permettant de les guider dans la réalisation de systèmes de commande « sûrs ».

3.2. Quelques normes incontournables

Plusieurs normes ont été élaborées pour aider les concepteurs, en particulier celles qui traitent des règles de base à respecter, appelées également « règles de l'art », et dont certaines sont rappelées ci-après.

Systèmes utilisant de l'énergie hydraulique ou pneumatique

- NF EN ISO 4413 – Transmissions hydrauliques. Règles générales et exigences de sécurité relatives aux systèmes et leurs composants [5].
- NF EN ISO 4414 – Transmissions pneumatiques. Règles générales et exigences de sécurité pour les systèmes et leurs composants [6].

Ces deux normes traitent, dans les limites de leur champ d'application, des généralités applicables à la conception, la construction et la modification des systèmes de commande, ainsi qu'à la mise en œuvre de leurs composants. L'objectif est de réduire les phénomènes dangereux significatifs associés aux transmissions hydrauliques et pneumatiques.

Systèmes utilisant de l'énergie électrique

▶ NF EN 60204-1 – Sécurité des machines. Équipement électrique des machines. Partie 1 : règles générales [7].

Cette norme détaille de nombreuses règles de l'art. Sont abordés par exemple, la mise en œuvre des équipements et systèmes électriques, électroniques et électroniques programmables de commande des machines, la protection contre les chocs électriques, la protection de l'équipement, les liaisons équipotentielles, le câblage et les interfaces homme/machines.

Sécurité des systèmes de commande

Les systèmes de commande relatifs à la sécurité doivent répondre à des principes leur permettant d'atteindre un niveau requis de sûreté de fonctionnement. Ce dernier est défini en corrélation avec le niveau attendu de contribution du système de commande à la réduction des risques. Pour les machines, les concepteurs ont les référentiels suivants à leur disposition :
▶ NF EN ISO 13849-1 – Sécurité des machines. Parties des systèmes de commande relatives à la sécurité. Partie 1 : principes généraux de conception.

> *Note*
> *Cette norme a définitivement remplacé la norme NF EN 954-1 [8] depuis décembre 2011, en conservant en grande partie ses principes de conception, complétée par d'autres paramètres tels que la fiabilité des composants.*

Elle détaille des exigences de sécurité et des recommandations relatives à la conception des systèmes de commande traitant de fonctions de sécurité, de diverses technologies (électrique et électronique, hydraulique, pneumatique, mécanique...), afin d'atteindre un niveau de performance minimum de sécurité (PL pour Performance Level). Elle introduit la notion de Parties de Systèmes de Commande Relatives à la Sécurité (SRP/CS, pour Safety Related Parts of Control System), qui peuvent être réalisées par assemblage de composants logiques « simples » (des composants électromécaniques, des distributeurs hydrauliques, par exemple) ou par intégration de modules ou composants du commerce dédiés à la sécurité, programmables ou non (des automates, des blocs logiques de sécurité, des électrovannes à sécurité intrinsèque...).

▶ NF EN ISO 13849-2 – Sécurité des machines. Parties des systèmes de commande relatives à la sécurité. Partie 2 : validation [9].

Cette norme décrit les différentes étapes de validations à effectuer pour les parties de systèmes de commande relatives à la sécurité (SRP/CS) conçues conformément à la norme NF EN ISO 13849-1.
Elle détaille également les principes de sécurité de base, les principes de sécurité éprouvés pour différentes technologies concernées, fournit une liste de composants éprouvés ainsi qu'une liste de défauts et d'exclusions de défauts possibles.

▶ NF EN 62061 – Sécurité des machines. Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité.

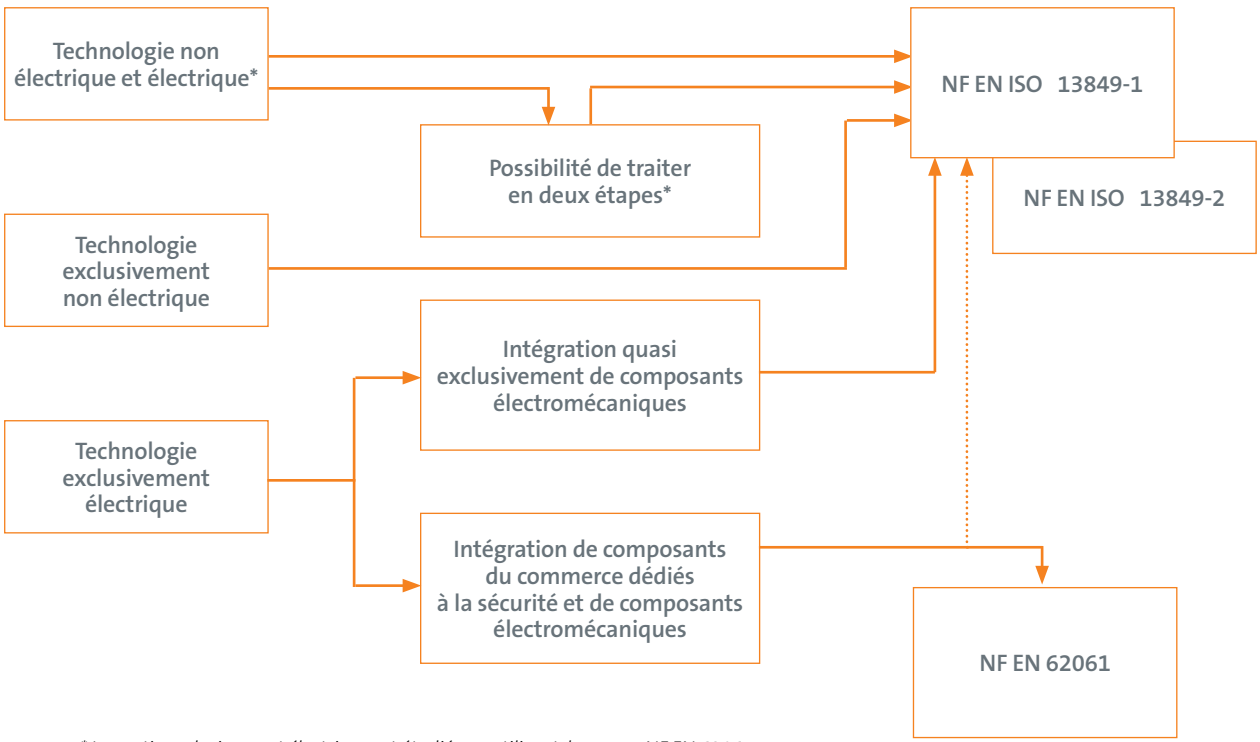
Cette norme détaille des exigences de sécurité et des recommandations relatives à la conception des systèmes de commande traitant de fonctions de sécurité, de technologie

électrique, électronique et électronique programmable, afin d'atteindre un niveau d'intégrité minimum de sécurité (SIL pour Safety Integrity Level). Elle introduit la notion de Systèmes de commande électrique relatifs à la sécurité (SRECS, pour Safety Related Electrical Control System) qui peuvent être réalisés par intégration de modules/composants du commerce dédiés à la sécurité, programmables ou non (des automates, des blocs logiques de sécurité...) et par assemblage de composants logiques « simples » (des relais, des composants électroniques, par exemple).

La figure 5 permet de guider les concepteurs dans le choix des référentiels les mieux appropriés.

→ Si le concepteur prévoit d'utiliser, pour la partie électrique, de nombreux composants électromécaniques, alors la norme NF EN ISO 13849-1 est plus adaptée que la norme NF EN 62061. Lorsqu'il utilise principalement des modules/composants du commerce dédiés à la sécurité, programmables ou non (des automates, des blocs logiques de sécurité...) ou des composants électroniques, alors la norme NF EN 62061 est plus adaptée que la norme NF E N ISO 13849-1.

Figure 5. Choix des normes spécifiques et appropriées pour traiter l'aspect « sureté de fonctionnement » d'un système de commande relatif à la sécurité



** La partie exclusivement électrique est étudiée en utilisant la norme NF EN 62061 si elle est mieux adaptée au cas à traiter. La norme NF EN ISO 13849-1 est utilisée pour traiter des autres technologies et intégrer l'ensemble des résultats*

4

DÉTERMINATION D'UN « NIVEAU DE SÉCURITÉ » REQUIS

4.1. Principes généraux

Lorsque les mesures techniques de prévention déterminées sont dépendantes d'un système de commande, ce dernier joue un rôle d'interface important, car il contribue à la réduction des risques.

Le système de commande doit être suffisamment « résistant » aux conditions de fonctionnement et aux défaillances raisonnablement prévisibles pouvant l'affecter pendant sa durée de vie prévue (temps de mission).

Pour la partie du système de commande de chaque fonction de sécurité, le concepteur doit déterminer un niveau de sécurité minimal à atteindre en fonction du niveau des risques à couvrir. Ce niveau symbolise la contribution du système de commande à la réduction du risque. Il représente le degré de résistance du système de commande relatif à la sécurité aux défaillances dangereuses pouvant l'affecter. Suivant les normes, il s'agit de :

- Un PLr, qui est un niveau de performance requis (traduction de « Performance Level required ») pour la norme NF EN ISO 13849-1. Cinq niveaux sont prévus, de PLr = a pour une contribution à la réduction d'un risque faible, jusqu'à PLr = e pour un risque élevé.
- Un SIL requis, qui est un niveau d'intégrité de sécurité (traduction de « Safety Integrity Level ») pour la norme NF EN 62061. Trois niveaux sont prévus, de SIL1 pour une contribution à la réduction d'un risque faible, à SIL3 pour un risque élevé.

Chaque norme fournit une méthode propre pour définir les niveaux « cibles » à atteindre par cette partie de système de commande, en procédant à une estimation des risques encourus par les personnes exposées.

La figure 6 représente les relations qui existent entre le niveau de risque à couvrir par la mesure technique de prévention, les niveaux de PL ou SIL recommandés et donc la « résistance » minimale aux défaillances dangereuses qui en résulte.

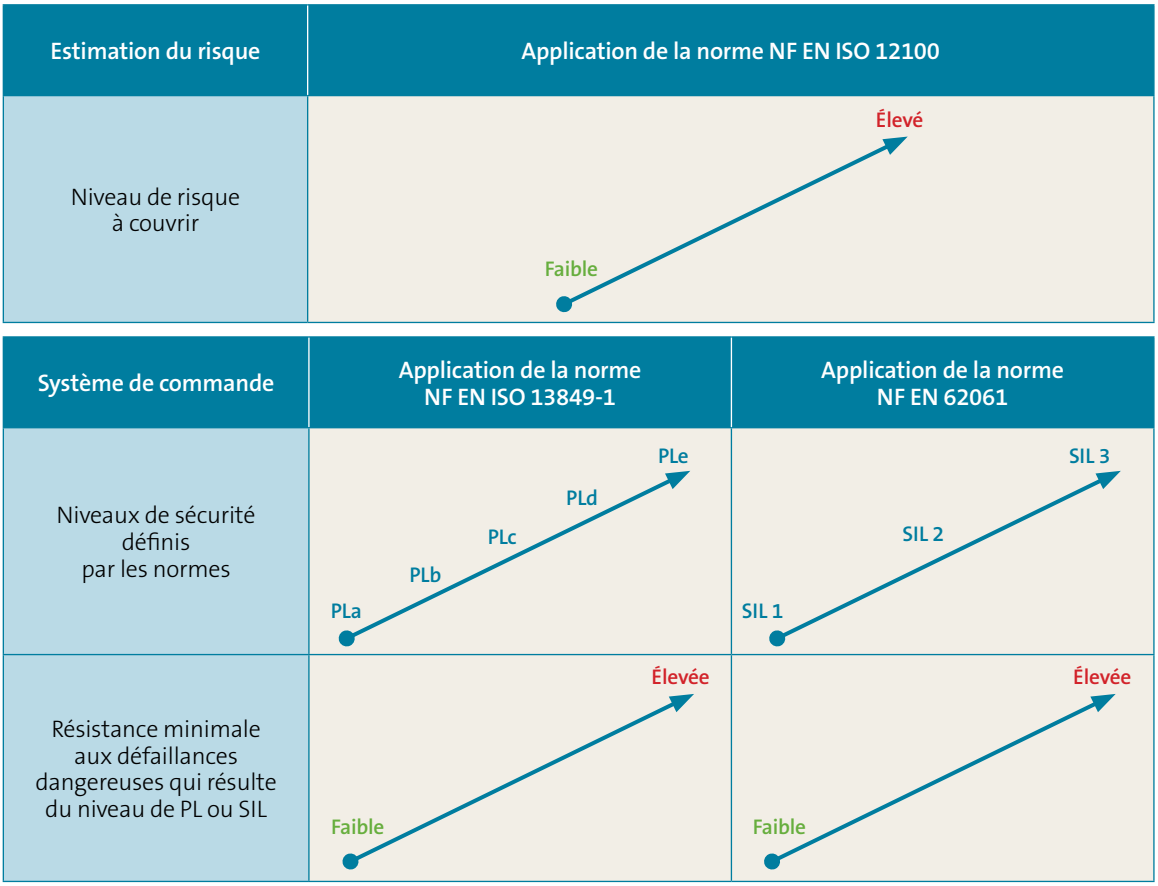
> *Note*
> *Un concepteur peut utiliser une norme « produit » harmonisée, appelée également norme de type « C » dans le domaine des machines. Lorsqu'il l'applique, il doit prendre en compte les niveaux de sécurité minimum indiqués pour chaque fonction de sécurité.*

→ Les normes NF EN ISO 13849-1 et NF EN 62061 (voir figure 7) proposent des méthodes pour déterminer le niveau de contribution du système de commande à la réduction des risques. Bien qu'utilisant certains critères identiques à ceux du processus de réduction des risques, ces méthodes ne sont en aucun cas prévues pour estimer le risque tel que décrit en § 1.3 et dans la norme NF EN ISO 12100.

→ L'estimation des « niveaux de sécurité » doit être effectuée au début du cycle de conception. Ces niveaux ne doivent pas être remis en cause lors de la conception sauf en cas de modifications de la machine affectant le niveau de risque à couvrir ou les mesures d'élimination/réduction du risque. Une nouvelle estimation du niveau de sécurité est alors nécessaire dans le nouveau contexte.

→ Les résultats de l'estimation des « niveaux de sécurité » à atteindre seront plus réalistes et plus probants si celle-ci est effectuée de façon collective et consensuelle.

Figure 6. Relations entre niveau de risque, niveaux de sécurité et résistance minimale aux défaillances



4.2. Niveau de performance de sécurité suivant NF EN ISO 13849-1 et NF EN 62061. Aspects généraux

Pour chaque fonction de sécurité, les normes NF EN ISO 13849-1 et NF EN 62061 préconisent de procéder en suivant les trois étapes principales décrites figure 7 page suivante.

Pour chaque niveau de sécurité, les éléments de la figure 8 doivent être pris en compte lors de la conception du système de commande relatif à la sécurité.

→ Un PL ou un SIL ne se résume pas à une valeur de PFH_D ou de $MTTF_D$; il faut aussi tenir compte de tous les autres critères (voir figure 8).

Figure 7. Étapes principales préconisées par les normes NF EN ISO 13849-1 et NF EN 62061

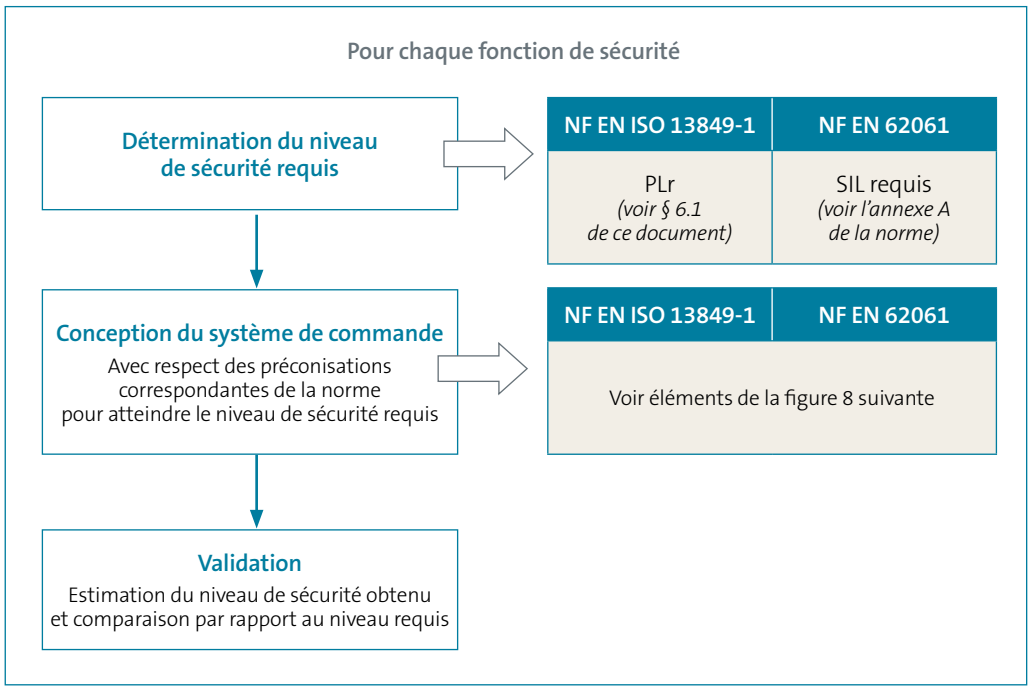


Figure 8. Critères de conception préconisés par les normes NF EN ISO 13849-1 et NF EN 62061

Application de NF EN ISO 13849-1	Application de NF EN 62061
Choix et mise en œuvre d'une architecture spécifique liée à la résistance aux défauts et au comportement consécutif à des défauts (détection) ou à la fiabilité des composants	
Détermination du temps moyen avant défaillance dangereuse ***($MTTF_D$)***, de la catégorie et de la couverture de diagnostics ***(DC)***	Détermination de la probabilité moyenne de défaillance dangereuse par heure ***(PFH_D)***.
Mise en œuvre de diverses mesures, comme celles destinées à contrer les ***défaillances systématiques,*** contrer les ***défaillances de cause commune,*** …	
Choix de composants aptes à résister aux contraintes environnementales prévues.	
Le cas échéant, application de règles spécifiques au développement du logiciel relatif à la sécurité.	

