Institut National de Recherche et de Sécurité

Aborder la norme NF EN ISO 13849-1 via la conception d'une fonction de sécurité basique

NS 302 NOTE SCIENTIFIQUE ET TECHNIQUE

Aborder la norme NF EN ISO 13849-1 via la conception d'une fonction de sécurité basique

James BAUDOIN
Jean-Paul BELLO
INRS, Département Ingénierie des Equipements de Travail
Laboratoire Sûreté des Systèmes Automatisés

NS 302
février 2013

Institut national de recherche et de sécurité pour la prévention des accidents du travail et des maladies professionnelles
Siège social : 65 boulevard Richard Lenoir 75011 Paris • Tél. 01 40 44 30 00 • Fax 01 40 44 30 99
Centre de Lorraine : 1, rue du Morvan CS 60027 54519 Vandœuvre-les-Nancy cedex • Tél. 03 83 50 20 00 • Fax 03 83 50 20 97

Résumé :

Le présent document a pour objectif de guider les concepteurs devant réaliser le circuit de commande de machines intégrant seulement une ou quelques fonctions de sécurité « basiques », telles qu'un arrêt d'urgence ou un protecteur mobile.

Parmi les référentiels disponibles pour la conception des machines, la norme NF EN ISO 13849-1 permet de traiter les systèmes de commande mettant en œuvre différents types d'énergie tels que l'électrique, l'hydraulique ou le pneumatique. Cette norme décrit les principes généraux de conception des parties des systèmes de commande relatives à la sécurité (SRP/CS).

Ce document est basé sur la mise en œuvre de la méthode simplifiée de la norme NF EN ISO 13849-1 et permet d'appréhender les notions nouvelles qu'elle introduit.

La première partie du document intitulée : Guide de conception d'une SRP/CS, apporte des éclairages sur certaines parties de la norme et propose également des outils (graphes, tableaux,…) destinés à en faciliter la compréhension et l'utilisation mais également les choix que les concepteurs seront amenés à faire.

La deuxième partie est constituée d'un cas pratique d'une fonction de sécurité traité par l'INRS sur la base de la norme et des outils présentés dans le guide. L'ensemble des phases de conception est abordé, en faisant ressortir les détails et commentaires jugés nécessaires pour assimiler les principes préconisés par la norme.

Bien que nouvelle, la norme NF EN ISO 13849-1 n'apporte pas de grands changements dans la conception des systèmes de commande relatifs à la sécurité. Elle conserve en grande partie les principes de conception préconisés dans la norme NF EN 954-1 qu'elle remplace désormais. La principale nouveauté de ce référentiel réside dans la quantification d'un certain nombre de paramètres.

Abstract:

This document is intended to guide designers to perform machinery control systems with only one or a few "basic" safety functions such as emergency stop or movable guard.

Among the available standards for machine design, NF EN ISO 13849-1 is the one providing recommendations to design safety related parts of control systems (SRP / CS) implementing different types of energy such as electric, hydraulic or pneumatic.

This document is based on the implementation of the simplified method of NF EN ISO 13849-1 and helps to understand the new concepts introduced by this standard.

The first part of the document entitled: Design guide for a SRP/CS, sheds light on some parts of the standard and also provides tools (graphs, tables ...) to facilitate the understanding and use but also choices that designers will have to do.

The second part consists of a practical case of a safety function designed by INRS using the standard and the tools shown in the guide. All phases of design are discussed, highlighting details and comments deemed necessary to assimilate the principles advocated by the standard.

Although new, the standard NF EN ISO 13849-1 does not bring major changes in the design of control systems related to safety. It retains much of the design principles recommended in the standard NF EN 954-1 that it replaces. The main new of this framework lies in the quantification of a number of parameters.

SOMMAIRE

Préambule

Lors de la conception d'un équipement de travail, tel qu'une machine, il est nécessaire de prendre en compte sa partie « système de commande ». Cette dernière est destinée à assurer les fonctionnalités attendues de l'équipement. Lorsque des fonctions de sécurité sont nécessaires, le système de commande doit également les traiter afin de contribuer à la réduction des risques générés par l'équipement de travail, vis-à-vis des opérateurs et tierces personnes exposés.

Parmi les référentiels disponibles pour la conception des machines, la norme NF EN ISO 13849-1[1] permet de traiter les systèmes de commande mettant en œuvre différents types d'énergie tels que l'électrique, l'hydraulique ou le pneumatique. Elle décrit les principes généraux de conception des parties des systèmes de commande relatives à la sécurité (SRP/CS[2]).

Cette norme remplace la norme NF EN 954-1[3] qui était largement connue des industriels mais qui n'est désormais plus en vigueur.

Bien que nouvelle, la NF EN ISO 13849-1 n'apporte pas de grands changements dans la conception des systèmes de commande relatifs à la sécurité. Elle conserve en grande partie les principes de conception préconisés dans la NF EN 954-1. Le concepteur doit continuer à mettre en œuvre :

- des composants aptes à la fonction pour laquelle ils sont destinés,
- des composants conçus selon des principes de sécurité éprouvés,
- des architectures simple ou double canal (redondance),
- en cas de besoin, des diagnostics destinés à tester les composants (autocontrôle),
- des mesures contre les défaillances systématiques,

La principale nouveauté de ce référentiel réside dans la quantification d'un certain nombre de paramètres nécessitant :

- le calcul du $MTTF_d$[4] (temps moyen avant défaillance dangereuse) à partir des données de fiabilité et de sollicitation des composants mis en œuvre,
- la quantification des mesures prises pour assurer la couverture de diagnostic des composants,
- la quantification des mesures prises contre des défaillances de cause communes.

Contrairement à certaines idées reçues, ces calculs sont abordables et limités, si on utilise la procédure simplifiée de la norme, et surtout lorsque les fonctions de sécurité sont simples et mettent en œuvre peu de composants ou lorsque les composants choisis ont des niveaux de performance connus.

Pour les cas d'application plus complexes, un outil logiciel est disponible gratuitement : SISTEMA. Il permet d'assister le concepteur dans l'application de la norme NF EN ISO 13849-1 en imposant de passer par les phases de conception préconisées par cette norme et en calculant les données nécessaires sans avoir à utiliser les formules de calcul.

Le présent document a pour objectif de guider les concepteurs de SRP/CS dans l'utilisation de la norme et de les aider à appréhender les notions nouvelles qu'elle introduit. Il est basé sur un cas pratique traité par l'INRS.

Avertissement 1

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.

Note : Dans la suite du document, tous les renvois (paragraphe, tableau,…) non spécifiés renvoient au présent document.

[1] NF EN ISO 13849-1 : 2008 : Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1 : Principes généraux de conception (appelée « **la norme** » dans le document)
[2] SRP/CS : Safety Related Part/ Control System
[3] NF EN 954-1 : 1997 : Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1 : Principes généraux de conception
[4] $MTTF_d$: Mean Time To dangerous Failure

Guide de conception d'une SRP/CS

1 Introduction

Ce document propose de guider les concepteurs dans la réalisation de SRP/CS, en prenant pour base la méthode simplifiée de la norme NF EN ISO 13849-1 (dont les conditions sont listées au § 4.5.4 de cette norme), mais sans aborder la partie logicielle (§ 4.6 et annexe J de cette norme), ni la phase de validation (§ 8 de cette norme qui renvoie notamment à la norme NF EN ISO 13849-2[5]).

Le système de commande de sécurité d'une machine est constitué d'une ou plusieurs fonctions de sécurité. Chaque fonction de sécurité est réalisée par sa propre partie de système de commande qui, pour faciliter la lecture de ce guide, porte l'abréviation (SC/FS[6]).

Chaque SC/FS intègre au moins une partie matérielle (SRP/CS) et comprend éventuellement une partie logicielle. Un SC/FS doit respecter un niveau de performance de sécurité défini et adapté à l'importance des risques que la fonction de sécurité qu'il traite doit réduire.

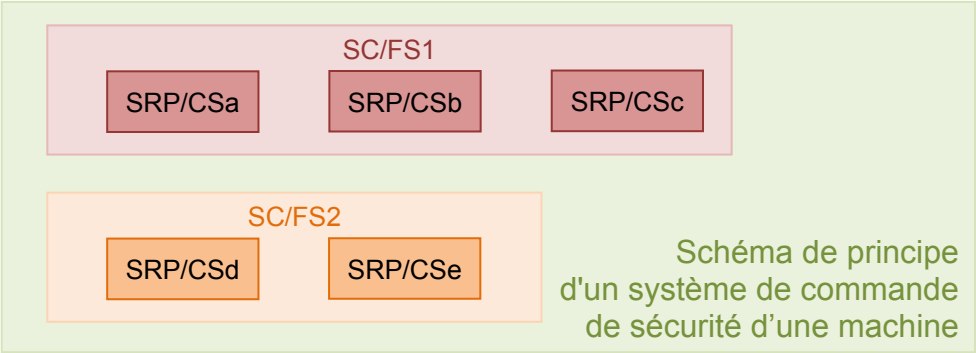


Figure 1 : Exemple de structure d'un système de commande de sécurité d'une machine

2 Spécification d'une fonction de sécurité

La première étape préalable à la conception d'un SC/FS est de spécifier précisément la fonction de sécurité qu'il contribuera à réaliser, en décrivant notamment :

- son niveau de performance de sécurité requis PL_r (voir § 3),
- ses conditions d'activation, comme par exemple les modes de marche dans lesquels la fonction est active/inactive,
- son fonctionnement, en décrivant l'action attendue, en fonction des informations d'entrée,
- sa priorité par rapport à d'autres fonctions simultanées,
- son temps de réaction maximal,
- sa fréquence de sollicitation,
- les conditions environnementales,
- …

3 Détermination d'un niveau de performance requis

Un SC/FS doit posséder un certain niveau de performance de sécurité pour pouvoir assurer la fonction de sécurité qui lui est confiée. Dans la norme NF EN ISO 13849-1, la capacité d'un SC/FS à réaliser une fonction

[5] NF EN ISO 13849-2 : 2008 : Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2 : Validation
[6] SC/FS : Système de Commande de la Fonction de Sécurité (cette abréviation n'est pas normalisée).

de sécurité est exprimée au travers de la détermination du niveau de performance (PL[7]). La norme définit 5 niveaux de performance possibles pour un système de commande, qui s'échelonnent de PL « a » à PL « e » (voir Figure 2). Avant de concevoir un SC/FS, il est indispensable de déterminer un niveau de performance requis (PL_r) pour la fonction de sécurité qu'il devra réaliser. Le PL atteint par le SC/FS devra être au moins égal au PL_r de cette fonction de sécurité. Le PL_r est fonction de l'importance de la contribution de la fonction de sécurité à la réduction du risque, déterminée suite à une estimation de ce risque. L'annexe A de la norme décrit une méthode pour la détermination du PL_r.

La valeur de PL_r déterminée pour le SC/FS doit au minimum être requise pour la ou les SRP/CS qui le constituent.

Pour chaque niveau de performance, la norme a fait correspondre une valeur de probabilité moyenne d'une défaillance dangereuse par heure (PFH_d[8]) du système de commande (tableau 3 de la norme). Une défaillance est qualifiée de dangereuse lorsqu'elle peut conduire à une situation potentiellement dangereuse.