4.3. Relation entre PL et SIL

Le tableau 3 de la norme NF EN ISO 13849-1, dont les éléments sont rappelés figure 9, donne la relation qui existe entre les PL et les SIL.

→ Grâce à la relation formalisée entre SIL et PL, des parties de système de commande conçues à l'aide de l'une ou l'autre de ces deux normes peuvent être combinées dans un même système.

Figure 9. Extrait du tableau 3 de la norme NF EN ISO 13849-1

PL	SIL (IEC 61508-1, pour information) Mode de fonctionnement continu/élevé
a	Pas de correspondance
b	1
c	1
d	2
e	3

5

REPÈRES GÉNÉRAUX POUR LA CONCEPTION D'UN SYSTÈME DE COMMANDE RELATIF A LA SÉCURITÉ

La conception de systèmes de commande relatifs à la sécurité nécessite le respect des référentiels réglementaires et normatifs applicables. Le présent paragraphe a pour but de fournir quelques repères importants et utiles pour les concepteurs.

5.1. Processus de conception

La conception d'un système de commande relatif à la sécurité doit être effectuée dans des conditions rigoureuses et faire l'objet d'une traçabilité précise. Cette dernière facilite le processus de conception et de modification ultérieure.

La norme NF EN 62061 prévoit la mise en place d'un « plan de sécurité fonctionnel ». Il est conseillé d'adopter le même principe lors de l'application de la norme NF EN ISO 13849-1.

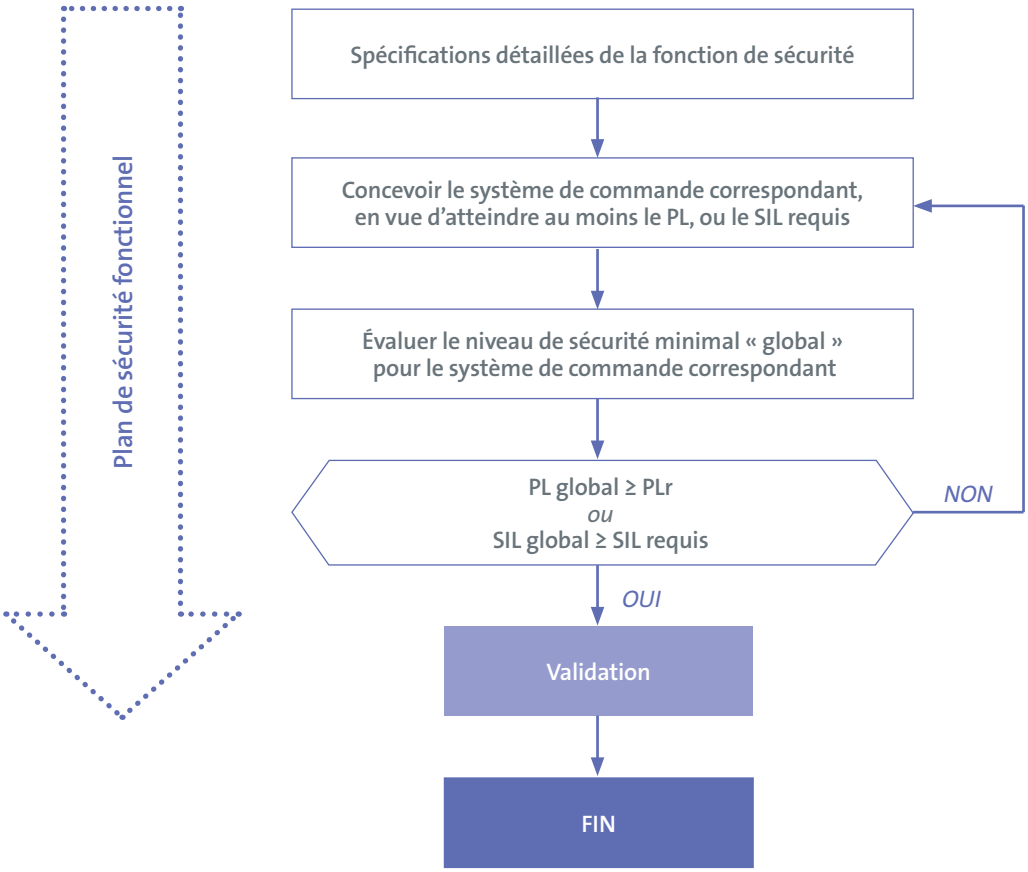
Les préconisations du plan de sécurité fonctionnelle concernent par exemple, l'identification des activités de développement du système de commande, la stratégie pour satisfaire aux exigences de sécurité fonctionnelle, la stratégie de gestion de configuration, la mise à jour de la documentation, l'identification et la qualification du personnel chargé des activités de conception...

Le plan de sécurité fonctionnelle est vivant, mis à jour et enrichi tout au long du développement du système de commande. Au départ, il formalise essentiellement l'organisation du cycle de conception avec ses étapes principales. Son contenu est ensuite complété par des informations organisationnelles et techniques, dont certaines ne sont connues qu'en avançant dans la conception.

Un système de commande relatif à la sécurité traite d'une ou plusieurs fonctions de sécurité. Il est chargé d'assurer les fonctionnalités des différents moyens de protection choisis, en respectant les niveaux de sécurité requis.

Pour chaque fonction de sécurité, un cycle de conception doit être réalisé tel que décrit de manière synthétique figure 10.

Figure 10. Graphe de conception d'un système de commande d'une fonction de sécurité



L'objectif est d'atteindre finalement un niveau de performance de sécurité (PL ou SIL global) pour chaque fonction de sécurité qui soit supérieur ou égal à la valeur cible déterminée (PLr ou SIL requis).

Par exemple, pour atteindre un PLr = b, le PL global acceptable en fin de conception pourra donc être égal à b, c, d, ou e.

5.2. Spécification des fonctions de sécurité

La première phase d'un cycle de conception d'une fonction de sécurité consiste à définir précisément ses caractéristiques sous forme d'une spécification fonctionnelle. Celle-ci doit comprendre notamment les informations décrites tableau 1, dont un exemple concret est fourni dans le chapitre B (partie 4).

5.3. Logiciel applicatif relatif à la sécurité

Des logiciels sont de plus en plus souvent utilisés dans le traitement des fonctions de sécurité. Une erreur affectant le logiciel peut au même titre qu'une défaillance matérielle, rendre inopérante une fonction de sécurité. C'est pourquoi les normes NF EN ISO 13849-1 et NF EN 62061 traitent toutes les deux de la partie logicielle avec des préconisations qui doivent être respectées pour que le PL ou le SIL d'une fonction de sécurité soit atteint.

Le logiciel applicatif est développé par l'intégrateur d'un composant programmable apte à réaliser des fonctions de sécurité, tels qu'un automate programmable dédié à la sécurité ou des composants de sécurité paramétrables. Généralement les fabricants de ce type de matériel proposent des « blocs fonction logiciels verrouillés et approuvés », qui contribuent à réaliser des fonctions de sécurité courantes, telles que le traitement de dispositifs de verrouillage de protecteurs ou d'arrêts d'urgence... Cette manière de procéder facilite la programmation, si les blocs correspondent bien aux besoins spécifiés pour la fonction de sécurité.

Pour la norme NF EN 62061, la note scientifique et technique NS 305 [10] de l'INRS apporte des précisions complémentaires sur la base d'un exemple.

La note scientifique et technique NS 252 [11] de l'INRS est utilisable en tant que guide pour la mise en œuvre d'une méthode de validation par tierce partie, lors de l'utilisation de l'une ou l'autre de ces deux normes.

→ Il ne faut surtout pas négliger le respect des règles applicables au logiciel, car ce dernier est aussi important que le composant qui l'exploite. Quid par exemple d'un composant de sécurité apte à réaliser des fonctions de PLe dont le logiciel applicatif serait déficient ?

Tableau 1. Exemple de tableau de spécification fonctionnelle d'une fonction de sécurité

Spécification des exigences fonctionnelles de la fonction de sécurité	
N°	**Nom de la fonction** ....
Niveau de performance requis	Préciser le PLr ou le SIL requis
Conditions d'activation de la fonction	À décrire pour le cas des fonctions qui ne sont pas actives en permanence, par exemple uniquement dans un mode de marche particulier.
Interface	Décrire ses entrées (Ex. dispositif de verrouillage d'un protecteur) et sorties (Ex. entrées de l'actionneur générateur d'un mouvement potentiellement dangereux).
Comportement de la fonction	Décrire : – l'état du déclencheur qui active la fonction (ex. ouverture protecteur) – le résultat attendu en étant le plus précis possible (ex. arrêt d'un actionneur dans une phase particulière du cycle).
Priorité par rapport à d'autres fonctions simultanées	Si plusieurs fonctions de commande « standard » ou fonctions de sécurité, sont actives simultanément et pourraient engendrer des conflits au niveau des ordres de commande générés, il y a lieu de définir des priorités au niveau de la spécification afin d'anticiper ces conflits.
Autres fonctions agissant sur le même actionneur	Si plusieurs fonctions de sécurité doivent agir sur le même élément de sortie (par exemple le même actionneur) il y a lieu de préciser les éléments de sortie concernés/les fonctions de sécurité concernées.
Temps de réaction maximal de la fonction	Indiquer le temps de réaction maximal attendu, compris entre les commutations de l'entrée et de la sortie (par exemple le temps pris en référence dans le calcul de la distance minimale de sécurité de positionnement d'une barrière immatérielle).
Taux de demande de la fonction	Préciser la fréquence de fonctionnement, ou de sollicitation de la fonction en usage normal. Certaines fonctions sont sollicitées cycliquement (ex. cas d'une barrière immatérielle sollicitée à chaque chargement d'une machine), d'autres beaucoup moins fréquemment (ex. protecteur ouvert uniquement pour des opérations de réglage).
Réaction aux fautes/conditions de redémarrage	Détailler : – le comportement attendu de la fonction en présence d'un dysfonctionnement dans son traitement. – les conditions de redémarrage suite à la suppression du dysfonctionnement.
Conditions d'ambiance	Décrire les contraintes liées à l'environnement de la machine (ex. température, humidité, poussières, vibrations et autres nuisances).

6

REPÈRES POUR L'UTILISATION DE LA NORME NF EN ISO 13849-1

Les principes décrits ci-après sont basés sur la méthode dite « simplifiée » de la norme.

6.1. Méthode de détermination d'un niveau de performance requis (PLr)

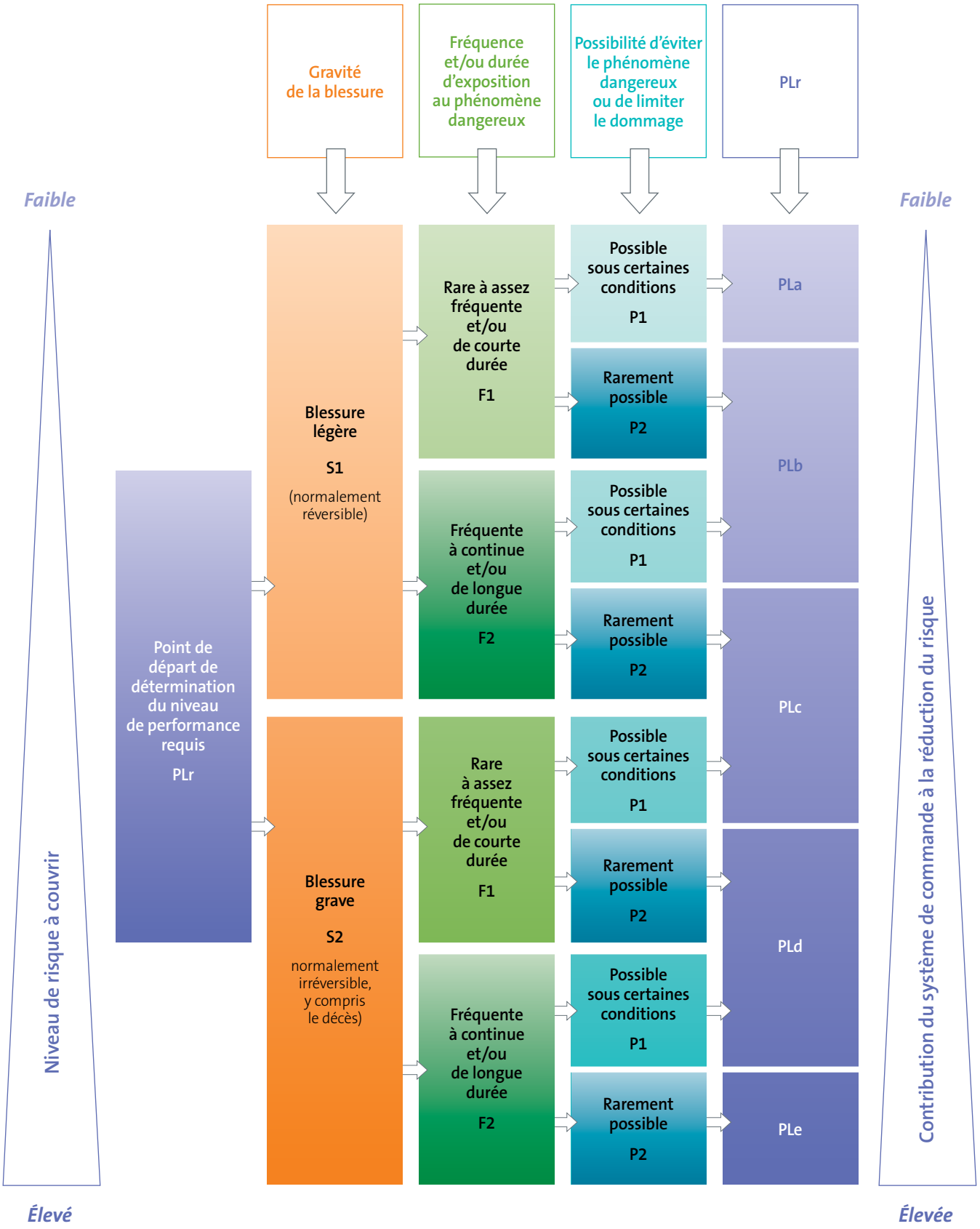
L'annexe informative « A » de la norme NF EN ISO 13849-1 décrit une méthode pour la détermination du PLr, dont les principes sont rappelés figure 11.
Des critères de détermination sont donnés dans le chapitre B (partie 5).

L'analyse s'effectue en ne prenant pas en compte la contribution à la réduction du risque du moyen de protection prévu. Elle se base sur des critères dont certains ont été pris en compte lors de l'évaluation des risques ayant servi à la détermination des mesures techniques de prévention appropriées.

Les différents paramètres à prendre en compte sont :
- la gravité potentielle de la blessure (S),
- la fréquence et ou durée d'exposition aux phénomènes dangereux (F),
- la possibilité d'éviter le phénomène dangereux ou de limiter le dommage (P),
- la probabilité d'occurrence d'un événement dangereux (qui n'apparaît pas dans le graphe et qui doit être traitée séparément).

Un exemple détaillé de détermination de PLr pour la fonction de sécurité FS1 du lave-vaisselle et un tableau synthétique des résultats pour l'intégralité des fonctions de sécurité sont donnés dans le chapitre B (voir parties 6 et 7).