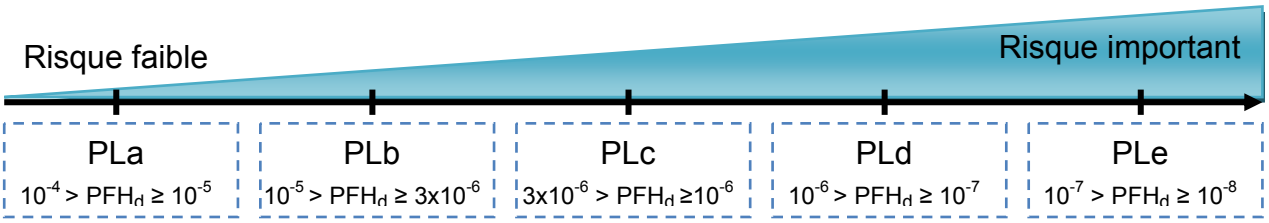


Figure 2

4 Processus général de conception d'un SC/FS

4.1 Modèle général de structure logique pour un SC/FS

Chaque SC/FS comprend généralement plusieurs entités logiques pour traiter les ordres d'entrée et commander des pré-actionneurs via une unité de traitement. La Figure 3 représente le cas le plus fréquent constitué de trois entités.

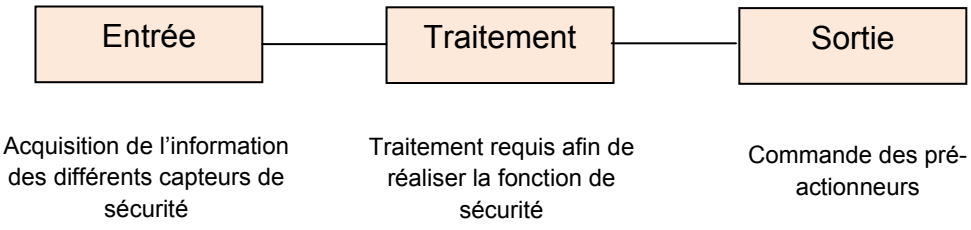


Figure 3

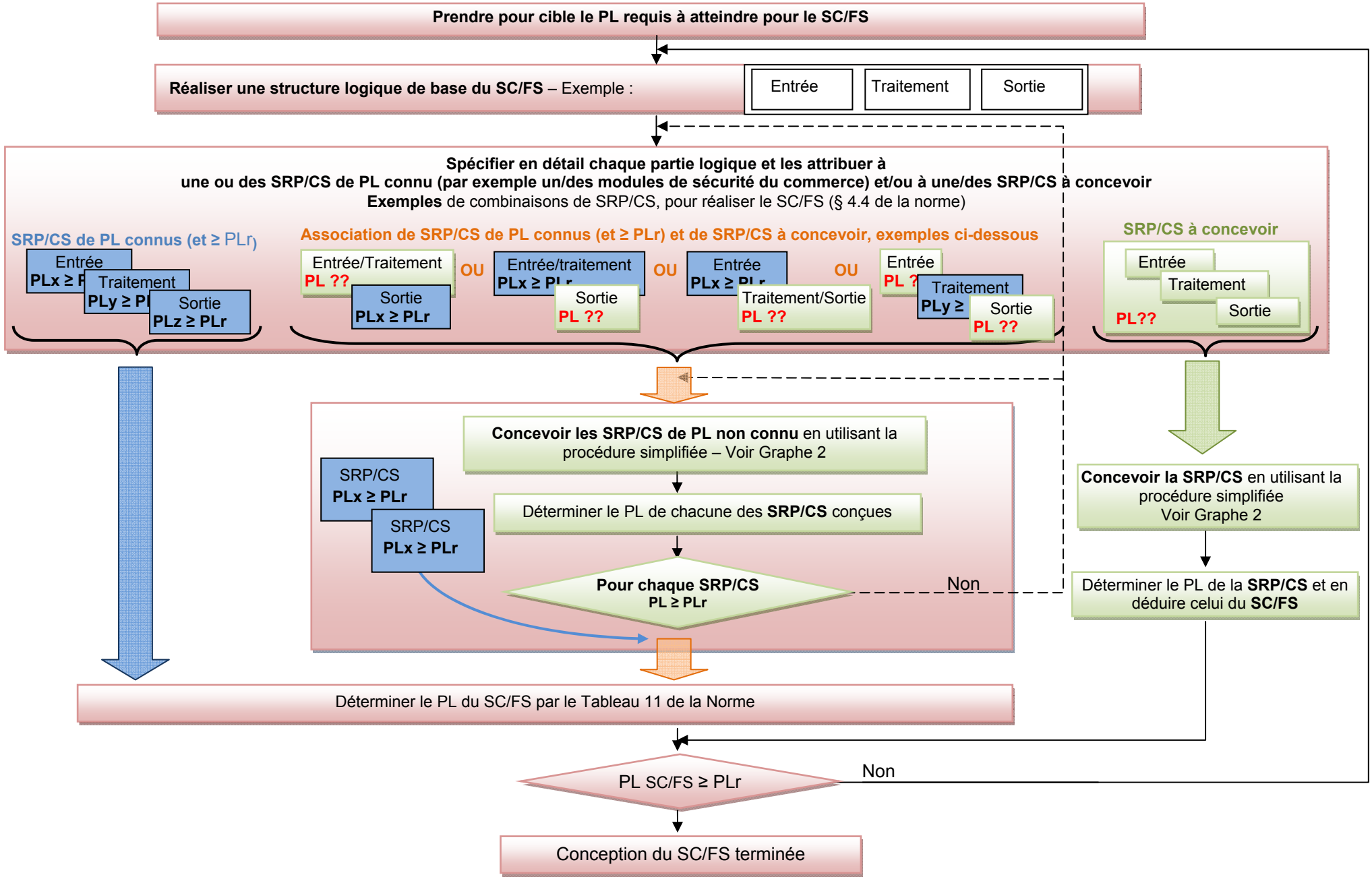
Le concepteur a le choix de décliner ces entités logiques en une ou plusieurs SRP/CS suivant le matériel qu'il envisage de mettre en œuvre. Cette déclinaison peut s'effectuer de différentes manières illustrées dans le paragraphe 4.2.

[7] PL : Performance Level
[8] PFH_d : average Probability of dangerous Failure per Hour

4.2 Graphe du processus général de conception d'un SC/FS en vue d'atteindre un PL requis

Le Graphe 1 illustre :

- différentes voies de conception proposées par la norme NF EN ISO 13849. Le choix du concepteur est déterminé par les composants existant sur le marché, par les pratiques de conception propres à chaque entreprise, par la complexité du SC/FS à réaliser, par la technologie des composants utilisés,…
- différentes façons de déterminer le niveau de performance « PL » obtenu pour un SC/FS en vue de le comparer au PL requis.



Graphe 1 : Processus général de conception d'un SC/FS en vue d'atteindre un PL requis

Le Graphe 1 montre que le concepteur du système de commande a le choix entre trois possibilités :

- Dans la branche de gauche, il associe uniquement des SRP/CS de PL connu (données fournies par le constructeur) et supérieur ou égal au PL requis pour la SC/FS (représentées en couleur bleue), telles qu'un module de sécurité du commerce, un barrage immatériel,... (exemple Figure 4).
  Le PL du SC/FS est déterminé en appliquant le paragraphe 6.3 de la norme et notamment son tableau 11 (Prendre en compte l'Avertissement 2 de ce document).

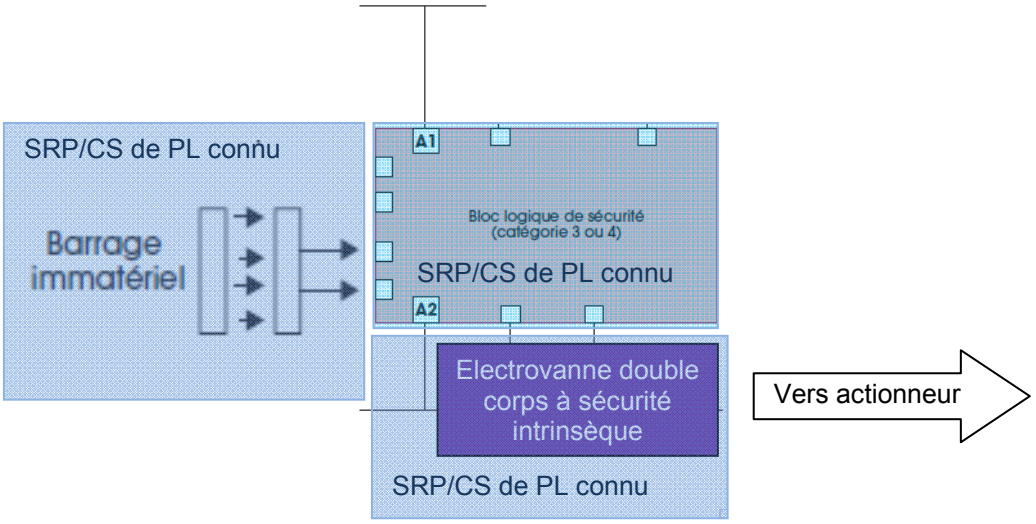


Figure 4 : Exemple de SC/FS constituée de 3 SRP/CS de PL connus

- Dans la branche centrale, c'est une solution mixte qui est illustrée. Le concepteur associe une ou des SRP/CS de PL connu et supérieur ou égal au PL requis pour le SC/FS (représentées en couleur bleue) et une ou des SRP/CS de sa propre conception (représentées en couleur verte), exemple Figure 5. Les étapes de la conception d'une SRP/CS sont présentées dans le Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis.
  Le PL du SC/FS est déterminé en appliquant le paragraphe 6.3 de la norme et notamment son tableau 11 (Prendre en compte l'Avertissement 2 de ce document).

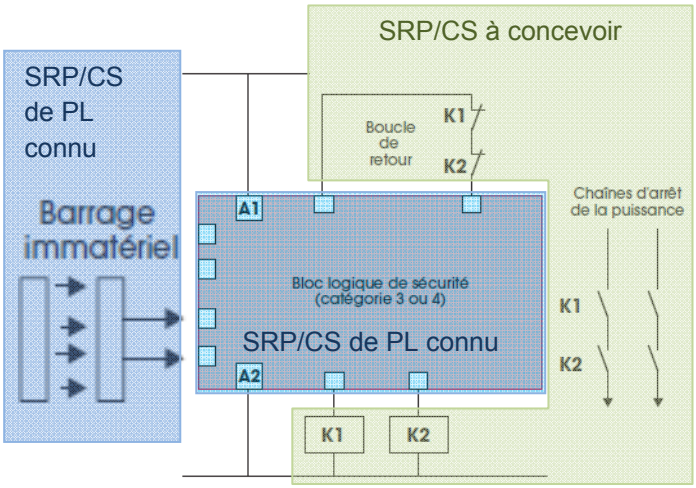


Figure 5 : Exemple de SC/FS constituée d'une combinaison de SRP/CS de PL connus et d'une à concevoir

- Dans la branche de droite, le concepteur met en œuvre une seule SRP/CS de sa propre conception (représentée en couleur verte), exemple Figure 6.