Figure 11. Illustration du graphique de détermination du niveau de performance requis (PLr) tiré de l'annexe A de la norme NF EN ISO 13849-1

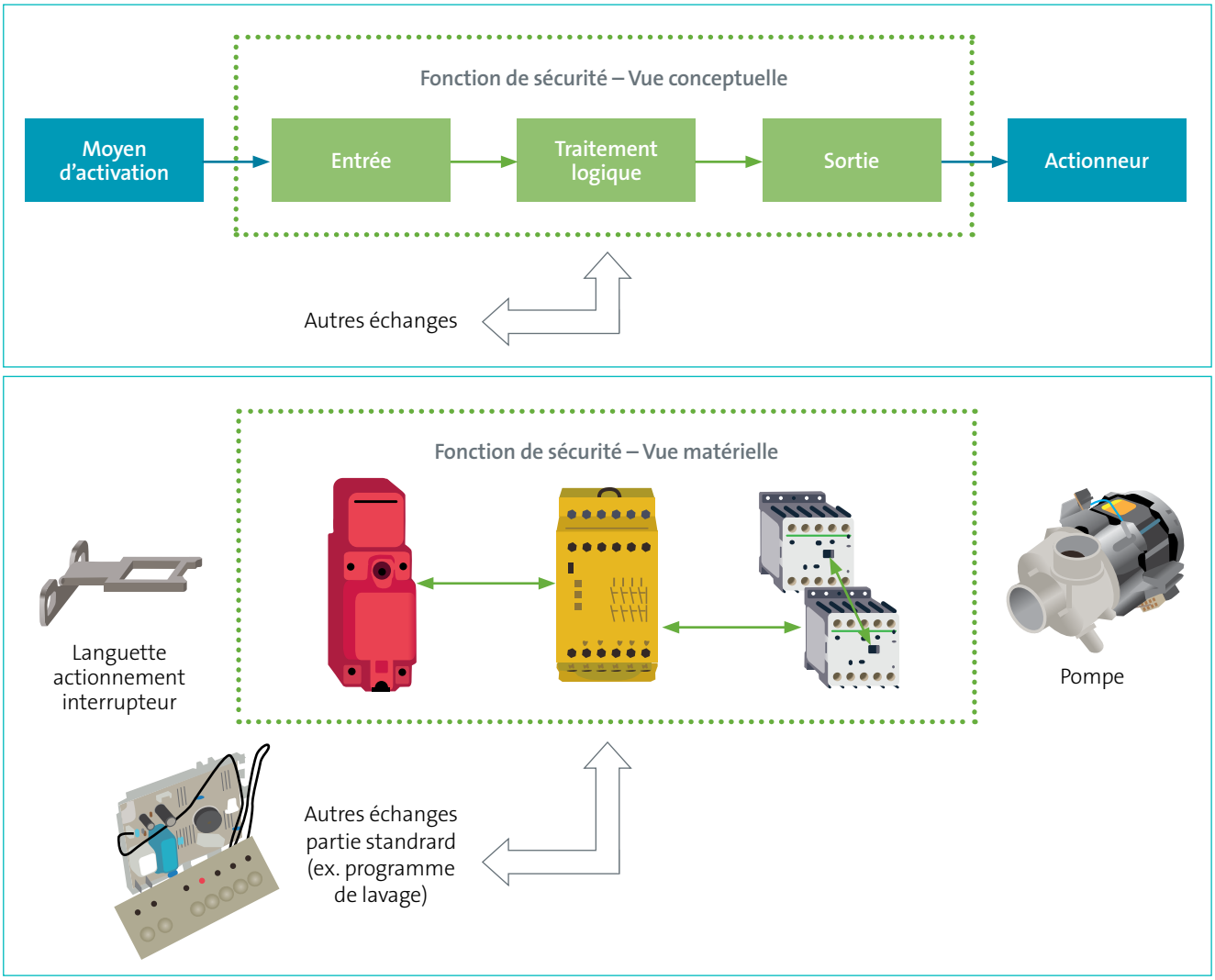


6.2. Composition d'une fonction de sécurité

Selon la norme NF EN ISO 13849-1, les fonctions de sécurité sont constituées de différentes parties, généralement au nombre de trois, appelées « SRP/CS », et combinées en série pour assurer la fonction attendue.

Ces parties sont d'abord « conceptuelles ». Leur association répond aux spécifications de la fonction de sécurité à assurer. Elles sont ensuite déclinées en parties matérielles qui sont conçues par le concepteur du système de commande, soit par intégration de composants de sécurité du commerce, soit par un développement spécifique.

Figure 12. Exemple de décomposition d'une fonction de sécurité et éléments externes



Chaque fonction est activée en entrée par un moyen externe, et agit en sortie sur un actionneur. Par exemple, pour une fonction d'arrêt d'une pompe par protecteur, la décomposition peut se présenter comme décrit ci-après :

▶ Une partie conceptuelle « entrée » de la fonction. Elle est déclinée matériellement par un dispositif de verrouillage d'un protecteur, par exemple un interrupteur de sécurité. Il est sollicité extérieurement à la fonction de sécurité par un moyen d'activation tel que la languette d'un interrupteur de sécurité.

▶ Une partie conceptuelle « traitement logique ». Elle est déclinée matériellement par un bloc logique de sécurité prévu pour assurer le comportement de la fonction.

▶ Une partie conceptuelle « sortie » de la fonction. Elle correspond généralement à des pré-actionneurs. Elle est déclinée matériellement par des contacteurs de puissance. Elle agit extérieurement à la fonction de sécurité sur un actionneur comme par exemple une pompe électrique.

La figure 12 illustre cette description. Les autres échanges ont lieu entre la fonction de sécurité et la partie standard du système de commande (par exemple avec un programmateur électronique de cycles de lavage), ou avec d'autres fonctions de sécurité. Les échanges doivent être pris en compte pour s'assurer qu'ils ne perturbent pas le bon fonctionnement des fonctions de sécurité.

> *Note*
> *La décomposition en trois parties conceptuelles, bien qu'usuelle, n'est pas impérative.*

6.3. Configuration matérielle d'une fonction de sécurité

Après la phase de décomposition d'une fonction de sécurité en parties conceptuelles, il faut :
– spécifier chacune des parties sur la base de la spécification de la fonction,
– attribuer à chacune d'elles par défaut le PLr de la fonction,
– choisir un type de matériel approprié pour chacune d'elles.

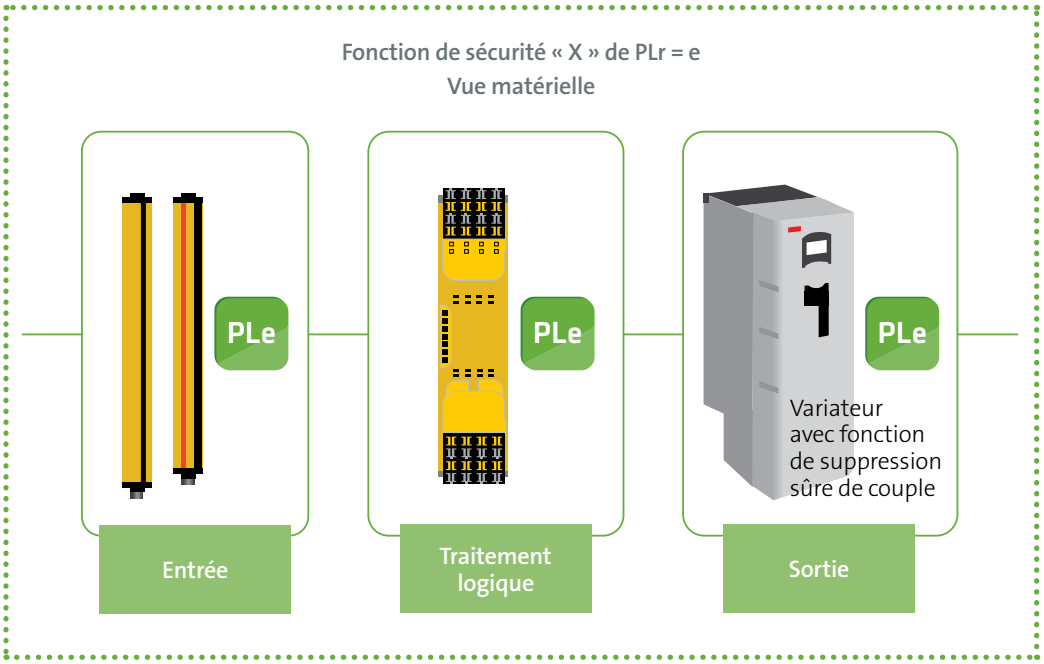
> *Note*
> *Suivant ses caractéristiques, un même matériel peut assurer à lui seul le rôle de plusieurs parties conceptuelles, par exemple traitement logique et sortie combinés.*

Pour le choix du matériel, plusieurs solutions sont possibles :

▶ Utilisation exclusive de composants de sécurité mis isolément sur le marché, donc de PL connu (voir figure 13, page suivante). Il faut cependant être prudent avec ce genre de composant. En effet, le fabricant revendique souvent la possibilité d'atteindre « jusqu'à » un certain PL, sous réserve de respecter les consignes de mise en œuvre et d'utilisation pour le matériel et le logiciel.

> *Note*
> *Lorsque les spécifications fonctionnelles et de sécurité du composant correspondent à celles attendues, ce choix a pour avantage de faciliter la détermination du PL de la fonction, qui dépend du PL de chaque partie.*
> *Les composants doivent être compatibles entre eux.*
> *La détermination du PL de la fonction, qui dépend du PL de chaque partie, peut s'effectuer en appliquant les règles du § 6.3 de la norme.*

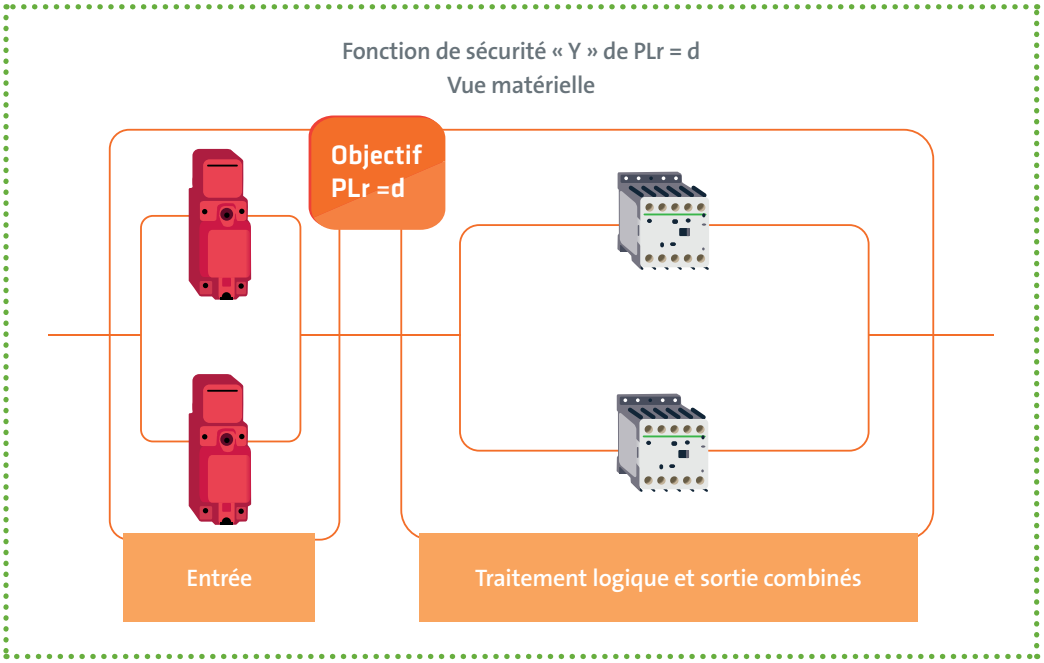
Figure 13. Utilisation de composants de sécurité de PL connus



▶ Utilisation exclusive de composants basiques, tels que des relais électromécaniques, des distributeurs électropneumatiques, des dispositifs de verrouillage électromécaniques, qui sont associés en respectant les préconisations de la norme, en vue d'atteindre le PLr (figure 14).

> *Note*
> *Ce choix est souvent motivé par l'absence sur le marché de composant de sécurité répondant aux spécifications fonctionnelles et de sécurité déterminées.*
> *Une connaissance approfondie de la norme est nécessaire pour concevoir le système de commande.*

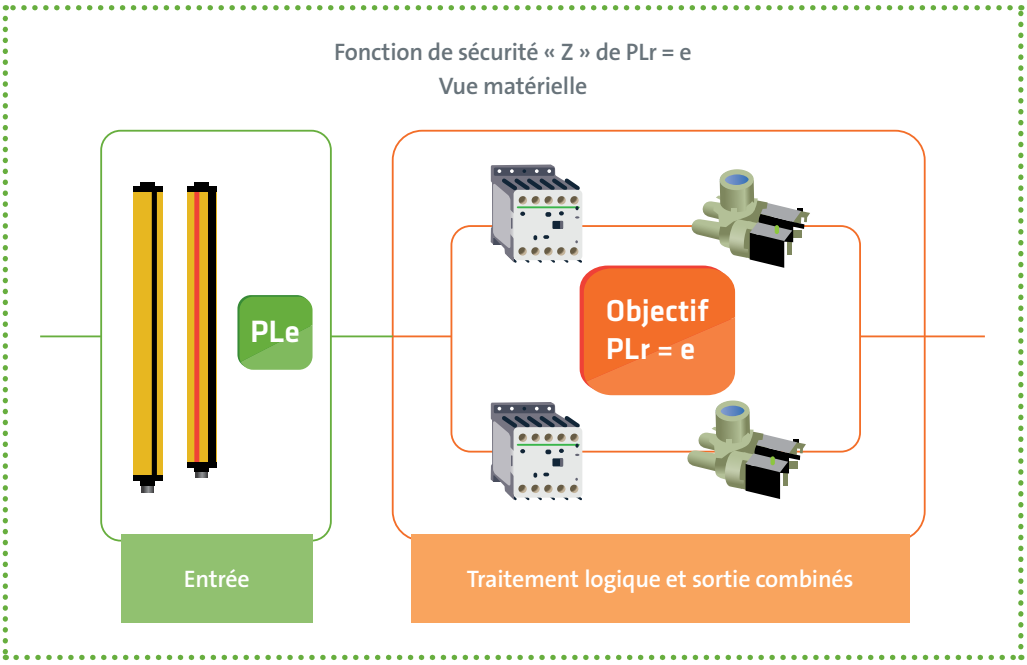
Figure 14. Utilisation de composants basiques



▶ Utilisation mixte de composants de sécurité mis isolément sur le marché (avec respect des consignes d'utilisation comme décrit précédemment) et de parties de système de commande conçues avec des composants basiques dont le PL a été déterminé (voir figure 15).

Note
Cette solution s'applique lorsqu'une des parties n'est pas disponible en tant que composant de sécurité mis isolément sur le marché.
La détermination du PL de la fonction nécessite de déterminer préalablement le PL de la partie conçue avec des composants basiques.
La détermination du PL de la fonction, qui dépend du PL de chaque partie, peut s'effectuer en appliquant les règles du § 6.3 de la norme.