Il s'agit par exemple d'assembler des composants le plus souvent basiques, tels que des interrupteurs de position, des détecteurs de proximité, des relais électromécaniques.
Les étapes de la conception d'une SRP/CS sont présentées dans le Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis.

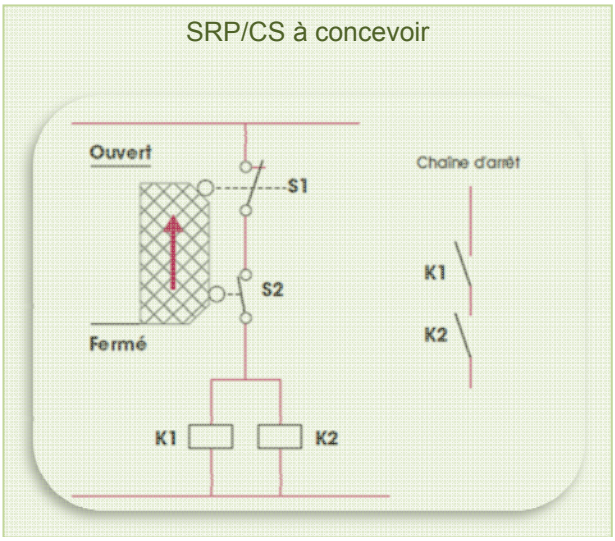


Figure 6 : Exemple de SC/FS constituée d'une SRP/CS à concevoir

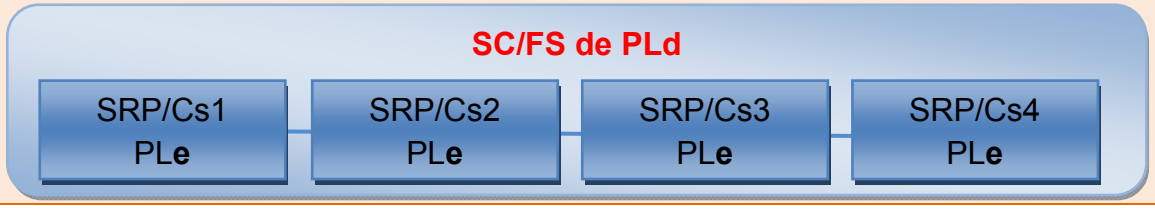
Avertissement 2

Combinaison de plusieurs SRP/CS au sein d'une même SC/FS

Lors de la combinaison de plusieurs SRP/CS en alignement série[9], il est nécessaire que le PL de chacune d'elles soit déterminé. Ensuite, le PL de la SC/FS va dépendre de celui de ces SRP/CS. Il sera alors :

- Egal au PL le plus bas parmi les SRP/CS, si une seule SRP/CS est de ce PL.
  Exemple

- Inférieur ou égal au PL le plus bas, suivant le nombre de SRP/CS qui sont de ce PL. Le tableau 11 de la norme indique le PL global en fonction du nombre de SRP/CS de PL le plus bas.
  Dans l'exemple suivant, le PL le plus bas est « PLe ». Pour un nombre SRP/CS de PLe supérieur à 3, le tableau 11 impose de réduire le PL de cette SC/FS à « PLd ».



[9] Alignement série : mise en œuvre de plusieurs SRP/CS de telle manière que la défaillance de chacune des SRP/CS entraîne une défaillance du SC/FS

4.3 Spécification d'une SRP/CS

En fonction de la voie de conception retenue, chacune des SRP/CS composant la SC/FS sera soit choisie "sur étagère", soit conçue spécifiquement. Pour l'une comme pour l'autre, il est nécessaire de spécifier, à partir de la spécification du SC/FS dans lequel elle va s'intégrer (cf. paragraphe 2), la fonction qu'elle devra réaliser, en précisant notamment :

- son PL requis, qui sera au moins égal au PL_r du SC/FS,
- ses conditions d'activation, comme par exemple les modes de marche dans lesquels la SRP/CS est active/inactive,
- son fonctionnement, en décrivant l'action attendue, en fonction des informations d'entrée,
- son interface avec les autres SRP/CS,
- sa priorité par rapport à d'autres fonctions simultanées,
- son temps de réaction maximal,
- sa fréquence de sollicitation (qui peut être différente de celle du SC/FS),
- les conditions environnementales,
- …

Note : lorsqu'un SC/FS est constitué d'une seule SRP/CS, la spécification de la SRP/CS est identique à celle de la fonction de sécurité et il n'y a pas nécessité d'une nouvelle spécification.

5 Association de SRP/CS de PL connu

Dans le cas d'un assemblage (ex : Figure 4) ou de l'intégration (ex : Figure 5) de SPR/CS de PL connu au sein d'un SC/FS, il est également nécessaire de mettre en œuvre des mesures contre les défaillances systématiques. Ces mesures concernent principalement le respect des notices de mise en œuvre des différents composants ainsi que les raccordements inter-composants (voir exemple, Figure 17 au paragraphe A5.2).

6 Détails de la conception d'une SRP/CS

6.1 Principe

Pour chacune des SRP/CS qu'il devra concevoir spécifiquement, l'objectif du concepteur sera de mettre en œuvre les mesures nécessaires pour atteindre un niveau de performance au moins égal au PL_r pour le SC/FS. Pour cela, il est indispensable de considérer l'ensemble des critères suivants, listés dans le § 4.5.1 de la norme :

- la structure (voir Article 6 de la norme),
- le comportement de la fonction de sécurité en cas de défaillance (voir Article 6 de la norme),
- l'aptitude à exécuter une fonction de sécurité dans des conditions environnementales prévues,
- les défaillances de cause commune « CCF » (voir Annexe F de la norme),
- les défaillances systématiques (voir Annexe G de la norme),
- la valeur de $MTTF_d$ (temps moyen avant défaillance dangereuse) pour des composants uniques (voir Annexes C et D de la norme),
- la Couverture de diagnostics « DC » (voir § 4.5.3 et Annexe E de la norme),
- le logiciel relatif à la sécurité (voir § 4.6 et Annexe J de la norme).

6.2 Aide aux choix des préconisations minimales les mieux appropriées pour la conception d'une SRP/CS

La présentation de la norme est telle qu'il est difficile, au moment d'engager les travaux de conception d'une SRP/CS, d'avoir une vue globale des différentes possibilités d'atteindre le PL_r ainsi que les critères minimaux à respecter. Quelles sont par exemple les catégories autorisées ou encore les valeurs de $MTTF_d$ cible à viser ?

C'est pourquoi des tableaux, fournis en annexe 1 de ce document, ont été créés pour faciliter ce choix. Ils sont notamment basés sur le tableau 7 de la norme et sont prévus pour appliquer la procédure simplifiée proposée pour atteindre le PL requis.

Cinq tableaux sont fournis correspondant aux cinq niveaux de PL_r (a, b, c, d et e) auxquels peut prétendre une SRP/CS. Chacun des tableaux est composé de colonnes correspondant aux catégories pouvant être mises en œuvre pour satisfaire le PL_r. Pour chaque colonne, on retrouve les préconisations minimales (architecture désignée, $MTTF_d$, DC_{avg}, CCF,…) nécessaires pour atteindre le PL_r.

Ces tableaux permettent d'avoir une vue globale des préconisations nécessaires pour la conception d'une SRP/CS pour un PL_r donné et ainsi de pouvoir anticiper des choix matériels (ex : $MTTF_d$) répondant aux critères minimaux requis.

Lors de la conception d'une SRP/CS, il est donc nécessaire de sélectionner le tableau correspondant au PL_r défini pour cette SRP/CS et de choisir une colonne correspondant à une catégorie. Le choix de la colonne peut être guidé par l'expérience du concepteur ou par les caractéristiques des composants disponibles susceptibles de satisfaire les critères de la colonne. Si le résultat de la conception ne peut aboutir, il peut être nécessaire de procéder par itération et de choisir une autre colonne du même tableau.

Note : Les plages de $MTTF_d$ par canal et de DC annoncées dans ces tableaux sont extraites de la norme et exprimées de manière à en faciliter l'exploitation. En effet, la norme annonce des valeurs minimales à respecter. Si les résultats des calculs de $MTTF_d$ ou de DC_{avg} sont supérieurs à ces valeurs préconisées, ils conviennent également, ce qui apparaît clairement dans les tableaux.

Rappel des plages de valeurs définies dans la norme : $MTTF_d$ par canal (Tableau 5) et DC (Tableau 6)

$MTTF_d$ (par canal)
$MTTF_d$ faible : 3 ans ≤ $MTTF_d$ < 10 ans
$MTTF_d$ moyen : 10 ans ≤ $MTTF_d$ < 30 ans
$MTTF_d$ élevé : 30 ans ≤ $MTTF_d$ ≤ 100 ans

DC
Nulle : DC < 60 %
Faible : 60 % ≤ DC < 90 %
Moyenne : 90 % ≤ DC < 99 %
Elevée : 99 % ≤ DC

Réflexions sur les critères de respect de la catégorie 2
(Si utilisation de la procédure simplifiée de calcul du $MTTF_d$)

Pour le respect de la catégorie 2, la norme exige notamment que le taux d'essais de la partie considérée soit au moins 100 fois supérieur à son taux de demande (§ 3.1.30 de la norme - fréquence de sollicitation d'une action relative à la sécurité d'une SRP/CS).

En pratique, cette exigence élimine de manière quasi systématique la possibilité d'utiliser des composants électromécaniques, pneumatiques ou hydrauliques. En effet, pour que le diagnostic de ces composants puisse être effectué, il est nécessaire qu'ils commutent. Ceci a pour effet de rendre leur taux d'essais équivalent à leur taux de demande, sauf dans des cas très rares où il serait possible :

- de commander « artificiellement » (autrement que par la sollicitation de la fonction de sécurité par son élément d'entrée) une commutation des composants électromécaniques du SC/FS à un taux 100 fois supérieur à son taux de demande,
- que cette commutation, à des fins d'essais, ne perturbe pas le fonctionnement normal de la machine.

Dans le cas d'un interrupteur de position à contacts électromécaniques actionné par un protecteur, il n'y a pas de moyen de solliciter « artificiellement » l'interrupteur pour pouvoir le tester. Il n'existe donc pas de moyen pour obtenir un taux d'essais supérieur au taux de demande.

L'usage de la catégorie 2 est donc réservé principalement aux systèmes électroniques, qui peuvent tolérer des micro-impulsions de tests suffisantes pour effectuer un diagnostic fréquent, mais sans effet sur les sorties du système concerné vis-à-vis des éléments commandés.

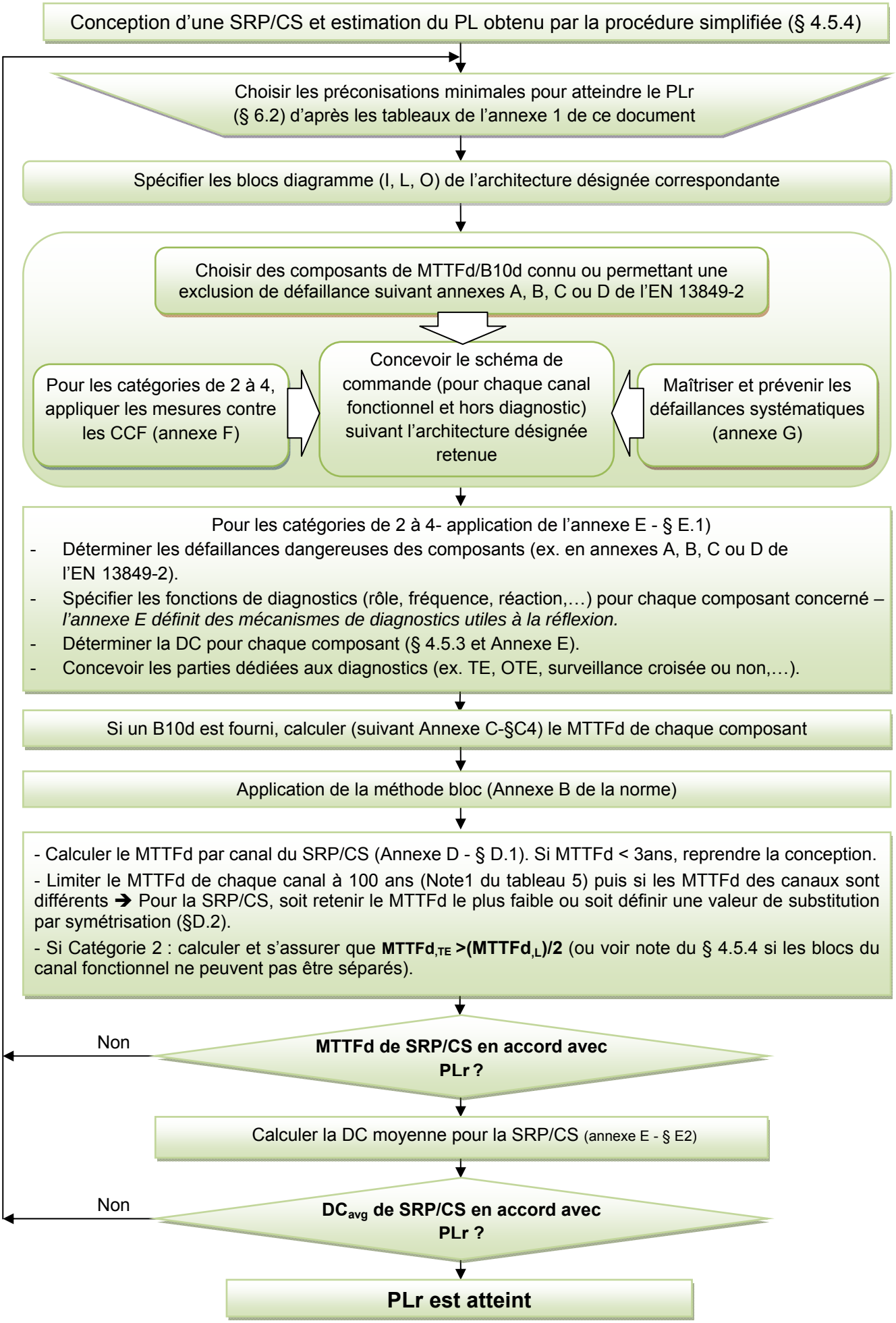
En conséquence, lorsque l'on veut développer une SRP/CS en utilisant des composants électromécaniques, pneumatiques ou hydrauliques, il est fortement déconseillé d'utiliser une architecture de catégorie 2. Il faut alors s'orienter vers une autre catégorie adaptée au PL_r.

6.3 Etapes de conception d'une SRP/CS

Afin de faciliter la conception d'une SRP/CS (hors partie logicielle) en utilisant la méthode simplifiée de la norme, le Graphe 2 a été conçu.

Rappel : la méthode simplifiée se base sur des architectures désignées pour lesquelles des "pré-calculs" ont été réalisés, facilitant d'autant l'application des exigences quantitatives requises par la norme.

Le graphe proposé liste, en les classant, les étapes à suivre et indique les différents paragraphes ou annexes de la norme NF EN ISO 13849-1 auxquels il faut se référer.



Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

6.4 Exigences pour la prise en compte des défaillances systématiques

Rappel : *défaillance systématique (§ 3.1.7 de la norme)*

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.

Beaucoup de concepteurs négligent la prise en compte des défaillances systématiques au profit des autres paramètres plus facilement chiffrables, tels que les $MTTF_d$. Or, sans mesures adaptées pour pallier ces défaillances, un système de commande ne pourra pas atteindre un niveau de sûreté de fonctionnement correct. Que penser en effet d'un système de commande relatif à la sécurité dont le comportement serait affecté par une simple mise à la masse accidentelle d'une de ses parties ?

Ces exigences s'adressent principalement aux circuits de commande électriques, mais lorsque des énergies hydrauliques ou pneumatiques sont utilisées, les mêmes objectifs de conception, maintien ou mise en état sûr d'une machine, doivent être atteints en mettant en œuvre des mesures appropriées.

Dans le cadre de l'exemple de conception d'une SC/FS traité dans ce document, les mesures à mettre en œuvre pour cet exemple ainsi qu'un rappel des préconisations de la norme sont fournies sous forme d'un tableau (voir Tableau 20). Ces mesures sont basées :

- soit sur les « principes de sécurité de base » et les « principes de sécurité éprouvés » des tableaux A1 et A2, B1 et B2, C1 et C2 ou D1 et D2 des annexes A, B, C et D de la norme ISO 13849-2, suivant les technologies mises en œuvre,
- soit sur l'état de l'art couramment rencontré dans l'industrie.

Lorsqu'une SRP/CS est constituée de plusieurs parties (par exemple, une entrée « I », une logique « L » et une sortie « O »), il faut considérer les exigences pour chacune des parties.

6.5 Exigences pour l'évaluation des mesures contre les défaillances de cause commune (CCF)

Rappel : *défaillance de cause commune CCF (§ 3.1.6 de la norme)*

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

Note : Comme indiqué dans les § 6.2.5 à 6.2.7 de la norme, la prise en compte des défaillances de cause communes CCF doit être effective lors de la conception des SRP/CS répondant aux prescriptions des catégories 2 à 4.

Pour les catégories 3 et 4, les mesures mises en œuvre sont destinées à éviter qu'une défaillance affecte simultanément les deux canaux fonctionnels.

Pour la catégorie 2, ces mesures sont destinées à éviter qu'une défaillance affecte simultanément le canal fonctionnel et le canal d'essai.

Les mesures à appliquer, préconisées dans l'annexe F de la norme NF EN ISO 13849-1 sont directement exploitables. Lorsqu'une SRP/CS est constituée de plusieurs parties (par exemple, une entrée « I », une logique « L » et une sortie « O »), il faut allouer un score global prenant en compte les mesures appliquées à chacune des parties.

Note : Il n'y a pas de calcul du score au prorata de l'application des exigences. Pour chaque exigence, le score maximal pouvant être revendiqué est appliqué si l'exigence est couverte **en totalité pour l'ensemble des parties constituant la SRP/CS**. Dans le cas contraire, le score appliqué est nul.

Dans l'exemple illustré au Tableau 1 (SRP/CS comportant une entrée, une logique et une sortie), on peut noter que :

- pour l'exigence n° 3.1, les mesures préconisées sont satisfaites pour les trois parties (I, L et O) constituant la SRP/CS. Le score alloué à cette exigence (15) est atteint,
- pour l'exigence n° 3.2, les mesures préconisées sont satisfaites uniquement pour deux (I et L) des trois parties constituant la SRP/CS. Le score alloué à cette exigence (5) n'est pas atteint.

Tableau 1 : Exemple de notation des mesures contre les CCF

N°	Notation des mesures contre les CCF (annexe F – Informative - de la norme)			
	Entrée (Input « I ») – Logique (« L ») – Sortie (Output « O ») =>	I	L	O
3	**Conception/application/expérience**			
3.1	*Protection contre surtension, surpression, surintensité, etc* **– Score atteint**	**15**		
	Fusible pour la partie électrique	**X**		
	Fusible pour la partie électrique		**X**	
	Limiteur de pression pour la partie hydraulique			**X**
3.2	*Utilisation de composants éprouvés* **– Score non atteint**	**0**		
	Composant éprouvé car usage de manœuvre positive d'ouverture	**X**		
	Composant éprouvé (contacteurs choisis et installés en respect du tableau D3 - EN13849-2)		**X**	
	Composant hydraulique non éprouvé (pas défini dans l'annexe C - EN13849-2)			**N**

Score total	Mesures pour éviter les CCF[a]
65 ou mieux	Satisfait les exigences
Moins de 65	Échec du procédé → choisir des mesures supplémentaires

[a] Lorsque des dispositions techniques ne sont pas pertinentes, les points détaillés dans la colonne de droite peuvent être considérés comme un calcul complet.

Extrait 1 : Extrait du tableau F.1 de la norme NF EN ISO 13849-1 (ancien Tableau F.2)

En application du Tableau F1 de la norme (voir **Extrait 1**), les mesures mises en œuvre pour éviter les CCF sont satisfaisantes lorsqu'un score global minimum de 65 est atteint pour une SRP/CS donnée.

6.6 Application de la « méthode bloc »

L'approche simplifiée de la norme nécessite une représentation par bloc de la SRP/CS. Cette « méthode bloc » est décrite dans l'annexe B de la norme.

La finalité de cette méthode est de permettre le calcul du $MTTF_d$ par canal et de la DC_{avg} avec les formules de la méthode simplifiée. Pour pouvoir appliquer la méthode bloc à une SRP/CS, le concepteur doit disposer du schéma de commande final prévu. Il devra identifier tous les composants dont la défaillance est potentiellement dangereuse. Chacun de ces composants constituera un bloc. La représentation sous forme de bloc doit faire apparaître clairement la séparation entre les deux canaux fonctionnels (en cas de redondance) et le canal d'essai (le cas échéant).

6.7 Couverture de diagnostic (DC) des défaillances dangereuses

Rappel : *Couverture de diagnostic DC* (§ 3.1.26 de la norme)

Mesure de l'efficacité du diagnostic, peut être définie comme la fraction de la probabilité de défaillances dangereuses détectées sur la probabilité de toutes les défaillances dangereuses

La DC est classée en quatre niveaux de pourcentage définis dans le tableau 6 de la norme. Une estimation de la DC est proposée en annexe E de la norme en fonction du type de mesures mises en œuvre pour assurer le diagnostic.

Dans la plupart des cas, cette estimation est parfaitement adaptée. Par contre, il existe des situations pour lesquelles le concepteur doit impérativement s'appuyer sur les informations du fabricant du composant mis en œuvre. C'est le cas par exemple pour l'utilisation de blocs logiques de sécurité, ou de certaines cartes d'entrée de composants de sécurité pour lesquels plusieurs modes d'utilisation sont possibles, mais avec une DC qui doit alors être déterminée pour chaque cas possible.