Figure 15. Conception mixte avec des composants de PL connus et des composants basiques



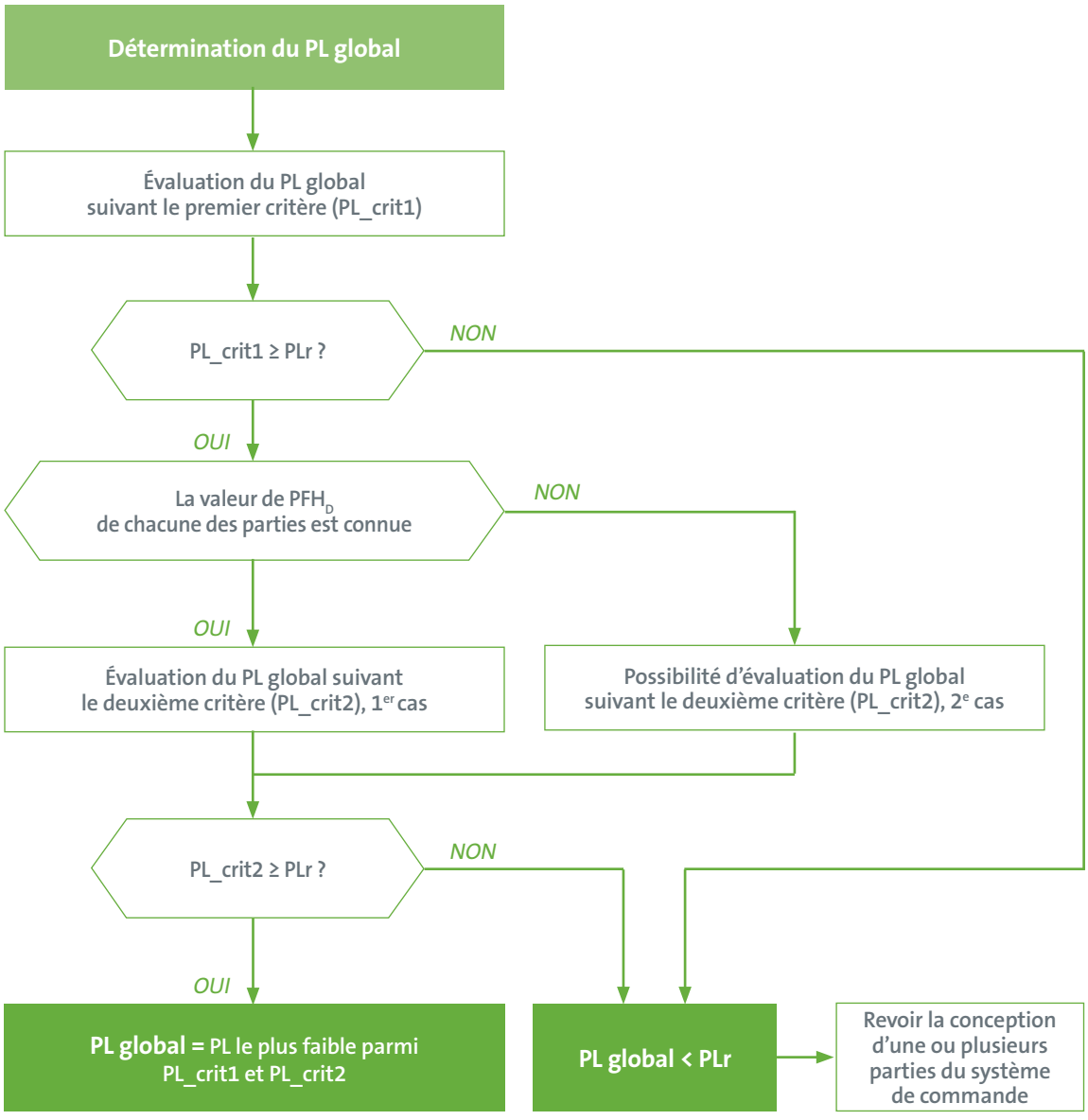
6.4. Détermination du PL global

6.4.1. Utilisation de parties de système de commande de PL connus

Lors de la conception d'une fonction de sécurité composée de plusieurs parties de système de commande de PL connus, le PL global du système de commande de la fonction est limité par deux critères précisés ci-après.

La méthode pour déterminer le niveau de performance global est présentée en figure 16.

Figure 16. Méthode de détermination du PL global



Premier critère : le PL maximum qui peut être atteint par le système de commande de la fonction est limité par le PL le plus faible des parties qui le composent (PL_crit1).

Si le PL de certaines parties est de niveau inférieur au PLr, le PL global ne peut pas être atteint et il faut revoir la conception des parties concernées.

Deuxième critère : le PL du système de commande de la fonction est aussi limité suivant le nombre et les caractéristiques des parties prévues. Sa détermination est décrite au § 6.3 de la norme et deux cas se présentent.

▶ 1er cas : la valeur de PFH_D de chacune des parties est connue.
Il faut utiliser la règle illustrée en figure 13 de la norme, et donc faire la somme de toutes ces valeurs pour calculer la PFH_D du système de commande de la fonction. Ensuite, son PL (PL_crit2) est déterminé suivant le tableau 2 de la norme (voir figure 17).

▶ 2e cas : la valeur de PFH_D de certaines parties n'est pas connue.
Il est alors possible d'utiliser le tableau 11 de la norme pour déterminer le PL du système de commande de la fonction en se basant sur le nombre « N_{low} » de parties ayant le PL le plus faible « PL_{low} » (voir figure 18).

Si le PL obtenu (PL_crit2) est de niveau inférieur au PLr, le PL global ne peut pas être atteint et il faut revoir la conception d'une ou plusieurs parties et déterminer de nouveau le PL global.

Détermination du PL global : le PL global du système de commande de la fonction correspond au PL le plus faible obtenu suivant ces deux critères.

Figure 17. Tableau 2 de la norme NF EN ISO 13849-1

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

Figure 18. Tableau 11 de la norme NF EN ISO 13849-1

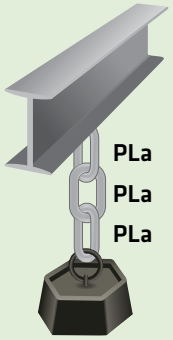
PL_{low}	N_{low}	=>	PL*
a	> 3	=>	Aucun, non autorisé
	≤ 3	=>	a
b	> 2	=>	a
	≤ 2	=>	b
c	> 2	=>	b
	≤ 2	=>	c
d	> 3	=>	c
	≤ 3	=>	d
e	> 3	=>	d
	≤ 3	=>	e

** Les valeurs calculées de ce tableau sont basées sur les valeurs de fiabilité moyennes de chaque PL*

Exemples d'application de la méthode

Cinq exemples de systèmes de commande, dont le PLr est connu, sont traités ci-après en utilisant la méthode illustrée en figure 16. Les parties constitutives des exemples sont symbolisées par des maillons d'une chaine, dont le PL est connu, ainsi que la PFH_D pour le cas de l'exemple 5.

Exemple n° 1 : PLr = a



Le système de commande de la fonction de sécurité est constitué de 3 parties, ayant chacune un PL connu de valeur a.

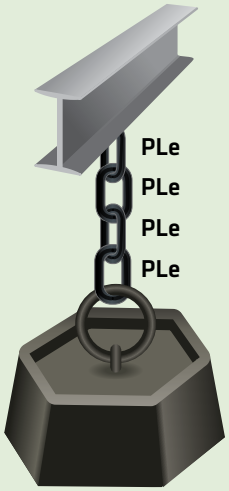
→ Premier critère : le PL le plus faible vaut a donc PL_crit1 = a. Étant égal au PLr, l'évaluation suivant le deuxième critère doit être effectuée.

→ Deuxième critère : la valeur de PFH_D n'est pas connue, le deuxième cas s'applique donc. Il y a 3 parties ayant le PL le plus faible (PL a). La lecture dans le tableau 11 de la norme (figure 18) donne PL_crit2 = a.

→ Détermination du PL global : le PL global est égal au plus faible des deux critères précédent, donc PL global = a.

→ PL global = PLr donc **le PL requis est atteint.**

Exemple n° 2 : PLr = e



Le système de commande de la fonction de sécurité est constitué de 4 parties, ayant chacune un PL connu de valeur e.

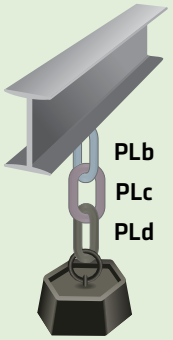
→ Premier critère : le PL le plus faible vaut e donc PL_crit1 = e. Étant égal au PLr, l'évaluation suivant le deuxième critère doit être effectuée.

→ Deuxième critère : la valeur de PFH_D n'est pas connue, le deuxième cas s'applique donc. Il y a 4 parties ayant le PL le plus faible (PL e). La lecture dans le tableau 11 de la norme (figure 18) donne PL_crit2 = d.

→ Détermination du PL global : le PL global est égal au plus faible des deux critères précédent, donc PL global = d.

→ PLglobal < PLr donc **le PL requis n'est pas atteint.** La conception doit être reprise.

Exemple n° 3 : PLr = a



Le système de commande de la fonction de sécurité est constitué de 3 parties, de PL connus de valeur respectivement b, c et d.

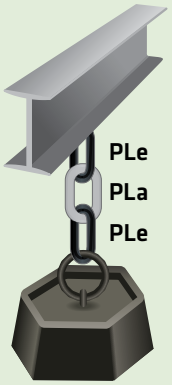
→ Premier critère : le PL le plus faible vaut b donc PL_crit1 = b. Etant supérieur au PLr, l'évaluation suivant le deuxième critère doit être effectuée.

→ Deuxième critère : la valeur de PFH_D n'est pas connue, le deuxième cas s'applique donc. Une seule partie possède le PL le plus faible (PL b). La lecture dans le tableau 11 de la norme (figure 18) donne PL_crit2 = b.

→ Détermination du PL global : le PL global est égal au plus faible des deux critères précédent, donc PL global = b.

→ PLglobal ≥ PLr donc **le PL requis est atteint.**

Exemple n° 4 : PLr = c



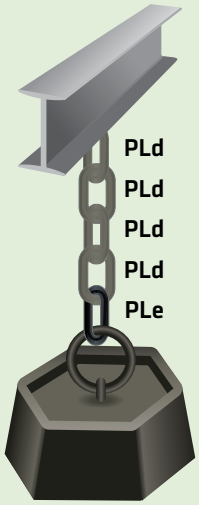
Le système de commande de la fonction de sécurité est constitué de 3 parties, de PL connus de valeur respectivement e, a et e.

→ Premier critère : le PL le plus faible vaut a donc PL_crit1 = a. Etant inférieur au PLr, l'évaluation suivant le deuxième critère n'est pas nécessaire.

→ Exploitation directe du premier critère pour la détermination du PL global : le PL global est limité par le PL_crit1, donc PL global = a.

→ PLglobal < PLr, donc **le PL requis n'est pas atteint.** La conception doit être reprise.

Exemple n° 5 : PLr = d



Le système de commande de la fonction de sécurité est constitué de 5 parties, de PL et de PFH_D connus.

Partie 1	Partie 2	Partie 3	Partie 4	Partie 5
PL = **d**	PL = **d**	PL = **d**	PL = **d**	PL = **e**
PFH_D : 1.10^{-7}	PFH_D : 1.10^{-7}	PFH_D : 3.10^{-7}	PFH_D : 2.10^{-7}	PFH_D : 5.10^{-8}

→ Premier critère : le PL le plus faible vaut d donc PL_crit1 = d. Étant égal au PLr, l'évaluation suivant le deuxième critère doit être effectuée.

→ Deuxième critère : la valeur de PFH_D de chaque partie est connue, donc le 1er cas s'applique. La somme des PFH_D vaut $7{,}5.10^{-7}$. On lit la valeur du PL dans le tableau 2 de la norme (figure 17) : PL_crit2 = d

Limitation du PL du système de commande par sa PFH_D

$PFH_D = \sum PFH_{D(1-5)} = 7{,}5.10^{-7}$ => D'après tableau 2 de la norme : PL = d

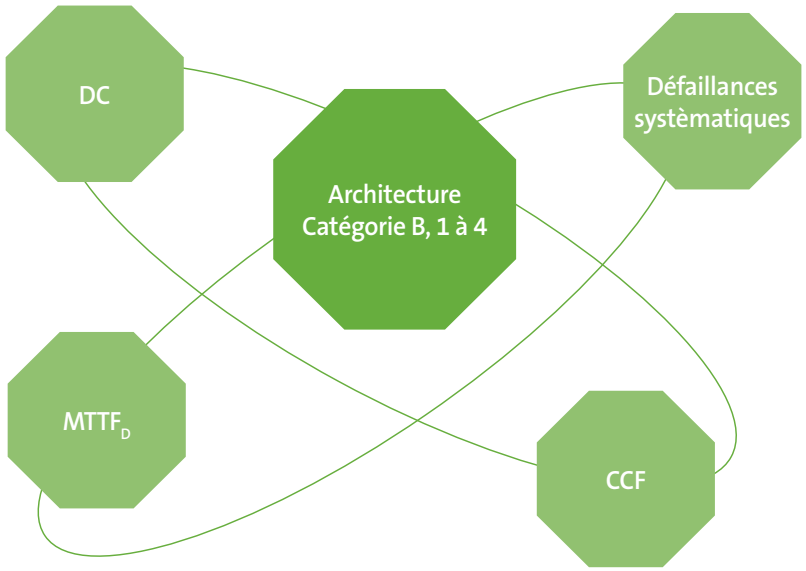
→ Détermination du PL global : le PL global est égal au plus faible des deux critères précédent, donc PL global = d.

→ PL global = PLr, donc **le PL requis est atteint.**

6.4.2. Notions pour l'utilisation de composants basiques

Lorsqu'il faut concevoir tout ou partie d'une fonction de sécurité avec des composants basiques, le § 4.5.1 de la norme définit des critères à respecter, pour que le PLr puisse être atteint. Ces critères sont définis en fonction du PLr (de « PLa » à « PLe ») et sont rappelés succinctement dans la figure 19.

Figure 19. Les différents critères qui composent un PL



Le présent document ne reprend pas en détail tous ces critères. Une appropriation de la norme est nécessaire par le concepteur. Elle peut être complétée par la consultation de la note scientifique et technique NS 302 de l'INRS qui traite d'un exemple concret [12].

Une procédure simplifiée pour l'estimation d'un PL est décrite dans la norme NF EN ISO 13849-1 en § 4.5.4. La figure 5 et le tableau 6 de cette norme facilitent l'exploitation des critères nécessaires.

Pour revendiquer un PL donné, il faut :

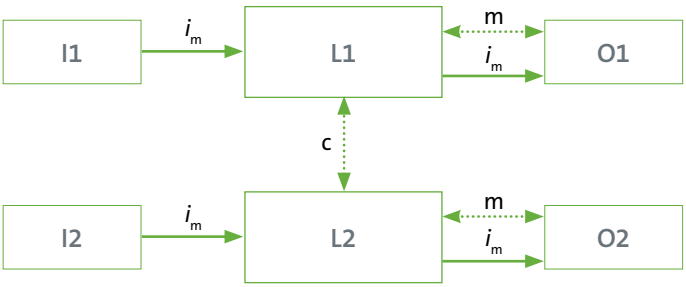
▶ Appliquer une des cinq catégories décrites dans le § 6.2 de la norme et notamment l'architecture désignée correspondante. Cette dernière consiste à prévoir un ou deux canaux fonctionnels, avec ou sans équipement d'essai (pour effectuer des tests de bon fonctionnement). Le comportement attendu de chaque architecture en présence d'une défaillance est clairement décrit. Les échanges mutuels entre canaux et équipements de test sont représentés dans les figures de la norme. Le tableau 10 de la norme résume les exigences à respecter. La figure 20 présente un exemple de deux types d'architectures désignées.

▶ Respecter une valeur minimale de $MTTF_D$ pour chaque canal de l'architecture désignée retenue. Ce $MTTF_D$ doit être calculé conformément à l'annexe D de la norme, en fonction des caractéristiques des composants.

Figure 20. Exemples d'architectures désignées de la norme

Architecture désignée pour la catégorie 1

Architecture désignée pour la catégorie 3



i_m	Moyens de connexion
I, I1, I2	Dispositifs d'entrée, par exemple détecteur
L, L1, L2	Logique
O, O1, O2	Dispositifs de sortie, par exemple contacteur principal
c	Surveillance croisée
m	Surveillance

Les traits interrompus représentent la détection de défaut raisonnablement praticable.

Pour certains composants, leur $MTTF_D$ est fourni dans leur fiche technique. À défaut, il doit être calculé conformément à l'annexe C de la norme en se basant sur des informations de leur fiche technique, et en fonction de leur nombre prévu de sollicitations. Lorsque les caractéristiques nécessaires ne sont pas fournies par le fabricant, la norme propose dans cette même annexe la possibilité d'utiliser des valeurs par défaut.

▶ Respecter, à partir de la catégorie 2, une valeur minimale de couverture moyenne de diagnostic « DCavg » pour l'ensemble du système de commande de la fonction. L'annexe E de la norme fournit des exemples de critères d'appréciation à prendre en compte ainsi qu'une formule de calcul.

▶ Adopter, à partir de la catégorie 2, des mesures pour contrer les défaillances de cause commune « CCF ». L'annexe F de la norme décrit une méthode pour quantifier le niveau de couverture atteint, suivant les mesures techniques retenues. Il s'agit par exemple de règles à appliquer, telle que la protection des circuits contre les surtensions ou surpressions, qui pourraient affecter simultanément plusieurs canaux (fonctionnels et/ou d'essai) du système de commande, et empêcher une fonction de sécurité de jouer son rôle.

▶ Adopter des mesures pour maîtriser et prévenir les défaillances systématiques. L'annexe G de la norme fournit une liste de mesures applicables. Il s'agit de règles de bonnes pratiques et de principes à respecter dès la conception. Par exemple, utiliser la désactivation énergétique afin de permettre à une fonction de sécurité de rester opérationnelle lors d'une perte d'alimentation en énergie.