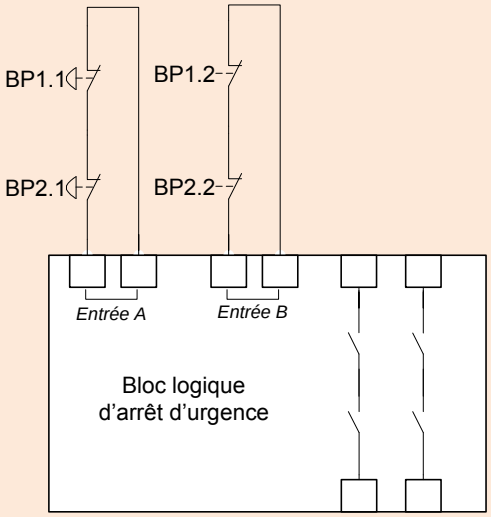
Avertissement 3

Mise en série de plusieurs entrées sur un bloc logique de sécurité

Il est important, lors de l'utilisation d'un bloc logique de sécurité, de respecter les consignes de câblage préconisées par son fabricant et de tenir compte des spécificités de l'application, notamment au niveau des possibilités de commutation simultanée des éléments raccordés en série sur les entrées.

Exemple d'évolution de la DC pour une mise en série de boutons-poussoirs sur un bloc logique de sécurité d'arrêt d'urgence pouvant atteindre un PLe :

- lorsqu'un seul bouton poussoir peut être actionné à la fois, la DC est généralement supérieure ou égale à 99 %(DC élevée),
- si plusieurs boutons d'arrêt d'urgence peuvent être actionnés simultanément, la DC se dégrade et l'atteinte d'un PLe devient alors impossible. Certains fabricants annoncent une DC de 60 % (DC faible) lors du raccordement de deux arrêts d'urgence.



Lorsque le fabricant du bloc logique prévoit la possibilité de raccorder plusieurs organes d'entrées câblés en série, il doit préciser la valeur correspondante de la DC en fonction du nombre de composants prévus en entrée.

Au-delà de deux éléments raccordés en série, il est conseillé de considérer une DC inférieure à 60 %, donc d'indice « nul ».

L'exemple 8.2.34 du document BGIA Report 2/2008e[10] stipule également en remarque qu'il n'est pas possible d'atteindre la catégorie 4 lorsque plusieurs entrées sont connectées en cascade sur un même module.

Par ailleurs, le projet de norme ISO/DIS 14119[11] aborde ce problème dans son annexe J (*Evaluation d'une connexion en série masquant les défauts de dispositifs de verrouillage avec contacts libres de potentiel*) et donne, pour le cas de câblage en série de dispositifs de verrouillage de protecteur sur un module de sécurité, un tableau récapitulatif fixant la règle à appliquer pour déterminer le DC.

[10] BGIA Report 2/2008e : Functional safety of machine controls – Application of EN ISO 13849
[11] ISO/DIS 14119 : Sécurité des machines - Dispositifs de verrouillage associés à des protecteurs - Principes de conception et de choix

Nombre de protecteurs mobiles fréquemment utilisés[a]		Nombre de protecteurs mobiles supplémentaires	Probabilité de masquage	DC pour le dispositif de verrouillage limitée à
1	+	1	faible	faible
		2 à 4	moyenne	faible
		> 4	élevée	aucune
> 1			élevée	aucune
[a] Si la fréquence est supérieure à une fois par heure.				

Extrait 2 : Tableau J.1 de la norme ISO/DIS 14119

6.8 Calcul du $MTTF_d$ pour les composants pneumatiques, mécaniques et électromécaniques (Annexe C de la norme)

Pour chaque canal de l'architecture désignée d'une SRP/CS, la valeur de $MTTF_d$ correspondante doit être calculée, à partir des valeurs de $MTTF_d$ des composants simples (unitaires) mis en œuvre. Pour les composants, pneumatiques, mécaniques et électromécaniques, les fabricants fournissent une caractéristique « B10d » qui est nécessaire pour calculer le $MTTF_d$ de ces composants. En effet, ces derniers mettant en œuvre des parties sujettes à usure mécanique, il est nécessaire de prendre en compte leurs conditions réelles d'utilisation pour l'application prévue. La méthode de calcul du $MTTF_d$ d'un tel composant est résumée dans la Figure 7.

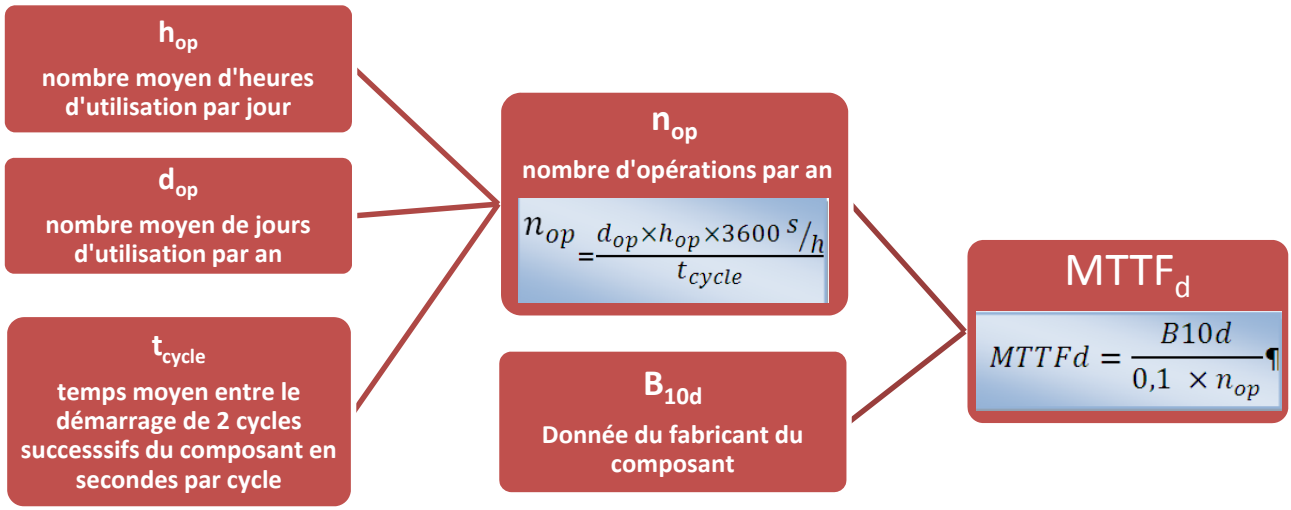


Figure 7 : Calcul du $MTTF_d$ d'un composant simple à partir de son B_{10d}

Note : t_{cycle} doit tenir compte du nombre réel de sollicitations du composant, qui peut être supérieur à la sollicitation de la fonction de sécurité. C'est le cas lorsqu'un composant est commun à plusieurs fonctions de fréquences de sollicitations différentes.

7 Combinaison de plusieurs fonctions agissant sur un même actionneur

Lorsque plusieurs fonctions de sécurité ou une (des) fonction(s) de sécurité et une (des) fonction(s) « standard » doivent intervenir sur un même actionneur pour commander son arrêt, il est nécessaire de réaliser une logique entre ces fonctions afin que chacune d'elles puisse jouer son rôle indépendamment ou simultanément en préservant, le cas échéant, la priorité des fonctions de sécurité sur les fonctions « standard ».

Dans la mise en œuvre pratique, une ou des parties d'une fonction de sécurité ou d'une fonction « standard » vont être utilisées pour faire transiter les ordres d'arrêt issus d'une ou d'autres fonctions de sécurité vers l'actionneur. Un exemple est illustré Figure 8.

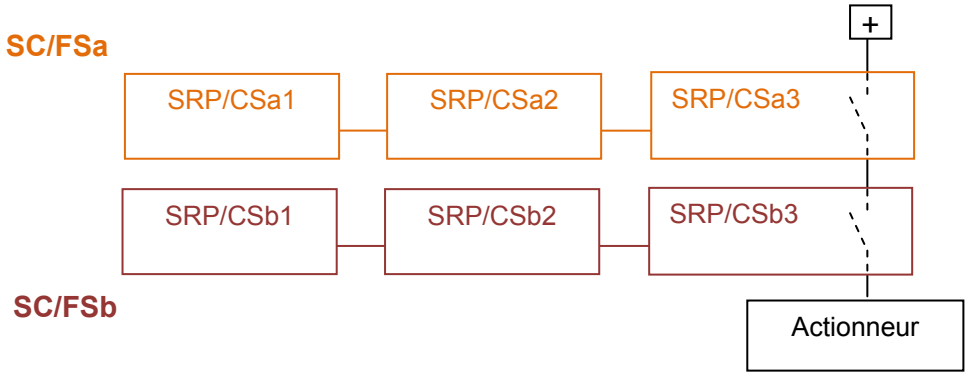


Figure 8 : Le signal de SC/FSa vers l'actionneur transite par SRP/CSb3 qui est un élément de SC/FSb

Dans cet exemple, l'ordre d'arrêt de la fonction de sécurité FSa vers l'actionneur transite par la SRP/CSb3 qui est une partie constitutive de SC/FSb. La SRP/CSb3 n'a pas de rôle fonctionnel pour la fonction FSa.

Questions :

- La fonction de sécurité FSa pourrait-elle être affectée par une défaillance de SRP/CSb3 ?
- Si oui, quelle est sa conséquence sur l'évaluation du PL de SC/FSa ?

Pour répondre à ces interrogations, il faut procéder à une analyse des modes de défaillance de la SRP/CSb3 afin de vérifier l'influence de ces défaillances par rapport au comportement de la fonction de sécurité FSa.

Etude sur deux exemples de réalisations :

1er cas – SRP/CSb3 est dotée de sorties à contact libres de potentiel

Dans ce cas, la défaillance de SRP/CSb3 n'a aucune influence sur le comportement de SC/FSa qui reste pleinement opérationnelle.

L'estimation du PL de la fonction FSa s'effectuera en prenant en compte uniquement SRP/Csa1, SRP/Csa2 et SRP/Csa3.

2ème cas – SRP/CSb3 est dotée de sorties électroniques

La Figure 9 représente le cas d'utilisation de sorties à contacts libres de potentiel pour la fonction FSa et de sorties électroniques pour FSb. La sortie de FSb (SRP/CSb3) est supposée défaillante en réinjectant de l'énergie (représentée par un trait de couleur rouge) suffisante pour maintenir alimenté l'actionneur.

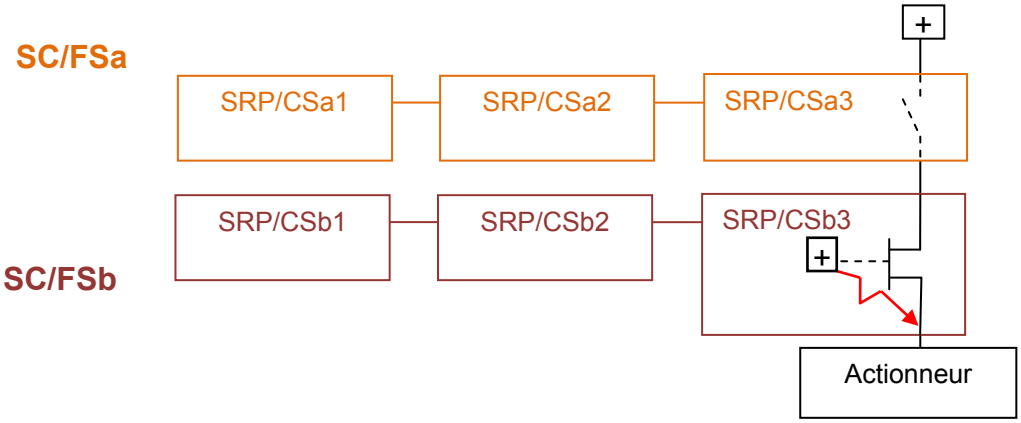


Figure 9 : Exemple de défaillance d'une sortie électronique

Cette défaillance est potentiellement dangereuse pour la fonction FSb, car sa sortie défaillante ne peut plus ordonner d'arrêt à l'actionneur. De plus, cette défaillance est potentiellement dangereuse pour la fonction FSa. L'ouverture des contacts de sortie de cette fonction devient inopérante et n'ordonne pas l'arrêt de l'actionneur.