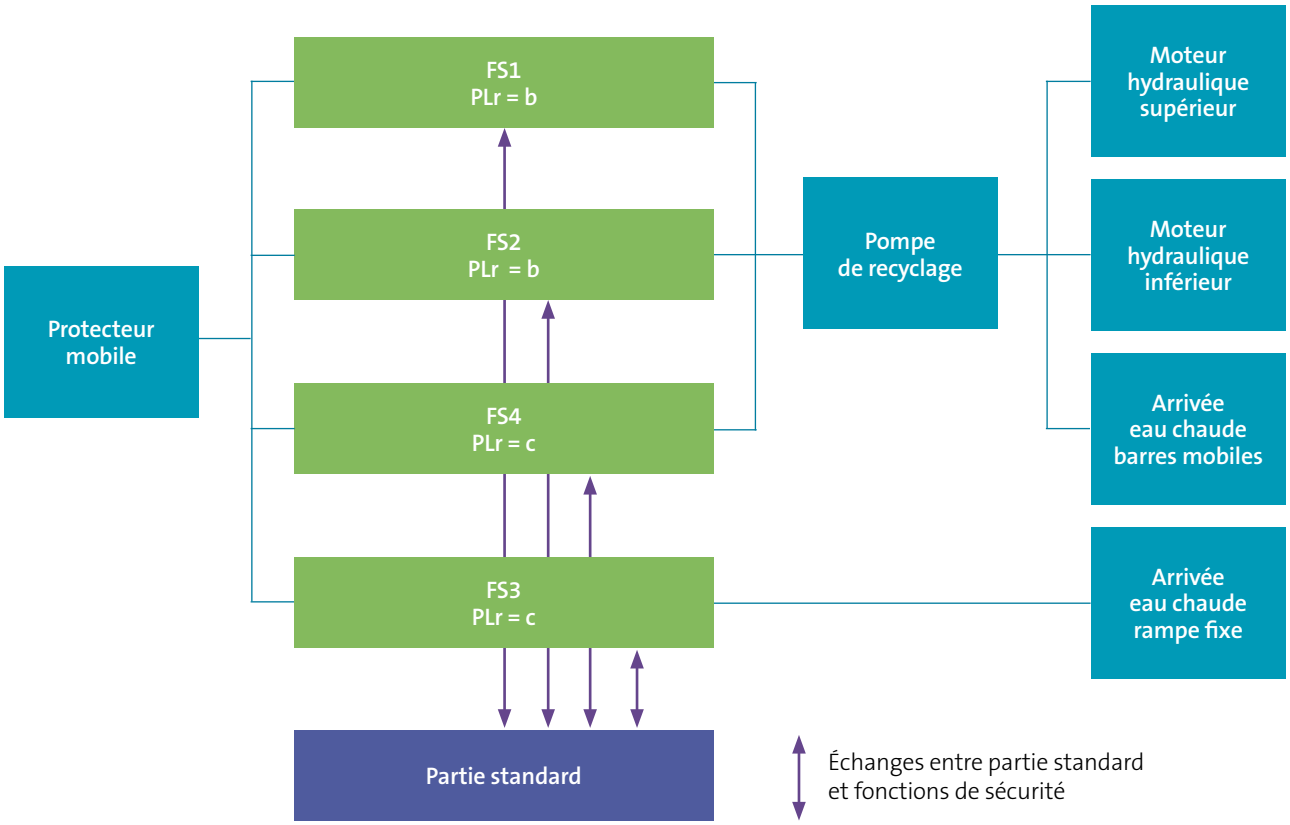
▶ Mettre en œuvre, le cas échéant, pour la partie logicielle, les exigences décrites dans le § 4.6 de la norme.

→ Une même catégorie peut être utilisée pour atteindre des PL différents, donc une catégorie exprimée « seule » ne suffit pas pour exprimer un PL.
→ Un PL dépend de critères qualitatifs non quantifiables, tels que l'architecture du système de commande (simple canal, redondant...) et de critères quantifiables, tels que les valeurs de $MTTF_D$ et du taux de couverture de dagnostics (DC).
→ Une valeur de $MTTF_D$ seule ne suffit pas à qualifier un PL.

6.5. Système de commande traitant plusieurs fonctions de sécurité

Il est très courant de concevoir un système de commande relatif à la sécurité qui doit traiter de plusieurs fonctions de sécurité pour une même machine.
Fréquemment, les fonctions de sécurité n'ont pas toutes le même PLr. C'est ce que représente la figure 21, basée sur l'exemple du lave-vaisselle.

Figure 21. Représentation schématique du système de commande

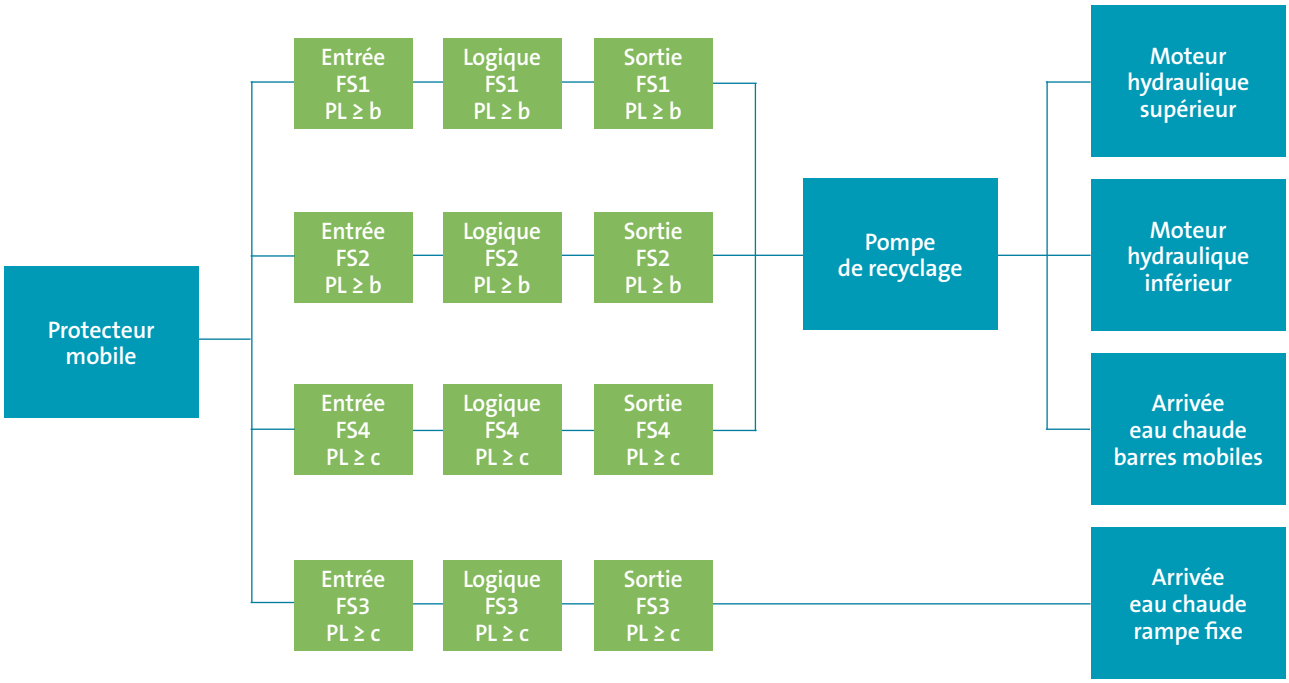


Ce cas montre :

- des fonctions de sécurité FS1, FS2 et FS4 qui agissent sur le même actionneur (pompe de recyclage) ;
- un même moyen de protection (le protecteur mobile) qui agit en entrée de toutes les fonctions de sécurité ;
- des fonctions de sécurité qui ont un PLr différent ;
- une partie de système de commande standard qui doit échanger avec les fonctions de sécurité.

La figure 22 montre un exemple de décomposition des fonctions de sécurité en 3 parties conceptuelles, sans représenter les échanges avec la partie standard ni anticiper sur les choix de la partie matérielle.

Figure 22. Exemple de décomposition des fonctions de sécurité



6.6. Exemple de répartition et de choix du matériel entre plusieurs fonctions de sécurité

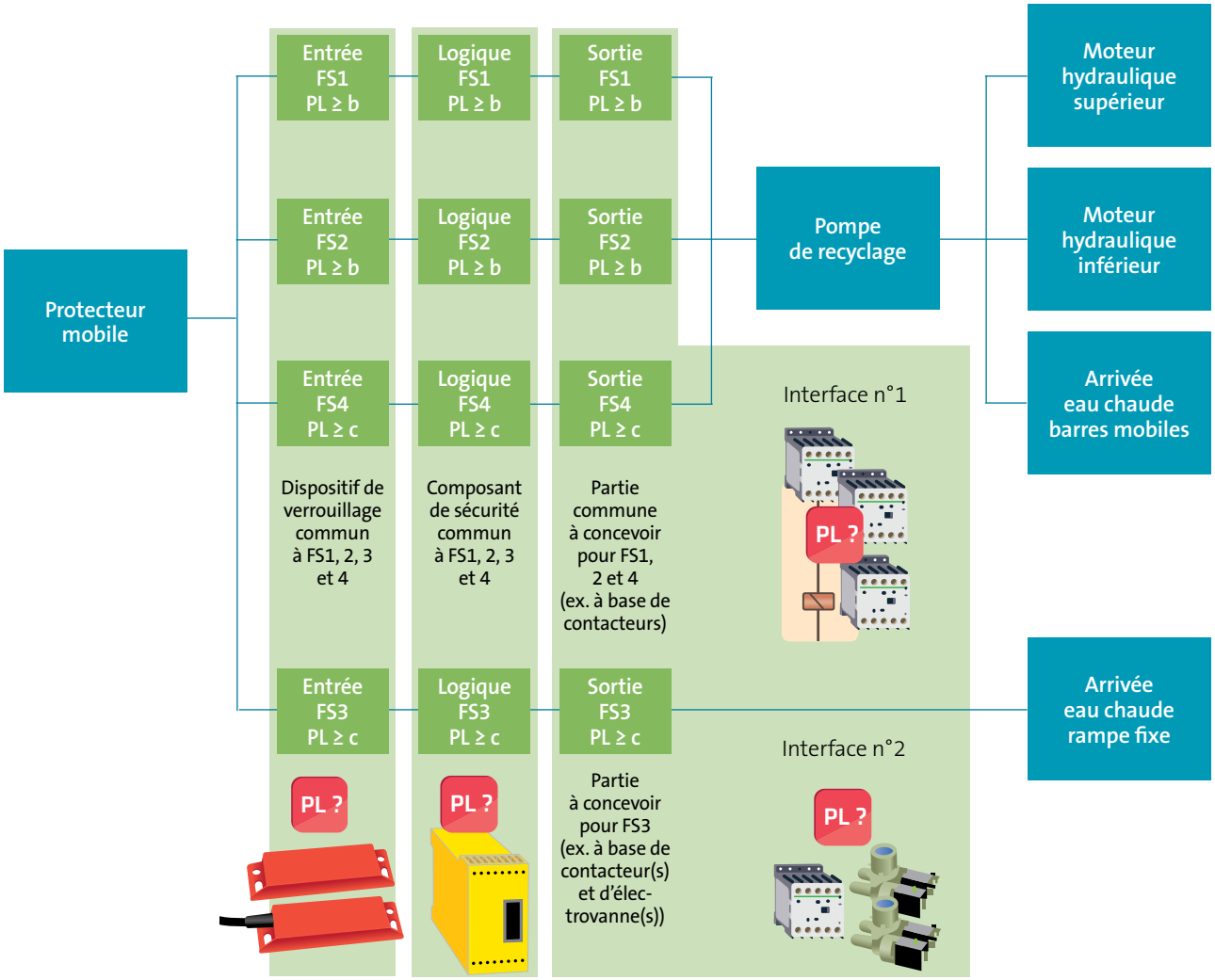
Après avoir décomposé chaque fonction de sécurité en parties « conceptuelles », la phase de choix du matériel envisagé se pose pour l'intégralité du système de commande relatif à la sécurité.

Des précautions doivent être prises lors de la conception du système de commande pour que la combinaison de toutes ces fonctions ne soit pas une source de dégradation des PL. Par exemple :

- une fonction de PLb ne doit pas dégrader une fonction de PLc, notamment lorsqu'elle agit sur le même actionneur ;
- la partie standard ne doit pas dégrader le fonctionnement des fonctions de sécurité.

La figure 23 page suivante, montre pour cet exemple, la première itération de choix et de répartition de matériel en tenant compte du PLr des fonctions.

Figure 23. Exemple de choix et de répartition de matériel



Choix et conséquences de la configuration matérielle retenue pour cet exemple

À la lecture de la figure 23, on déduit les conditions suivantes :

▶ Un seul dispositif de verrouillage du protecteur commun aux fonctions de sécurité FS1, FS2, FS3 et FS4. Cette partie matérielle doit respecter le PLr le plus haut requis pour les fonctions traitées, donc PL ≥ c.

▶ Un composant de sécurité commun pour les parties logiques des fonctions de sécurité FS1, FS2, FS3 et FS4. Cette partie matérielle doit respecter le PLr le plus haut requis pour les fonctions traitées, donc PL ≥ c.

▶ Une interface n° 1 conçue avec des composants basiques, commune pour la partie sortie des fonctions FS1, FS2 et FS4. Cette partie matérielle doit respecter le PLr le plus haut requis pour les fonctions traitées, donc PL ≥ c.

▶ Une interface n° 2 conçue avec des composants basiques pour la partie sortie de la fonction FS3. Cette partie matérielle doit respecter le PLr de FS3, donc PL ≥ c.

Si l'on considère que la PFH_D d'au moins une des parties n'est pas connue, il est possible d'utiliser le tableau 11 du § 6.3 de la norme. Dans ce cas, pour les fonctions qui doivent respecter un PLr de niveau b ou c, le découpage en trois SRP/CS peut être pénalisant pour déterminer le PL global de la partie du système de commande de la fonction de sécurité. Il est alors nécessaire qu'au moins une des trois SRP/CS ait pour objectif un niveau de performance supérieur au niveau requis pour la fonction de sécurité.

▶ Un matériel de PL = e a été retenu pour la partie logique de FS3 et FS4 afin d'atteindre leur PLr (choix définitif du PL, voir tableau 2). Cette partie logique étant commune aux autres fonctions, elle les impacte, mais leur PL reste supérieur ou égal au PLr.

Tableau 2. Synthèse du matériel retenu

Fonction de sécurité et choix relatifs au matériel	Entrée	Logique	Sortie	PL global minimum suivant tableau 11 de la NF EN ISO 13849-1	Commentaire
FS1 - PLr = b					
Type de matériel	Dispositif de verrouillage commun	Composant de sécurité commun	Interface n°1 commune (FS1, FS2 et FS4)		
Choix primaire du PL	PL ≥ c	PL ≥ c	PL ≥ c	b	PL ≥ PLr
Choix définitif du PL	PL = c	**PL = e** (Impact du choix de FS3 et FS4)	PL = c	**c**	PL ≥ PLr
FS2 - PLr = b					
Type de matériel	Dispositif de verrouillage commun	Composant de sécurité commun	Interface n°1 commune (FS1, FS2 et FS4)		
Choix primaire du PL	PL ≥ c	PL ≥ c	PL ≥ c	b	PL ≥ PLr
Choix définitif du PL	PL = c	**PL = e** (Impact du choix de FS3 et FS4)	PL = c	**c**	PL ≥ PLr
FS3 - PLr = c					
Type de matériel	Dispositif de verrouillage commun	Composant de sécurité commun	Interface n°2		
Choix primaire du PL	PL ≥ c	PL ≥ c	PL ≥ c	**b**	**PL < PLr** donc une des parties doit être PL > c
Choix définitif du PL	PL = c	**PL = e**	PL = c	**c**	PL ≥ PLr
FS4 - PLr = c					
Type de matériel	Dispositif de verrouillage commun	Composant de sécurité commun	Interface n°1 commune (FS1, FS2 et FS4)		
Choix primaire du PL	PL ≥ c	PL ≥ c	PL ≥ c	**b**	**PL < PLr** donc une des parties doit être PL > c
Choix définitif du PL	PL = c	**PL = e**	PL = c	**c**	PL ≥ PLr

6.7. Logiciels d'aide à la conception

Des logiciels ont été développés pour aider les concepteurs de systèmes de commande de sécurité dans l'application de la norme NF EN ISO 13849-1. Le logiciel SISTEMA, que nous évoquons ci-après, provient de l'organisme de prévention allemand « IFA » (Institut fur Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung), qui le met gracieusement à la disposition des industriels.

Ce logiciel permet de suivre pas à pas les principales phases de conception, tels que la spécification des fonctions de sécurité, la détermination du PLr, le calcul des $MTTF_D$ et le calcul du PL obtenu. Pour chaque phase, le concepteur doit saisir les données d'entrée nécessaires. Le logiciel se charge d'effectuer les calculs nécessaires. La traçabilité du projet est donc assurée, avec un numéro de code généré à chaque modification afin de suivre les évolutions. Un rapport final peut être édité.

Le logiciel offre la possibilité d'utiliser des bases de données de fiabilité de composants lorsqu'elles sont disponibles auprès des fabricants.

Ce logiciel a des limites car, par exemple :
- il ne traite pas du détail de la partie logicielle lorsqu'elle existe,
- il ne permet pas de conserver la trace de certaines informations prises en compte, comme les données concernant les défaillances systématiques, pour lesquels il faut cocher une seule case pour confirmer que des mesures ont été prévues.