L'estimation du PL de la fonction FSa doit alors s'effectuer en prenant en compte SRP/Csa1, SRP/Csa2, SRP/Csa3 et également SRP/CSb3.

Conclusions

Lorsque des éléments matériels (élément d'une autre fonction de sécurité ou élément d'une fonction standard) sont insérés entre un SC/FS et l'actionneur sur lequel il doit agir (ex. Figure 8), il est nécessaire d'analyser l'influence de la défaillance de ces éléments sur le SC/FS considéré.

Lorsque la défaillance de ces éléments n'a aucune influence sur le SC/FS considéré (ex : contacts libres de potentiel), ils ne seront pas pris en compte.

Lorsque la défaillance de ces éléments influe la fonction considérée, il peut être nécessaire de revoir la conception de la ou des fonctions et/ou de modifier leur emplacement au niveau de l'interconnexion. Si l'on maintient ces éléments, ils doivent être pris en compte pour l'évaluation du PL du SC/FS considéré.

Avertissement : Aucun élément d'une fonction standard dont la défaillance peut influer sur le SC/FS considéré ne doit être inséré entre ce SC/FS et son actionneur.

8 Remarques sur l'utilisation du logiciel SISTEMA

Le logiciel SISTEMA permet d'assister le concepteur dans l'application de la norme NF EN ISO 13849-1 en lui imposant de passer par les phases de conception préconisées par cette norme et en calculant les données de fiabilité demandées sans avoir à utiliser les formules de calcul.

Il offre la possibilité d'utiliser des bases de données de fiabilité des composants fournies par certains constructeurs.

Il ne traite pas explicitement des mesures à mettre en œuvre pour la prise en compte des défaillances systématiques, ce qui nécessite au concepteur de les traiter séparément en appliquant l'annexe G de la norme.

Il ne permet pas de s'affranchir de la connaissance précise de la norme, car les choix de conception restent à la charge du concepteur. Comment par exemple choisir d'utiliser une catégorie de sécurité et une architecture désignée, sans en connaître les caractéristiques ?

Par ailleurs, il ne traite pas de la partie logicielle des systèmes de commande relatifs à la sécurité.

Il nécessite une période d'adaptation, car la terminologie du logiciel est différente de celle de la norme NF EN ISO 13849-1 concernant les SRP/CS qui sont appelés SB, pour « Subsystem » et il introduit la notion

d'éléments (en tant que « sous-partie » d'un bloc) qui n'apparaît explicitement pas dans cette norme. Le découpage proposé est très proche de celui de la norme NF EN 62061.

L'utilisation du logiciel nécessite les mêmes préparations que lorsque la conception est réalisée sans l'utiliser, comme par exemples :

- spécification de la fonction de sécurité (appelée « SF »),
- spécification des SRP/CS (appelées « SB »), des composants (appelés « BL » et/ou « EL »)
- réflexion et choix de l'architecture désignée prévue,
- détermination des données de fiabilité des composants (B10d, $MTTF_d$) ou choix d'exclusion de défaillances – SISTEMA prévoit toutefois d'accéder à certaines bibliothèques de caractéristiques « constructeur » ou aux valeurs par défaut de la norme,
- spécification des mesures contre les CCF - SISTEMA affiche les mesures de l'annexe F de la norme et propose un choix parmi elles ou l'adoption d'autres mesures.
- analyse des défaillances possibles pour déterminer les parties à prendre en compte,
- spécifications des fonctions de diagnostics.

Enfin, avec ou sans SISTEMA, il reste à concevoir les schémas de commande des parties fonctionnelles et de diagnostics en respectant **strictement** les spécifications établies et les choix de conceptions annoncés.

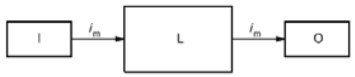
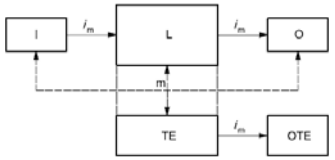
Le logiciel SISTEMA facilite les itérations de conception et permet de constituer un rapport final et comme tout outil informatique, permettra alors une traçabilité et une évolutivité des projets. Il constitue donc un outil appréciable dès lors qu'il est utilisé en complément de la norme, comme support et guide d'application de ses préconisations, et par du personnel ayant une connaissance de cette norme.

Note : Pour l'exemple de conception d'un SC/FS traité dans ce document, le résultat de PL obtenu avec SISTEMA est le même que celui obtenu en mettant en œuvre la méthode simplifiée de la norme.

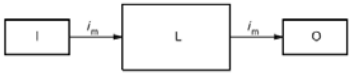
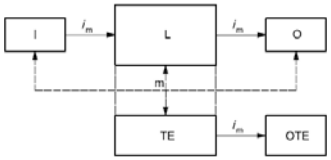
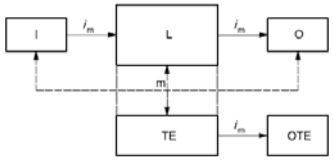
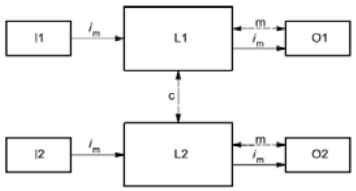
Annexe 1 : Tableaux des préconisations minimales pour un PL donné

Préconisations minimales pour atteindre un PL « a » – Suivant tableau 7 et pour utilisation de la procédure simplifiée

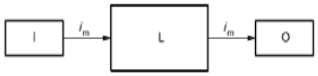
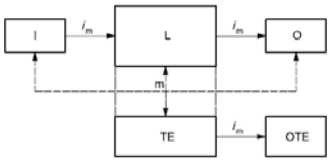
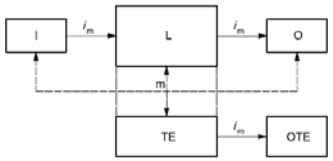
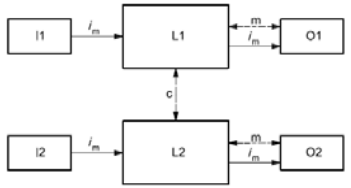
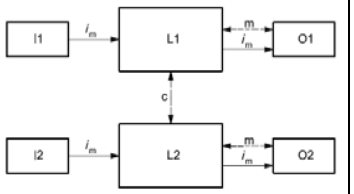
Dans les tableaux suivants, les références (tableau, §, annexe) citées renvoient à la norme EN ISO 13849-1

Catégories autorisées	**Cat B** *§ 6.2.3*	**Cat 2** *§ 6.2.5*
Respect autre catégorie		Respect exigences de Cat B
$MTTF_d$ par canal fonct. ***§ 4.5.2***	3 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ ≥ « Faible »)	3 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ ≥ « Faible »)
DC_{avg} mini ***§ 4.5.3 et Annexe E***	DC_{avg} ≥ 0 (DC_{avg} ≥ « Nulle »)	DC_{avg} ≥ 60% (donc DC_{avg} ≥ « Faible »)
CCF ***Annexe F***	Sans objet	Score ≥ 65
Spécificités	Composants aptes à la fonction	- Composants et principes de sécurité éprouvés (§ 6.2.4) - $MTTF_{d,TE}$ à considérer (§ 4.5.4)
Contrôle des fonctions - périodicité	Sans objet	Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais
Contrôle des fonctions - réaction	Sans objet	Si défaut détecté : Conduire à état sûr (arrêt) ou avertissement de danger
Architecture désignée		
Fautes systématiques	Annexe G	Annexe G

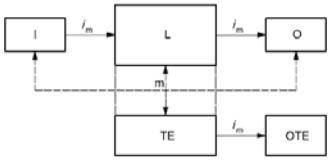
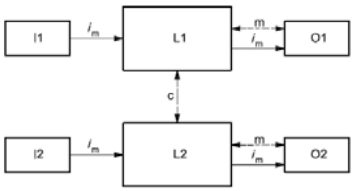
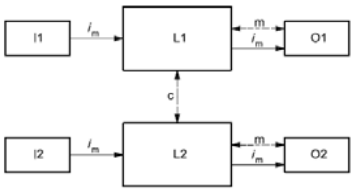
Préconisations minimales pour atteindre un PL « b » – Suivant tableau 7 et pour utilisation de la procédure simplifiée

Catégories autorisées	**Cat B** *§ 6.2.3*	**Cat 2** *§ 6.2.5*	**Cat 2** *§ 6.2.5*	**Cat 3** *§ 6.2.6*
Respect autre catégorie		Respect exigences de Cat B	Respect exigences de Cat B	Respect exigences de Cat B
$MTTF_d$ par canal fonct. ***§ 4.5.2***	10 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ ≥ « Moyen »)	10 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ ≥ « Moyen »)	3 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ ≥ « Faible »)	3 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ ≥ « Faible »)
DC_{avg} mini ***§ 4.5.3 et Annexe E***	DC_{avg} ≥ 0 (DC_{avg} ≥ « Nulle »)	DC_{avg} ≥ 60 % (donc DC_{avg} ≥ « Faible »)	DC_{avg} ≥ 90 % (donc DC_{avg} ≥ « Moyenne »)	DC_{avg} ≥ 60 % (donc DC_{avg} ≥ « Faible »)
CCF ***Annexe F***	Sans objet	Score ≥ 65	Score ≥ 65	Score ≥ 65
Spécificités	Composants aptes à la fonction	- Composants et principes de sécurité éprouvés (§ 6.2.4) - $MTTF_{d,TE}$ à considérer (§ 4.5.4)	- Composants et principes de sécurité éprouvés (§ 6.2.4) - $MTTF_{d,TE}$ à considérer (§ 4.5.4)	- Composant et principes de sécurité éprouvés (§ 6.2.4) - Défaut unique = état sûr
Contrôle des fonctions - périodicité	Sans objet	Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais	Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais	Si possible, dès ou avant prochaine sollicitation
Contrôle des fonctions - réaction		Si défaut détecté : Conduire à état sûr (arrêt) ou avertissement de danger	Si défaut détecté : Conduire à état sûr (arrêt) ou avertissement de danger	Si défaut détecté : Conduire à état sûr (arrêt)
Architecture désignée				
Fautes systématiques	Annexe G	Annexe G	Annexe G	Annexe G

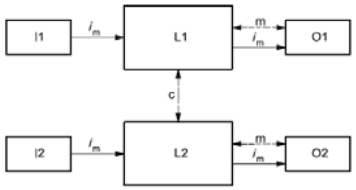
Préconisations minimales pour atteindre un PL « c » – Suivant tableau 7 et pour utilisation de la procédure simplifiée