De plus ce logiciel :
– ne remplace pas la norme qui reste indispensable,
– nécessite une connaissance technique de la norme afin de fournir les bonnes données et de pouvoir évaluer la pertinence des résultats.

Une fois le projet finalisé dans SISTEMA, le concepteur doit réaliser le schéma de commande en respectant strictement toutes les données et les hypothèses prises en compte.

→ Les résultats obtenus avec un logiciel dépendent de la pertinence des données d'entrées fournies par le concepteur.
→ Les données de conception qui ne sont pas mémorisées dans le logiciel doivent être consignées dans un rapport séparé car elles seront utiles pour la réalisation du système de commande.

GLOSSAIRE

Appréciation du risque
Processus qui comprend les phases de détermination des limites de la machine, d'identification des phénomènes dangereux, d'estimation et d'évaluation du risque.

Composant de sécurité
Composant qui sert à assurer une fonction de sécurité et qui n'est pas indispensable au fonctionnement de la machine.

Défaillances de cause commune
Défaillances qui affectent plusieurs entités à partir d'un même événement et qui ne résultent pas les unes des autres.

Défaillance dangereuse
Défaillance qui peut potentiellement mettre tout ou partie d'un système de commande dans un état dangereux ou défectueux.

Défaillance systématique
Défaillance associée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés.

Dispositif de verrouillage
Dispositif mécanique, électrique ou d'une autre technologie, destiné à empêcher certaines fonctions dangereuses de la machine de s'accomplir dans des conditions définies (généralement tant qu'un protecteur n'est pas fermé).

Fonction de sécurité
Fonction d'une machine dont la défaillance peut provoquer un accroissement immédiat du ou des risques.

Système de commande d'une machine
Système qui répond à un signal d'entrée provenant, par exemple du processus, d'autres éléments de la machine, d'un opérateur ou d'un matériel de commande externe, et génère une ou des sorties conduisant la machine à se comporter de la manière prévue.

ACRONYMES

CCF
Common Cause Failure – Défaillance de cause commune.

DC
Diagnostic Coverage – Couverture de diagnostic.
Possibilité pour un composant ou un circuit de détecter/diagnostiquer une défaillance le concernant.

DC_{avg}
Diagnostic Coverage average – Couverture de diagnostic moyenne.
Moyenne de la couverture de diagnostic lorsque plusieurs mesures pour la détection des défauts sont utilisées.

$MTTF_D$
Mean Time To dangerous Failure – Temps moyen de fonctionnement avant défaillance dangereuse.

PFH_D
Probability of dangerous failure per hour – Probabilité moyenne de défaillance dangereuse par heure.

PL
Performance Level – Niveau de performance
Niveau discret d'aptitude, de parties relatives à la sécurité, à réaliser une fonction de sécurité dans des conditions prévisibles.

PLr
Performance Level required – Niveau de performance requis.
Niveau de performance permettant d'atteindre la réduction du risque requise pour chaque fonction de sécurité.

SIL
Safety Integraty Level – Niveau d'intégrité de sécurité.
Niveau permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité.

SRP/CS
Safety Related Part/Control System – Partie d'un système de commande relative à la sécurité.

BIBLIOGRAPHIE

[1] NF EN ISO 13849-1 – Sécurité des machines. Parties des systèmes de commande relatives à la sécurité. Partie 1 : principes généraux de conception. AFNOR, 2016, 94 p.

[2] Directive 2006/42/CE du parlement européen et du conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (refonte). Journal Officiel de l'Union européenne, L157 du 9 juin 2006, 63 p.

[3] NF EN ISO 12100 – Sécurité des machines. Principes généraux de conception. Appréciation du risque et réduction du risque. AFNOR, 2010, 93 p.

[4] NF EN 62061 – Sécurité des machines. Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité. AFNOR, 2005, 106 p. (ainsi que les amendements NF EN 62061/A1. AFNOR, 2013 et NF EN 62061/A2. AFNOR, 2015).

[5] NF EN ISO 4413 – Transmissions hydrauliques. Règles générales et exigences de sécurité relatives aux systèmes et leurs composants. AFNOR.

[6] NF EN ISO 4414 – Transmissions pneumatiques. Règles générales et exigences de sécurité pour les systèmes et leurs composants. AFNOR.

[7] NF EN 60204-1 – Sécurité des machines. Équipement électrique des machines. Partie 1 : règles générales. AFNOR.

[8] NF EN 954-1 – Sécurité des machines. Parties des systèmes de commande relatives à la sécurité. Partie 1 : principes généraux de conception. AFNOR.

[9] NF EN ISO 13849-2 – Sécurité des machines. Parties des systèmes de commande relatives à la sécurité. Partie 2 : validation. AFNOR.

[10] Baudoin J, Bello J.P. – Exemple didactique d'application de la norme NF EN 62061. INRS, note scientifique et technique NS 305.

[11] Baudoin J, Bello J.P., Blaise J.C. – Guide pour la mise en œuvre d'une méthode de validation, par tierce partie, des parties de circuits de commande de presses traitées par un système de commande programmable. INRS, note scientifique et technique NS 252.

[12] Baudoin J, Bello J.P.- Aborder la norme NF EN ISO 13849-1 via la conception d'une fonction de sécurité basique. INRS, note scientifique et technique NS 302.

CHAPITRE

B

APPLICATION A UN LAVE-VAISSELLE PROFESSIONNEL

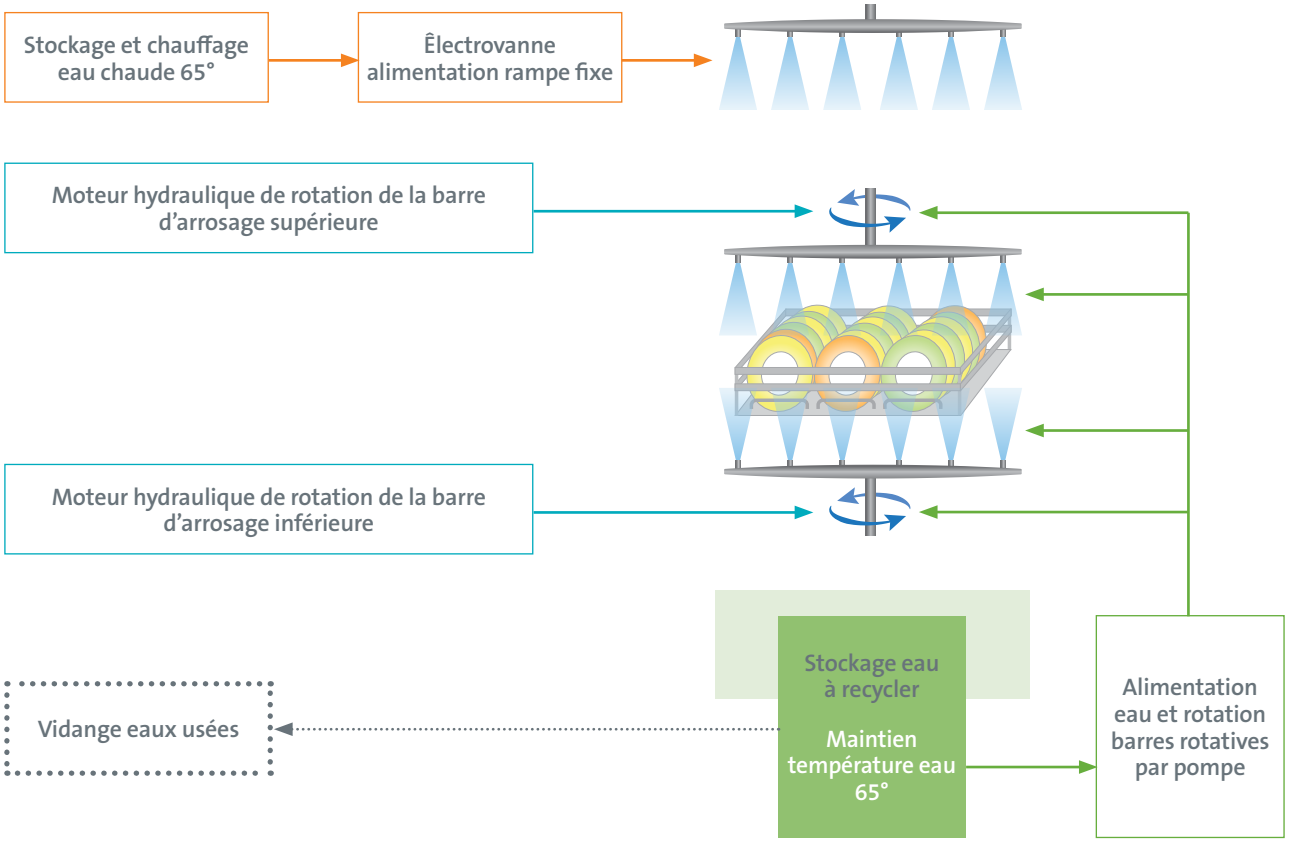
1. Description du lave-vaisselle professionnel pris en exemple

Les éléments de réflexion et les solutions techniques proposés dans cet exemple sont fournis à titre didactique, sur la base d'une machine dont le cahier des charges et les principes décrits ne sont pas nécessairement identiques à ceux des lave-vaisselle du marché. Seuls certains risques d'origine thermique et mécanique ont été retenus pour les besoins du document.

L'analyse présentée est donc incomplète. Par exemple, elle n'aborde pas les risques d'origine électrique, chimique (liés aux détergents utilisés) ou les risques thermiques liés à la vaisselle et aux parois chaudes. Seule la phase de vie en mode « production » du lave-vaisselle est prise en compte, sans aborder les autres phases telles que le nettoyage, la maintenance...

Ces éléments ne sont donc pas suffisants ni utilisables en l'état pour la conception d'un lave-vaisselle.

Éléments constitutifs du lave-vaisselle



Principes de base et fonctionnement

Cette machine comprend un seul mode de marche « automatique » mais avec plusieurs cycles préprogrammés possibles. Un cycle comprend par exemple des opérations d'alimentation en eau, de chauffage et maintien en température de l'eau, de lavage, de rinçage et de vidange. La gestion des phases est assurée par un programmateur électronique.

Elle est utilisée par un seul opérateur, situé en face avant, dont la mission consiste à charger et décharger un panier contenant de la vaisselle.

La mise en service de la machine s'effectue par impulsion sur un bouton « mise en service ». Une réserve d'eau chaude à une température de 65 °C est immédiatement constituée pour réduire les temps de cycle. Cette réserve est assurée jusqu'à la mise hors service de la machine.

Après chargement d'un panier de vaisselle sale, le départ d'un cycle s'effectue par impulsion sur un bouton.

L'eau chaude est projetée à la pression du réseau (électrovanne d'alimentation) par une rampe fixe à plusieurs jets sur la vaisselle (afin d'immédiatement commencer le mouillage/prélavage ou le rinçage de la vaisselle) jusqu'à obtention d'une quantité d'eau suffisante à recycler pour les phases de lavage et rinçage.

Cette eau est stockée et maintenue en température par des résistances électriques.

L'eau ainsi stockée est projetée sur la vaisselle par 2 barres (supérieure et inférieure) animées en rotation pour le lavage et le rinçage.

Lorsque prévu dans le cycle, les eaux usées sont évacuées de la cuve.

Le cycle se termine automatiquement à la fin du programme sélectionné et signale le moment ou la vaisselle propre peut être déchargée.

La machine reste en attente d'un nouveau cycle.

La mise hors service de la machine s'effectue par impulsion sur un bouton « arrêt ».

2. Extraits des résultats du processus d'appréciation et de réduction du risque suivant la norme NF EN ISO 12100

Les tableaux suivants présentent des extraits d'une analyse du risque qui doit être réalisée intégralement. Ces extraits sont destinés à illustrer les informations pouvant être recueillies en suivant la norme, et qui sont utiles dans la suite du document pour traiter de la conception d'une partie du système de commande relatif à la sécurité.

Tableau 1. Détermination des limites de la machine

NF EN ISO 1200 – § 5.3.2. Limites d'utilisation	
§ 5.3.2.a Modes de fonctionnement/ Procédures d'intervention	– Mode de fonctionnement « production » suivant des programmes automatiques. – Chargement/déchargement manuel de la vaisselle dans la zone de lavage, machine en pause (sous tension mais à l'arrêt), en attente d'un ordre de départ cycle.
§ 5.3.2.b et § 5.3.2.c Personnel/formation	– Personnel de cuisine polyvalent mais formé à l'utilisation de cette machine.
§ 5.3.2.d Autres personnes exposées aux phénomènes dangereux	– Sans objet. Lieu à accès limité.
§ 5.3.3 Limites dans l'espace	– La zone de lavage est dimensionnée en fonction des dimensions standard d'un panier/d'une cagette de vaisselle, y compris l'encombrement de la vaisselle. – Zone située à une hauteur de 850 mm du sol. – Les faces latérales droite et gauche et la face avant doivent être libres d'accès pour le chargement/déchargement. – La face arrière peut être totalement fermée.
§ 5.3.4 Limites dans le temps	– Chargement/déchargement de 5 fois par heure, chaque fois d'une durée d'environ 3 minutes de changement de panier à vaisselle. – Utilisation 210 jours/an. – Nettoyage 3 fois par jour (dont filtres), durée 5 min.
§ 5.3.5 Autres limites	– Machine prévue pour un usage professionnel, dans un local de cuisine.

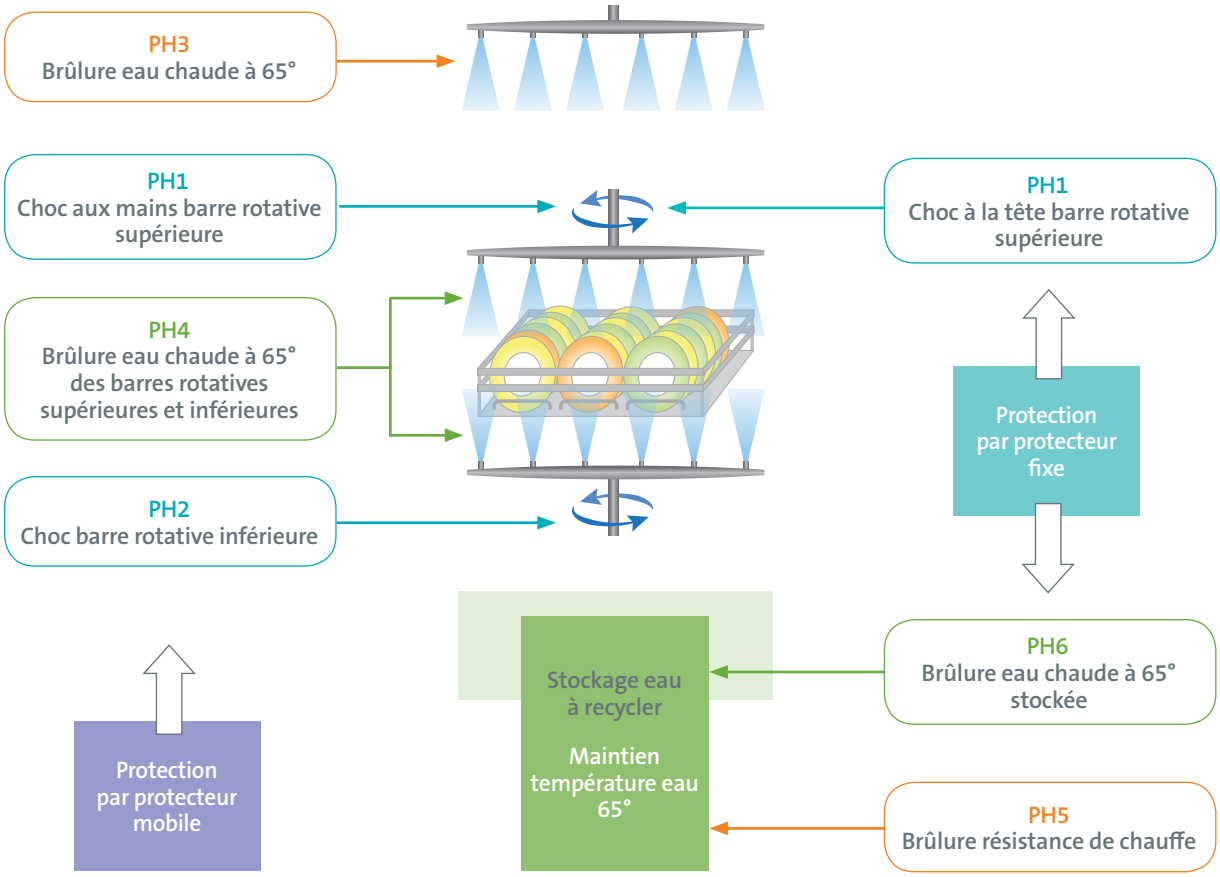
Tableau 2. Eléments d'appréciation et de réduction du risque

NF EN ISO 12100							
Identification des phénomènes dangereux (§ 5.4* et annexe B)		Estimation du risque (§ 5.5)				Réduction du risque (§ 6)	
Phénomène dangereux (PH)	Parties du corps exposées	Gravité (§ 5.5.2.2)	Exposition au phénomène dangereux (§ 5.5.2.3.1) Fréquence/Durée (F/D)	Possibilité d'éviter le dommage (§ 5.5.2.3.3)	Occurrence d'un événement dangereux (§ 5.5.2.3.2)	Mesure technique de prévention	Fonction de sécurité associée (FS)
PH1 Chocs avec la barre rotative d'arrosage supérieure en mouvement	Mains et tête	Blessure légère (contusion, choc léger)	**Mains** F = faible (car elles tiennent le bac ou sont éloignées de la rampe). **Tête** F = fréquente **Mains et tête** D = faible (temps de pose/retrait du panier)	Phénomènes survenant rapidement, donc laps de temps insuffisant pour une réaction de la personne exposée	Niveau d'occurrence « élevé »	Protecteur mobile verrouillé pour arrêt rotation de la barre supérieure	**FS1** Arrêt par protecteur mobile de la rotation de la barre supérieure
						Protecteur fixe contre les chocs à la tête par la barre	Sans objet
PH2 Chocs avec la barre rotative d'arrosage inférieure en mouvement	Mains	Blessure légère (contusion, chocs léger)	F = faible (car les mains tiennent le bac et le bac fait obstruction au phénomène dangereux) D = faible (mêmes raisons)	Phénomènes survenant rapidement donc laps de temps insuffisant pour une réaction de la personne exposée	Niveau d'occurrence « élevé »	Protecteur mobile verrouillé pour arrêt rotation de la barre inférieure	**FS2** Arrêt par protecteur mobile de la rotation de la barre inférieure

PH3 Brûlure par l'eau chaude issue des barres rotatives supérieure et inférieure à température de 65°	Mains et tête	Brûlure –blessure réversible	F = fréquente (car correspondant à la fréquence d'intervention) D = Importante (par rapport à la température élevée de l'eau)	Phénomènes survenant rapidement donc laps de temps insuffisant pour une réaction de la personne exposée	Niveau d'occurrence « élevé »	Protecteur mobile verrouillé pour coupure d'arrivée d'eau chaude depuis les barres rotatives	**FS3** Arrêt par protecteur mobile des jets d'eau depuis les barres rotatives
PH4 Brûlure par l'eau chaude issue de la rampe fixe à température de 65°	Mains et tête	Brûlure –blessure réversible	F = fréquente (car correspondant à la fréquence d'intervention) D = Importante (par rapport à la température élevée de l'eau)	Phénomènes survenant rapidement donc laps de temps insuffisant pour une réaction de la personne exposée	Niveau d'occurrence « élevé »	Protecteur mobile verrouillé pour coupure d'arrivée d'eau chaude depuis la rampe fixe	**FS4** Arrêt par protecteur mobile des jets d'eau depuis la rampe fixe
PH5 Brûlure par la résistance de chauffage de 65°	Mains	Brûlure – blessure réversible	F et D = faibles (car les mains tiennent le bac et le bac fait obstruction au phénomène dangereux)	Perception de la chaleur, donc conscience du risque	Niveau d'occurrence « élevé »	Protecteur fixe pour empêcher accès à la résistance	Sans objet
PH6 Brûlure avec l'eau chaude de lavage stockée à température de 65°	Mains	Brûlure –blessure réversible	F et D = faibles (car les mains tiennent le bac et le bac fait obstruction au phénomène dangereux)	Perception de la chaleur, donc conscience du risque	Niveau d'occurrence « élevé »	Protecteur fixe pour empêcher accès à l'eau chaude	Sans objet
PH7 Chocs/contacts avec les différentes parties mécaniques à l'arrêt	Mains et tête	Blessure légère	F = fréquente (car correspondant à la fréquence d'intervention) D = faible	Impossible car mouvements de l'opérateur cadencés	Niveau d'occurrence « élevé »	Mesure intrinsèque Suppression des angles vifs et des parties saillantes	Sans objet

** Extraits de la norme NF EN ISO 12100*
§ 5.4.a) En mode production lors du chargement/déchargement de la vaisselle, si un ordre de départ cycle est ordonné (ex. commande normale de départ cycle).
§ 5.4.b) En cas de départ intempestif (ex. défaillance d'un composant du système de commande.
§ 5.4.c) Lors d'un accès inopiné à la zone de lavage en cour de cycle (ex. comportement réflexe d'une personne en cas d'incident de lavage.

Représentation synthétique des phénomènes dangereux (hors PH7) et des moyens de protection associés



3. Exemples de défaillances de diverses origines qui pourraient affecter une fonction de sécurité

▶ Un relais électromécanique qui reste bloqué « actionné » à cause d'un de ses contacts qui s'est soudé.

▶ Un capteur électromécanique qui ne commute plus à cause d'un amoncellement de poussières ou de particules dans son enveloppe.

▶ Un court-circuit entre les conducteurs externes de raccordement d'une pédale de commande, dû à la dégradation de son câble.

▶ Un défaut de masse avec des conducteurs électriques qui viennent en contact avec le bâti d'une machine, par exemple des conducteurs écrasés mécaniquement, dénudés par usure de l'isolant, ...

▶ Une perturbation électromagnétique qui fait commuter intempestivement des sorties de système électronique.

▶ Une surtension ou une surpression qui endommage simultanément plusieurs composants.

▶ Un capteur qui commute intempestivement suite à un choc ou des vibrations auxquelles il est soumis.

▶ Un distributeur hydraulique ou pneumatique qui ne fonctionne plus, à cause de joints internes défectueux ou de ressorts internes inopérants.

▶ Un vérin pneumatique qui se met intempestivement en mouvement à cause d'une pression résiduelle stockée dans le circuit.

▶ Un bouton poussoir qui ne revient pas au repos à cause d'un blocage mécanique interne.

▶ Une séquence logicielle qui ne se déroule pas comme prévu et qui tourne en boucle plutôt que de commander un ordre d'arrêt.

▶ Une fuite d'huile qui survient suite à une détérioration d'un tuyau flexible et qui crée un mouvement intempestif.

▶ Une coupure intempestive d'alimentation en énergie qui survient suite à une panne de réseau.

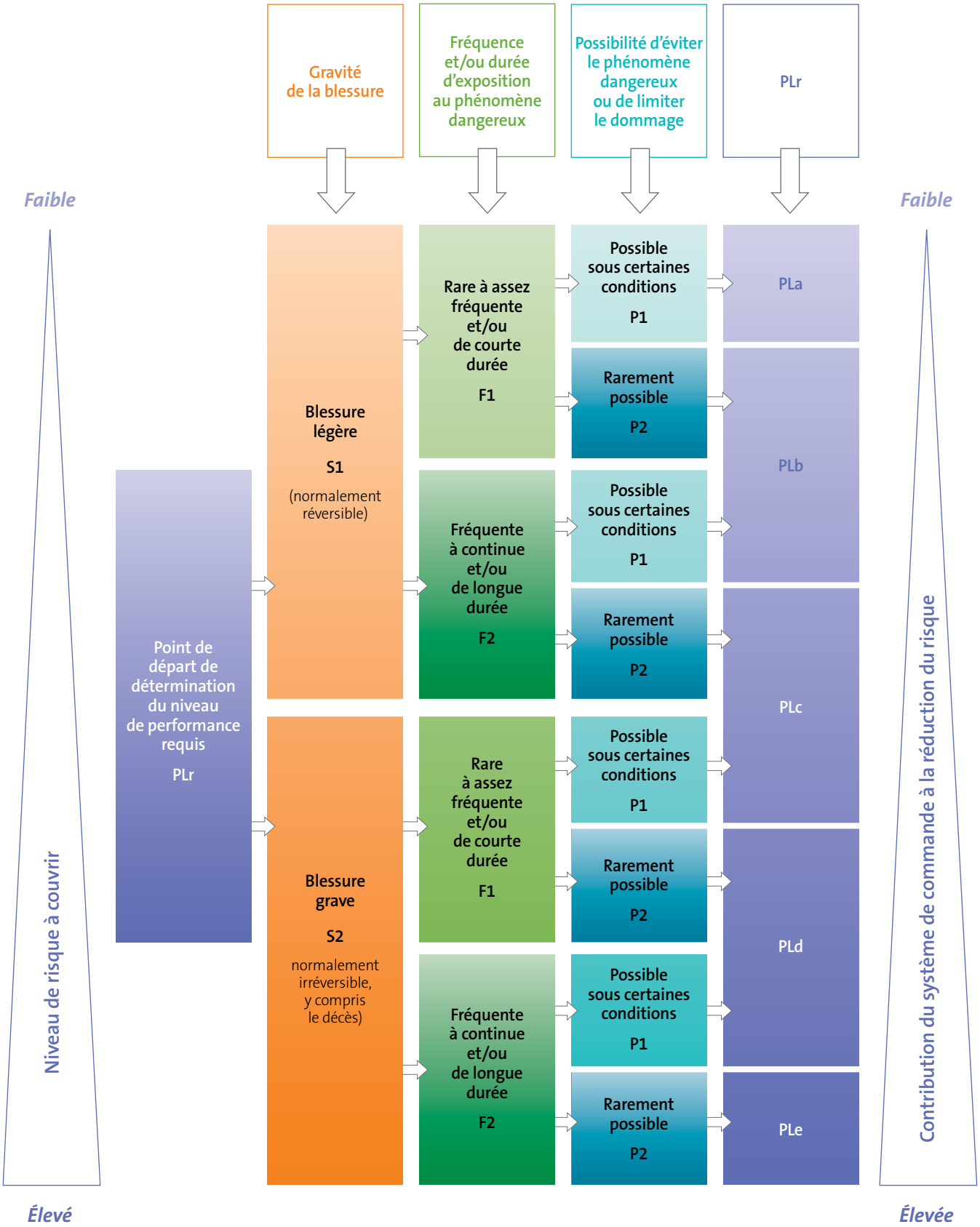
▶ Un composant dont la panne est liée au dépassement de la durée de vie préconisée par son fabricant.

▶ (...)

4. Exemple de spécification détaillée d'une fonction de sécurité

Spécification des exigences fonctionnelles de la fonction de sécurité	
N° FS1	**Nom de la fonction** Arrêt par protecteur mobile de la rotation de la barre supérieure.
Niveau de performance requis	PLr = b
Conditions d'activation de la fonction	Cette fonction est active en permanence
Interface	Entrée : dispositif de verrouillage du protecteur mobile. Sortie : bornes du moteur électrique de la pompe de recyclage.
Comportement de la fonction	Cette fonction consiste à arrêter et empêcher le mouvement de rotation de la barre rotative d'arrosage si le protecteur est ouvert et, si celui-ci est fermé, à autoriser le mouvement de rotation par les ordres de commande issus du programmateur électronique de cycles de lavage.
Priorité par rapport à d'autres fonctions simultanées	Cette fonction de sécurité doit être prioritaire sur les ordres de commande du mouvement de rotation issus du programmateur électronique de cycles de lavage.
Autres fonctions agissant sur le même actionneur	FS2 et FS4.
Temps de réaction maximal de la fonction	Le temps de réaction maximal compris entre l'information d'entrée et la sortie doit être tel que l'opérateur ne puisse pas atteindre la barre supérieure avant son arrêt complet.
Taux de demande de la fonction	La fréquence d'ouverture de la porte est de 5 fois par heure, chaque fois d'une durée d'environ 3 minutes de changement de panier à vaisselle. Utilisation 210 jours/an.
Réaction aux fautes/Conditions de redémarrage	La réaction en cas de défaut doit conduire à arrêter et empêcher le mouvement de rotation de la barre. L'autorisation de redémarrage peut avoir lieu après disparition du défaut.
Conditions d'ambiance	Degré de protection minimal, compte tenu de l'environnement prévisible : IP55 IK07.

5. Critères de détermination du PLr d'une fonction de sécurité



Lignes directrices pour la sélection des paramètres S, F et P

Gravité d'une blessure S1 et S2

Dans l'estimation du risque résultant d'une défaillance de la fonction de sécurité, seules les blessures légères (normalement réversibles) et les blessures graves (normalement irréversibles y compris le décès) sont traitées.

Pour prendre une décision, il convient de prendre en compte les conséquences habituelles des accidents et les processus de guérison normaux pour déterminer S1 et S2; par exemple, les ecchymoses et/ou lacérations sans complication seraient classées S1, tandis qu'une amputation ou un décès serait classé S2..

Fréquence et/ou durée d'exposition aux phénomènes dangereux F1 et F2

Il n'est pas possible de spécifier une durée valable dans tous les cas pour laquelle il conviendrait de sélectionner le paramètre F1 ou le paramètre F2. Cependant, les explications suivantes peuvent aider à prendre la bonne décision en cas de doute.

Il convient de sélectionner F2 si une personne est fréquemment ou continuellement exposée au phénomène dangereux. Le fait que les mêmes personnes ou des personnes différentes soient exposées au phénomène dangereux lors d'expositions successives, par exemple lors de l'utilisation d'ascenseurs, est sans importance. Il convient de choisir le paramètre fréquence en fonction de la fréquence et de la durée d'exposition au phénomène dangereux.

Si le taux de sollicitation de la fonction de sécurité est connu par le concepteur, la fréquence et la durée de cette sollicitation peuvent être choisies en lieu et place de la fréquence et de la durée d'exposition au phénomène dangereux. Dans la présente partie de l'ISO 13849, il est posé pour hypothèse que le taux de sollicitation de la fonction de sécurité est supérieur à une fois par an.

Il convient d'évaluer la durée d'exposition au phénomène dangereux sur la base d'une valeur moyenne qui peut être mise en relation avec la durée totale d'utilisation de l'équipement. Par exemple, s'il est nécessaire d'introduire régulièrement les mains entre les outils d'une machine fonctionnant par cycles pour charger et décharger des pièces, il convient de sélectionner F2. En l'absence d'autres justifications, il convient de choisir F2 si la fréquence est supérieure à un accès par 15 minutes.

Il est possible de choisir F1 si la durée d'exposition cumulée ne dépasse pas 1/20 du temps de fonctionnement total et que la fréquence est inférieure à un accès par 15 minutes.

Possibilité d'éviter le phénomène dangereux P1 et P2 et probabilité d'occurrence

La probabilité d'éviter le phénomène dangereux et la probabilité d'occurrence d'un phénomène dangereux sont combinées dans le paramètre P. Lorsqu'une situation dangereuse se produit, il convient de ne sélectionner P1 que s'il existe une chance réelle d'éviter un phénomène dangereux ou de réduire ses effets de manière significative. Sinon, il convient de sélectionner P2.

Si la probabilité d'occurrence d'un phénomène dangereux peut être justifiée comme faible, le PLr peut être réduit d'un niveau, voir ci-après en 2.

1. Possibilité d'éviter le phénomène dangereux

Il est important de savoir si une situation dangereuse peut être reconnue avant de causer une blessure et être évitée. Par exemple, l'exposition à un phénomène dangereux peut-elle être identifiée directement par ses caractéristiques physiques, ou par des moyens techniques, par exemple des indicateurs. D'autres aspects importants qui influent sur la sélection du paramètre P sont par exemple les suivants :

- vitesse à laquelle le phénomène dangereux survient (par exemple, rapidement ou lentement),
- possibilités d'éviter le phénomène dangereux (par exemple, en prenant la fuite),
- opérateurs étant ou non compétents et formés,
- opérations réalisées avec ou sans surveillance.

2. Probabilité d'occurrence d'un événement dangereux

La probabilité d'occurrence d'un événement dangereux dépend soit du comportement humain, soit de défaillances techniques. Dans la plupart des cas, les probabilités appropriées ne sont pas connues ou sont difficiles à identifier. Il convient que l'estimation de la probabilité d'occurrence d'un événement dangereux repose sur des facteurs tels que les suivants :

- données de fiabilité,
- historique des accidents survenus sur des machines comparables.