Catégories autorisées	**Cat 1** *§ 6.2.4*	**Cat 2** *§ 6.2.5*	**Cat 2** *§ 6.2.5*	**Cat 3** *§ 6.2.6*	**Cat 3** *§ 6.2.6*
Respect autre catégorie	Respect exigences de Cat B	Respect exigences de Cat B	Respect exigences de Cat B	Respect exigences de Cat B	Respect exigences de Cat B
$MTTF_d$ par canal fonct. ***§ 4.5.2***	30 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ = « Elevé »)	30 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ = « Elevé »)	10 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ ≥ « Moyen »)	10 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ ≥ « Moyen »)	3 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF^d$ ≥ « Faible »)
DC_{avg} mini ***§ 4.5.3 et Annexe E***	DC_{avg} ≥ 0 (DC_{avg} ≥ « Nulle »)	DC_{avg} ≥ 60 % (donc DC_{avg} ≥ « Faible »)	DC_{avg} ≥ 90 % (donc DC_{avg} ≥ « Moyenne »)	DC_{avg} ≥ 60 % (donc DC_{avg} ≥ « Faible »)	DC_{avg} ≥ 90 % (donc DC_{avg} ≥ « Moyenne »)
CCF ***Annexe F***	Sans objet	Score ≥ 65	Score ≥ 65	Score ≥ 65	Score ≥ 65
Spécificités	Composant et principes de sécurité éprouvés	- Composants et principes de sécurité éprouvés (§ 6.2.4) - $MTTF_{d,TE}$ à considérer (§ 4.5.4)	- Composants et principes de sécurité éprouvés (§ 6.2.4) - $MTTF_{d,TE}$ à considérer (§ 4.5.4)	- Composant et principes de sécurité éprouvés (§ 6.2.4) - Défaut unique = état sûr	- Composant et principes de sécurité éprouvés (§ 6.2.4) - Défaut unique = état sûr
Contrôle des fonctions - périodicité	Sans objet	Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais	Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais	Si possible, dès ou avant prochaine sollicitation	Si possible, dès ou avant prochaine sollicitation
Contrôle des fonctions - réaction		Si défaut détecté : Conduire à état sûr (arrêt) ou avertissement de danger	Si défaut détecté : Conduire à état sûr (arrêt) ou avertissement de danger	Si défaut détecté : Conduire à état sûr (arrêt)	Si défaut détecté : Conduire à état sûr (arrêt)
Architecture désignée					
Fautes systématiques	Annexe G	Annexe G	Annexe G	Annexe G	Annexe G

Préconisations minimales pour atteindre un PL « d » – Suivant tableau 7 et pour utilisation de la procédure simplifiée

Catégories autorisées	**Cat 2** *§ 6.2.5*	**Cat 3** *§ 6.2.6*	**Cat 3** *§ 6.2.6*
Respect autre catégorie	Respect exigences de Cat B	Respect exigences de Cat B	Respect exigences de Cat B
$MTTF_d$ par canal fonct. ***§ 4.5.2***	30 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ = « Elevé »)	30 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ = « Elevé »)	10 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ ≥ « Moyen »)
DC_{avg} mini ***§ 4.5.3 et Annexe E***	DC_{avg} ≥ 90% (donc DC_{avg} ≥ « Moyenne »)	DC_{avg} ≥ 60 % (donc DC_{avg} ≥ « Faible »)	DC_{avg} ≥ 90 % (donc DC_{avg} ≥ « Moyenne »)
CCF ***Annexe F***	Score ≥ 65	Score ≥ 65	Score ≥ 65
Spécificités	- Composants et principes de sécurité éprouvés (§ 6.2.4) - $MTTF_{d,TE}$ à considérer (§ 4.5.4)	- Composant et principes de sécurité éprouvés (§ 6.2.4) - Défaut unique = état sûr	- Composant et principes de sécurité éprouvés (§ 6.2.4) - Défaut unique = état sûr
Contrôle des fonctions - périodicité	Démarrage machine, et périodiquement (automatique ou manuel), et taux de demande ≤ 1/100 du taux d'essais	Si possible, dès ou avant prochaine sollicitation	Si possible, dès ou avant prochaine sollicitation
Contrôle des fonctions - réaction	Si défaut détecté : Conduire à état sûr (arrêt) ou avertissement de danger	Si défaut détecté : Conduire à état sûr (arrêt)	Si défaut détecté : Conduire à état sûr (arrêt)
Architecture désignée			
Fautes systématiques	Annexe G	Annexe G	Annexe G

Préconisations minimales pour atteindre un PL « e » – Suivant tableau 7 et pour utilisation de la procédure simplifiée

Catégories autorisées	**Cat 4** *§ 6.2.7*
Respect autre catégorie	Respect exigences de Cat B
$MTTF_d$ par canal fonct. ***§ 4.5.2***	30 ans ≤ $MTTF_d$ ≤ 100 ans (donc $MTTF_d$ = « Elevé »)
DC_{avg} mini ***§ 4.5.3 et Annexe E***	DC_{avg} ≥ 99 % (donc DC_{avg} = « Elevée »)
CCF ***Annexe F***	Annexe F (CCF ≥ 65)
Spécificités	- Composant et principes de sécurité éprouvés (§ 6.2.4) - Défaut unique = état sûr
Contrôle des fonctions - périodicité	Dès ou avant prochaine sollicitation
Contrôle des fonctions - réaction	Défaut détecté : Conduire à état sûr (arrêt)
Architecture désignée	
Fautes systématiques	Annexe G

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

Cet exemple illustre la conception d'un SC/FS constitué de trois SRP/CS dont une de PL connu (branche centrale du Graphe 1 : Processus général de conception d'un SC/FS en vue d'atteindre un PL requis.

Toutes les phases de conception ont été abordées et rappelées en faisant ressortir les détails et les commentaires jugés nécessaires pour assimiler les principes préconisés par la norme et en utilisant les graphes, tableaux et conseils décrits dans la partie précédente de ce document.

Les deux SRP/CS de PL non connu sont développées en appliquant le paragraphe 6 de ce document. Pour faciliter la correspondance avec le Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis, des extraits de ce dernier sont rappelés à chaque étape de la conception.

Les itérations successives nécessaires au traitement de l'exemple ne sont pas rappelées dans ce document qui présente la version finale des phases de conception.

A1. Présentation de la fonction

Une machine comprend un élément mobile de travail dont le mouvement est animé en rotation par un moteur hydraulique. Le risque est lié au mouvement de rotation (horaire et anti horaire) de l'outil. Un protecteur mobile a été choisi pour couvrir les accès à l'élément mobile de travail.

La fonction de sécurité consiste à arrêter ce mouvement de rotation lorsque le protecteur mobile est ouvert.

Dans cet exemple, la détermination du niveau de performance requis (PL_r) n'est pas abordé (voir Annexe A de la norme). Les hypothèses de départ sont : **PL_r « d » et utilisation de la catégorie « 3 »**

Le choix est fait d'utiliser un module de sécurité pour assurer la partie traitement de la fonction de sécurité.

Dans un souci de simplification des exemples, le système d'actionnement du dispositif de verrouillage du protecteur mobile et le moteur hydraulique n'ont pas été considérés.

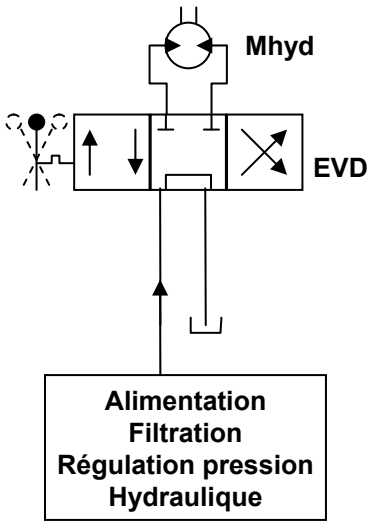


Figure 10 : Schéma hydraulique de base

A2. Spécification de la fonction de sécurité

Spécification des exigences fonctionnelles de la fonction de sécurité	
N°	**Nom de la fonction** Arrêt du moteur hydraulique par protecteur
Niveau de performance requis (suite à l'estimation des risques)	PL « d »
Conditions d'activation de la fonction	Cette fonction est active en permanence
Interface du SC/FS	Entrée : - Actionneur du dispositif de verrouillage du protecteur (ex. came d'actionnement). Sortie : - Les 2 orifices de commande du moteur hydraulique.
Description de la fonction	Cette fonction consiste à arrêter et empêcher le mouvement de rotation si le protecteur est ouvert et, si le protecteur est fermé, à autoriser le mouvement de rotation par la logique de commande de la machine.
Priorité par rapport à d'autres fonctions simultanées	Cette fonction de sécurité doit être prioritaire sur le mouvement de rotation (horaire et anti horaire) issu de la logique de commande de la machine (EVD).
Autres SC/FS agissant sur le même actionneur	Sans objet
Temps de réaction maximal du SC/FS	Le temps de réaction maximal compris entre l'information d'entrée et la sortie ne doit pas dépasser 80 ms.
Taux de demande de la fonction	La fréquence d'ouverture du protecteur est estimée à 10 fois par heure par période de 8 h à raison de 220 j/an.
Réaction aux fautes/Conditions de redémarrage	La réaction en cas de défaut doit conduire à arrêter et empêcher le mouvement de rotation de l'outil. L'autorisation de redémarrage peut avoir lieu après disparition du défaut.
Conditions d'ambiance	Degré de protection minimal compte tenu de l'environnement prévisible : IP 65

Tableau 2 : Spécification des exigences fonctionnelles de la fonction de sécurité

A3. Structure logique de base

A partir de la spécification des exigences fonctionnelles de la fonction « Arrêt du moteur hydraulique par protecteur » Tableau 2, le concepteur prévoit une structure logique représentée Figure 11, en s'appuyant sur sa culture en conception de machines identiques et sur sa connaissance des composants couramment utilisés dans ce domaine. Cette tâche peut s'effectuer sans a priori sur le matériel envisagé, mais souvent, le concepteur a déjà, par expérience, une idée sur le type de matériel qu'il compte utiliser. Par exemple, dans le cas de cette fonction d'arrêt, l'état de l'art est d'utiliser au moins un module de sécurité du commerce pour faciliter la phase de conception et de mise en œuvre.

Pour cette fonction, le concepteur prévoit :

- Une partie « entrée » qui sera constituée d'un dispositif de verrouillage composé d'interrupteur(s) de position.
- Une partie « traitement », qui sera constituée d'un « module de sécurité ». Ce type de composant permettra de réaliser l'interface entre le dispositif de verrouillage d'entrée et la partie hydraulique de sortie. L'offre du marché étant large en matière de modules de sécurité, il est souvent intéressant de choisir cette option pour s'affranchir du développement d'une SRP/CS. Ce type de composant facilitera la tâche du concepteur pour effectuer les éventuels diagnostics et/ou redondances à réaliser.
- Une partie « sortie », de technologie forcément hydraulique pour servir d'interface avec le moteur hydraulique, qui sera constituée de distributeur(s) hydraulique(s) à commande électrique pour être compatible avec la logique de commande de la machine. Cette partie sera utilisée pour assurer la priorité du SC/FS par rapport à la logique standard de commande du moteur constituée par EVD.
  En intercalant physiquement cette partie entre la partie standard et le moteur hydraulique, on est assuré que le SC/FS assurera toujours sa fonction quels que soient les ordres induits ou les défaillances de la partie standard (EVD).