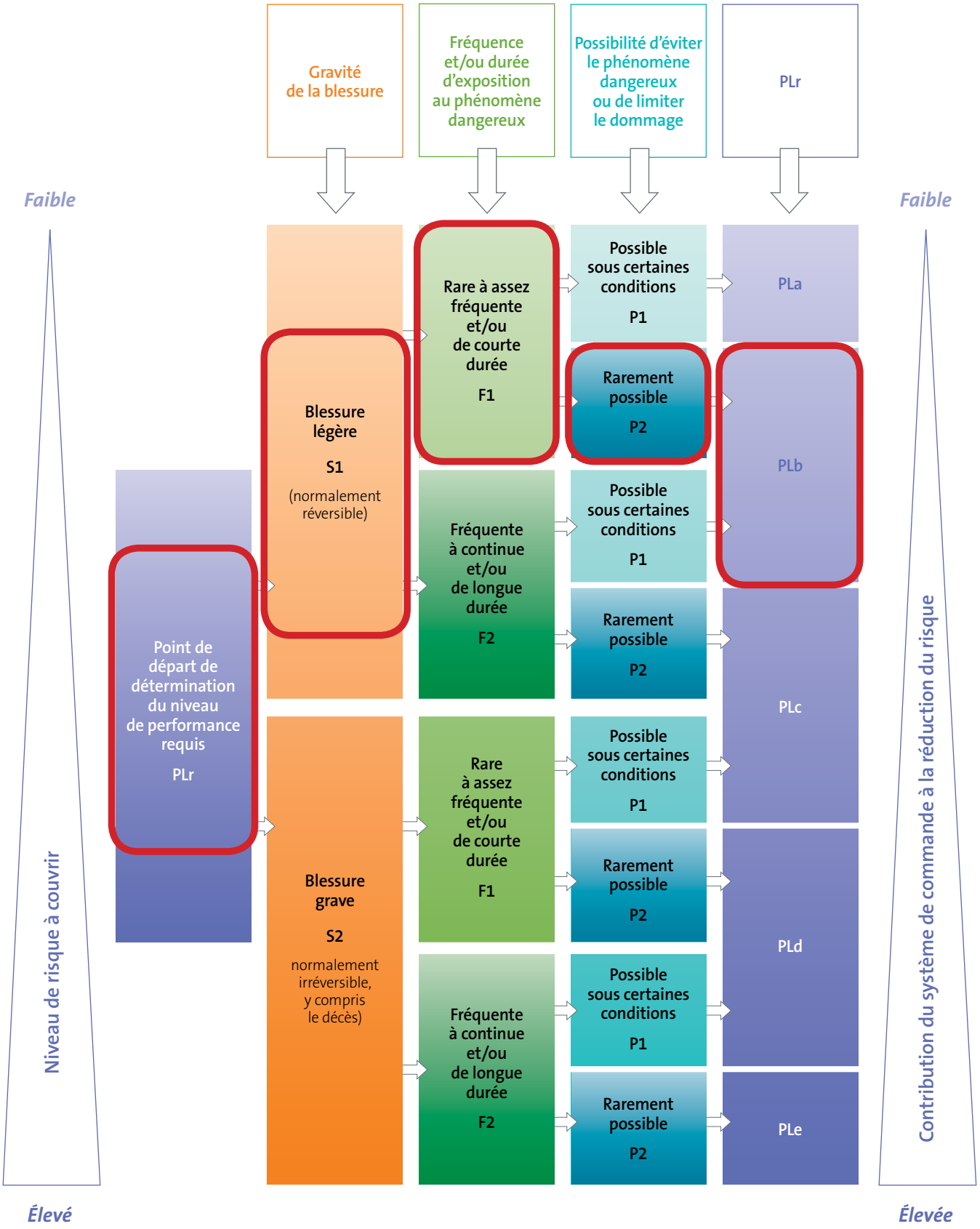
> *Note*
> *Un faible nombre d'accidents ne signifie pas nécessairement que l'occurrence de situations dangereuses est faible, mais que les mesures de sécurité des machines sont suffisantes.*

Lorsqu'il s'agit de machines comparables qui :

- comportent le(s) même(s) risque(s) que ceux que la fonction de sécurité considérée est censée réduire,
- exigent le même procédé et la même action de la part de l'opérateur,
- appliquent la même technologie provoquant l'événement dangereux.

6. Détermination du PLr pour la fonction de sécurité FS1

À l'aide des éléments de l'appréciation du risque (voir tableau 2, 1re ligne), on utilise le graphique de détermination du PLr. Pour la fonction FS1, le PL requis est b.


Gravité de la blessure
Fréquence et/ou durée d'exposition au phénomène dangereux
Possibilité d'éviter le phénomène dangereux ou de limiter le dommage
PLr
Faible
Faible
Point de départ de détermination du niveau de performance requis
PLr
Blessure légère
S1
(normalement réversible)
Blessure grave
S2
normalement irréversible, y compris le décès)
Rare à assez fréquente et/ou de courte durée
F1
Fréquente à continue et/ou de longue durée
F2
Rare à assez fréquente et/ou de courte durée
F1
Fréquente à continue et/ou de longue durée
F2
Possible sous certaines conditions
P1
Rarement possible
P2
Possible sous certaines conditions
P1
Rarement possible
P2
Possible sous certaines conditions
P1
Rarement possible
P2
Possible sous certaines conditions
P1
Rarement possible
P2
PLa
PLb
PLc
PLd
PLe
Niveau de risque à couvrir
Contribution du système de commande à la réduction du risque
Élevé
Élevée

7. Tableau synthétique de détermination des PLr des fonctions de sécurité du lave-vaisselle

Les éléments issus de l'appréciation des risques réalisée avec la norme NF EN ISO 12100 sont rappelés dans le tableau « *Exploitation de l'annexe A de la norme NF EN ISO 13849-1* ». Ils sont à prendre en considération lors de l'utilisation des critères de l'annexe A de la norme NF EN ISO 13849-1.

Fonction de sécurité associée (FS)	Gravité (§ 5.5.2.2)	S	Exposition au phénomène dangereux (§ 5.5.2.3.1) Fréquence/Durée (F/D)	F	Possibilité d'éviter le dommage (§ 5.5.2.3.3)	P	Occurrence d'un événement dangereux (§ 5.5.2.3.2)	Générateur du phénomène dangereux	PLr
FS1 Arrêt par protecteur mobile de la rotation de la barre supérieure	Blessure légère (contusion, choc léger)	**S1**	**Mains** F = faible (car elles tiennent le bac ou sont éloignées de la rampe) **Mains** D = faible (temps de pose/ retrait du panier)	**F1**	Phénomènes survenant rapidement, donc laps de temps insuffisant pour une réaction de la personne exposée	**P2**	Niveau d'occurrence « élevé »	Rotation de la barre supérieure	**PLb**
FS2 Arrêt par protecteur mobile de la rotation de la barre inférieure	Blessure légère (contusion, chocs léger)	**S1**	F = faible (car les mains tiennent le bac et le bac fait obstruction au phénomène dangereux) D = faible (mêmes raisons)	**F1**	Phénomènes survenant rapidement, donc laps de temps insuffisant pour une réaction de la personne exposée	**P2**	Niveau d'occurrence « élevé »	Rotation de la barre inférieure	**PLb**
FS3 Arrêt par protecteur mobile des jets d'eau depuis les barres rotatives	Brûlure –blessure réversible	**S1**	F = fréquente (car correspondant à la fréquence d'intervention) D = importante	**F2**	Phénomènes survenant rapidement, donc laps de temps insuffisant pour une réaction de la personne exposée	**P2**	Niveau d'occurrence « élevé »	Jets d'eau chaude	**PLc**
FS4 Arrêt par protecteur mobile des jets d'eau depuis les rampes fixes	Brûlure –blessure réversible	**S1**	F = fréquente (car correspondant à la fréquence d'intervention) D = importante	**F2**	Phénomènes survenant rapidement, donc laps de temps insuffisant pour une réaction de la personne exposée	**P2**	Niveau d'occurrence « élevé »	Jets d'eau chaude	**PLc**

Pour commander les brochures et les affiches de l'INRS,
adressez-vous au service Prévention de votre Carsat, Cram ou CGSS.

Services Prévention des Carsat et Cram

Carsat ALSACE-MOSELLE
(67 Bas-Rhin)
14, rue Adolphe-Seyboth
CS 10392
67010 Strasbourg cedex
tél. 03 88 14 33 00
fax 03 88 23 54 13
prevention.documentation@carsat-am.fr
www.carsat-alsacemoselle.fr

(57 Moselle)
3, place du Roi-George
BP 31062
57036 Metz cedex 1
tél. 03 87 66 86 22
fax 03 87 55 98 65
www.carsat-alsacemoselle.fr

(68 Haut-Rhin)
11, avenue De-Lattre-de-Tassigny
BP 70488
68018 Colmar cedex
tél. 03 69 45 10 12
fax 03 89 21 62 21
www.carsat-alsacemoselle.fr

Carsat AQUITAINE
(24 Dordogne, 33 Gironde,
40 Landes, 47 Lot-et-Garonne,
64 Pyrénées-Atlantiques)
80, avenue de la Jallère
33053 Bordeaux cedex
tél. 05 56 11 64 36
documentation.prevention@
carsat-aquitaine.fr
www.carsat-aquitaine.fr

Carsat AUVERGNE
(03 Allier, 15 Cantal,
43 Haute-Loire,
63 Puy-de-Dôme)
Espace Entreprises
Clermont République
63036 Clermont-Ferrand cedex 9
tél. 04 73 42 70 19
fax 04 73 42 70 15
offredoc@carsat-auvergne.fr
www.carsat-auvergne.fr

Carsat BOURGOGNE - FRANCHE-COMTÉ
(21 Côte-d'Or, 25 Doubs,
39 Jura, 58 Nièvre,
70 Haute-Saône,
71 Saône-et-Loire, 89 Yonne,
90 Territoire de Belfort)
46, rue Elsa-Triolet
21044 Dijon cedex
tél. 03 80 33 13 92
fax 03 80 33 19 62
documentation.prevention@carsat-bfc.fr
www.carsat-bfc.fr

Carsat BRETAGNE
(22 Côtes-d'Armor, 29 Finistère,
35 Ille-et-Vilaine, 56 Morbihan)
236, rue de Châteaugiron
35030 Rennes cedex 09
tél. 02 99 26 74 63
fax 02 99 26 70 48
drp.cdi@carsat-bretagne.fr
www.carsat-bretagne.fr

Carsat CENTRE - VAL DE LOIRE
(18 Cher, 28 Eure-et-Loir, 36 Indre,
37 Indre-et-Loire, 41 Loir-et-Cher, 45 Loiret)
36, rue Xaintrailles
CS44406
45044 Orléans cedex 1
tél. 02 38 79 70 21
prev@carsat-centre.fr
www.carsat-cvl.fr

Carsat CENTRE-OUEST
(16 Charente, 17 Charente-Maritime,
19 Corrèze, 23 Creuse, 79 Deux-Sèvres,
86 Vienne, 87 Haute-Vienne)
37, avenue du Président-René-Coty
87048 Limoges cedex
tél. 05 55 45 39 04
fax 05 55 45 71 45
cirp@carsat-centreouest.fr
www.carsat-centreouest.fr

Cram ÎLE-DE-FRANCE
(75 Paris, 77 Seine-et-Marne,
78 Yvelines, 91 Essonne,
92 Hauts-de-Seine, 93 Seine-Saint-Denis,
94 Val-de-Marne, 95 Val-d'Oise)
17-19, place de l'Argonne
75019 Paris
tél. 01 40 05 32 64
fax 01 40 05 38 84
demande.de.doc.inrs@cramif.cnamts.fr
www.cramif.fr

Carsat LANGUEDOC-ROUSSILLON
(11 Aude, 30 Gard, 34 Hérault,
48 Lozère, 66 Pyrénées-Orientales)
29, cours Gambetta
34068 Montpellier cedex 2
tél. 04 67 12 95 55
fax 04 67 12 95 56
prevdoc@carsat-lr.fr
www.carsat-lr.fr

Carsat MIDI-PYRÉNÉES
(09 Ariège, 12 Aveyron, 31 Haute-Garonne,
32 Gers, 46 Lot, 65 Hautes-Pyrénées,
81 Tarn, 82 Tarn-et-Garonne)
2, rue Georges-Vivent
31065 Toulouse cedex 9
tél. 36 79
fax 05 62 14 88 24
doc.prev@carsat-mp.fr
www.carsat-mp.fr

Carsat NORD-EST
(08 Ardennes, 10 Aube, 51 Marne,
52 Haute-Marne, 54 Meurthe-et-Moselle,
55 Meuse, 88 Vosges)
81 à 85, rue de Metz
54073 Nancy cedex
tél. 03 83 34 49 02
fax 03 83 34 48 70
documentation.prevention@carsat-nordest.fr
www.carsat-nordest.fr

Carsat NORD-PICARDIE
(02 Aisne, 59 Nord, 60 Oise,
62 Pas-de-Calais, 80 Somme)
11, allée Vauban
59662 Villeneuve-d'Ascq cedex
tél. 03 20 05 60 28
fax 03 20 05 79 30
bedprevention@carsat-nordpicardie.fr
www.carsat-nordpicardie.fr

Carsat NORMANDIE
(14 Calvados, 27 Eure, 50 Manche,
61 Orne, 76 Seine-Maritime)
Avenue du Grand-Cours
76028 Rouen cedex
tél. 02 35 03 58 22
fax 02 35 03 60 76
prevention@carsat-normandie.fr
www.carsat-normandie.fr

Carsat PAYS DE LA LOIRE
(44 Loire-Atlantique, 49 Maine-et-Loire,
53 Mayenne, 72 Sarthe, 85 Vendée)
2, place de Bretagne
44932 Nantes cedex 9
tél. 02 51 72 84 08
fax 02 51 82 31 62
documentation.rp@carsat-pl.fr
www.carsat-pl.fr

Carsat RHÔNE-ALPES
(01 Ain, 07 Ardèche, 26 Drôme, 38 Isère,
42 Loire, 69 Rhône, 73 Savoie,
74 Haute-Savoie)
26, rue d'Aubigny
69436 Lyon cedex 3
tél. 04 72 91 97 92
fax 04 72 91 98 55
preventionrp@carsat-ra.fr
www.carsat-ra.fr

Carsat SUD-EST
(04 Alpes-de-Haute-Provence,
05 Hautes-Alpes, 06 Alpes-Maritimes,
13 Bouches-du-Rhône, 2A Corse-du-Sud,
2B Haute-Corse, 83 Var, 84 Vaucluse)
35, rue George
13386 Marseille cedex 20
tél. 04 91 85 85 36
fax 04 91 85 75 66
documentation.prevention@carsat-sudest.fr
www.carsat-sudest.fr

Services Prévention des CGSS

CGSS GUADELOUPE
Espace Amédée Fengarol, bât. H
Parc d'activités La Providence, ZAC de Dothémare
97139 Les Abymes
tél. 05 90 21 46 00 – fax 05 90 21 46 13
risquesprofessionnels@cgss-guadeloupe.fr
www.cgss-guadeloupe.fr

CGSS GUYANE
Direction des risques professionnels
CS 37015, 97307 Cayenne cedex
tél. 05 94 29 83 04 – fax 05 94 29 83 01
prevention-rp@cgss-guyane.fr

CGSS LA RÉUNION
4, boulevard Doret, CS 53001
97741 Saint-Denis cedex 9
tél. 02 62 90 47 00 – fax 02 62 90 47 01
prevention@cgss.re
www.cgss-reunion.fr

CGSS MARTINIQUE
Quartier Place-d'Armes,
97210 Le Lamentin cedex 2
tél. 05 96 66 51 31 et 05 96 66 76 19 – fax 05 96 51 81 54
documentation.atmp@cgss-martinique.fr
www.cgss-martinique.fr

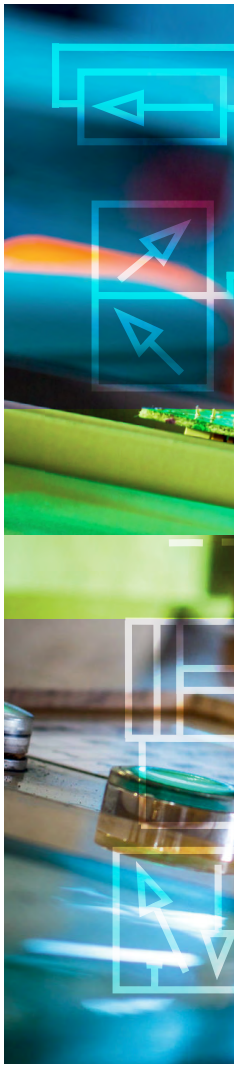
Achevé d'imprimer par xxxxxxx - Code postal Ville
N° d'imprimeur : xxxxxx - Dépôt légal : mois 2016 - Imprimé en France

Afin de réduire le nombre d'accidents du travail de façon pérenne, la sécurité doit être intégrée dès la conception des machines.

Cette brochure traite des principes de conception des systèmes de commande de machines, concernant les parties relatives à la sécurité.

Elle fournit des informations pour permettre l'assimilation et l'application des référentiels normatifs et rappelle les notions relatives à l'appréciation du risque et à sa réduction.

Un exemple d'application de la démarche globale de conception d'un système de commande est également présenté.



Institut national de recherche et de sécurité
pour la prévention des accidents du travail et des maladies professionnelles
65, boulevard Richard-Lenoir 75011 Paris • Tél. 01 40 44 30 00 • info@inrs.fr

Édition INRS ED 6310
1re édition • février 2019 • 3 000 ex. • ISBN 978-2-7389-2298-4

L'INRS est financé par la Sécurité sociale - Assurance maladie / Risques professionnels

www.inrs.fr YouTube