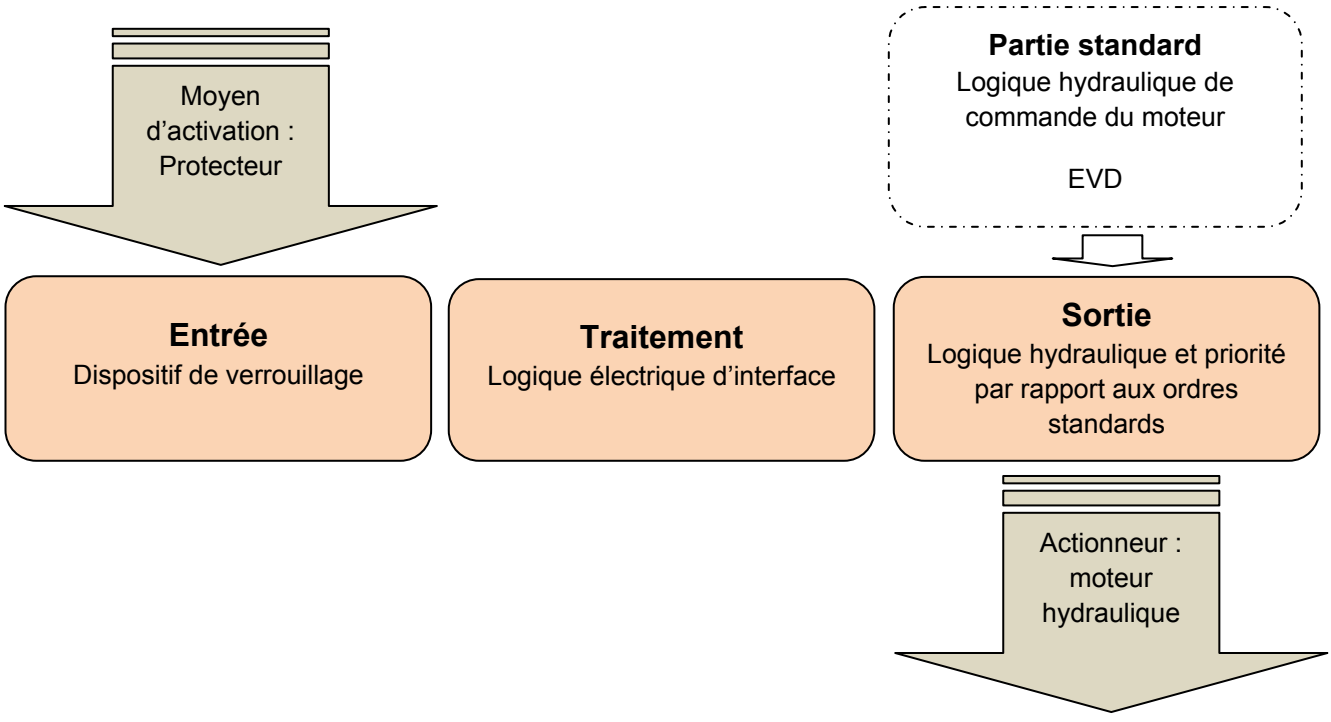


Figure 11 : Structure logique de base pour le SC/FS

A4. Définition des SRP/CS nécessaires pour la réalisation du SC/FS « arrêt du moteur hydraulique par protecteur »

Compte tenu de la structure logique envisagée pour le SC/FS dans le § A3, le concepteur applique la branche centrale du Graphe 1 : Processus général de conception d'un SC/FS en vue d'atteindre un PL requis, qui consiste à réaliser le SC/FS en associant une partie logique de PL connu, ici un module de sécurité du commerce pour la partie « traitement », avec des parties de sa propre conception pour l'entrée et la sortie. Il envisagera donc de travailler sur la base d'une SRP/CS pour chaque entité de la structure logique de base du SC/FS.

Le choix de conception pour ce SC/FS est représenté Figure 12

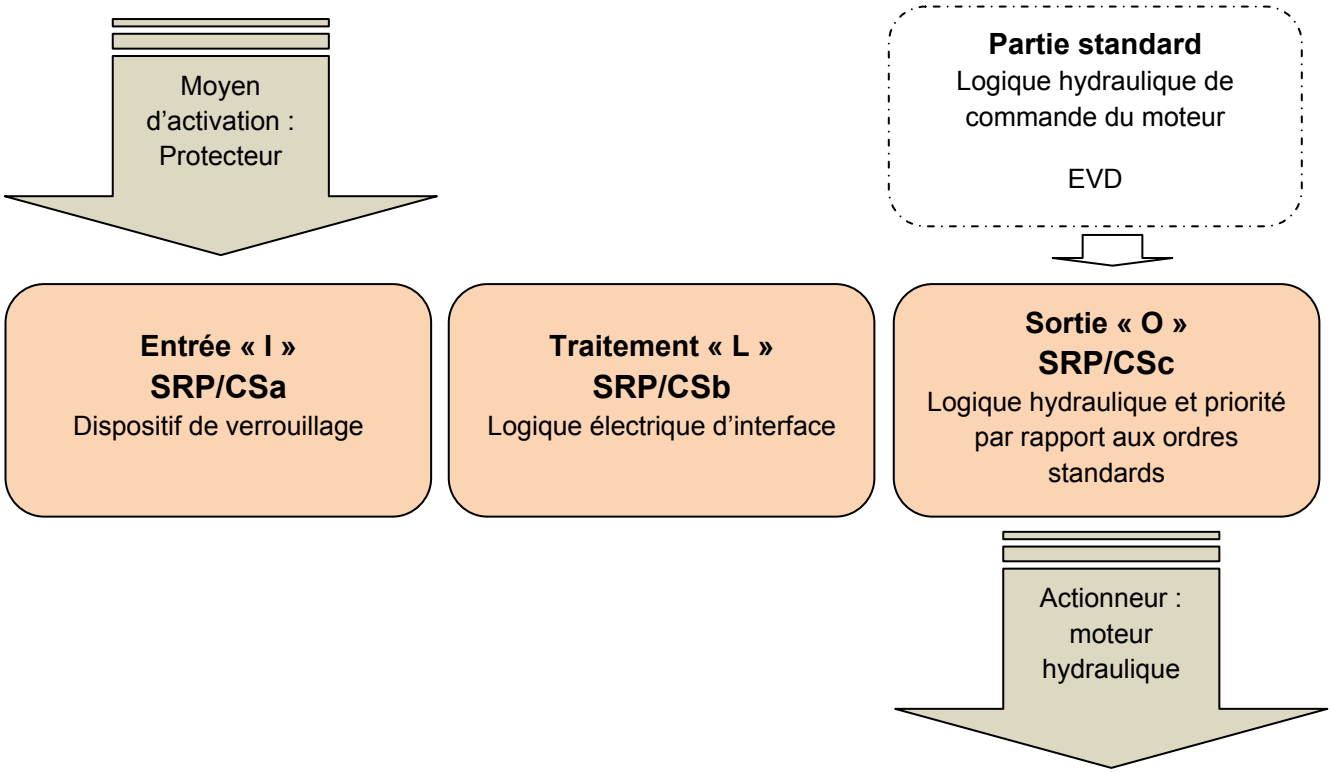
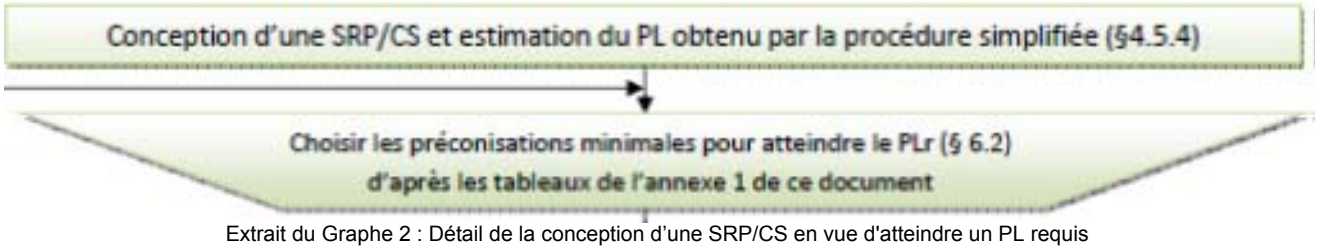


Figure 12 : Choix de conception pour le SC/FS

Note : Compte tenu du fait que le SC/FS compte 3 SRP/CS, chaque SRP/CS devra atteindre un PL supérieur ou égal au PLd requis pour le SC/FS (cf. Avertissement 2).

A5. Conception des SRP/CS

A5.1 Conception de la SRP/CSa



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

La SRP/CSa doit être conçue pour atteindre au moins un PL « d » en respectant les critères correspondants, synthétisés dans le Tableau 3 (extrait de l'annexe 1 de ce document). Le concepteur choisit de débuter son processus en retenant la catégorie 3.

nisations minimum pour un PL « d » – Suivant ta 7 et pour utilisat la procédure s

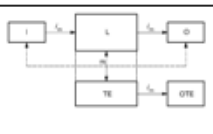
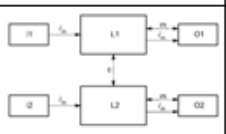
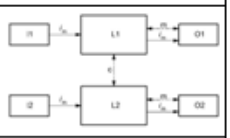
Catégories autorisées	Cat 2 § 6.2.5	Cat 3 § 6.2.6	Cat 3 § 6.2.6
Respect autre catégorie	Respect exigences de Cat B	Respect exigences de Cat B	Respect exigences de Cat B
MTTFd par canal fonct. §4.5.2	30ans ≤ MTTFd ≤ 100 ans (donc MTTFd = « Elevé »)	30ans ≤ MTTFd ≤ 100 ans (donc MTTFd = « Elevé »)	10ans ≤ MTTFd ≤ 100 ans (donc MTTFd ≥ « moyen »)
DC_{avg} mini §4.5.3 et Annexe E	UC_{avg} ≥ 90% (donc DC_{avg} ≥ « Moyenne »)	UC_{avg} ≥ 60% (donc DC_{avg} ≥ « Faible »)	UC_{avg} ≥ 90% (donc DC_{avg} ≥ « Moyenne »)
CCF Annexe F	score ≥ 65	score ≥ 65	score ≥ 65
Spécificités	- Composants et principes de sécurité éprouvés (§ 6.2.4) - $MTTF_{d\,cp}$ à considérer (§ 4.5.4)	- Composant et principes de sécurité éprouvés (§ 6.2.4) - Défaut unique = état sûr	- Composant et principes de sécurité éprouvés (§ 6.2.4) - Défaut unique = état sûr
Contrôle des fonctions - périodicité	Démarrage machine, et périodiquement (automatique ou manuel), et Taux de demande ≤ 1/100 du taux d'essais	Si possible, dès ou avant prochaine sollicitation	Si possible, dès ou avant prochaine sollicitation
Contrôle des fonctions - réaction	Si défaut détecté : Conduire à état sûr (arrêt) Ou avertissement de danger	Si défaut détecté : Conduire à état sûr (arrêt)	Si défaut détecté : Conduire à état sûr (arrêt)
Architecture désignée			
fautes systématiques	Annexe G	Annexe G	Annexe G

Tableau 3 : Préconisations minimales pour atteindre un PL « d »

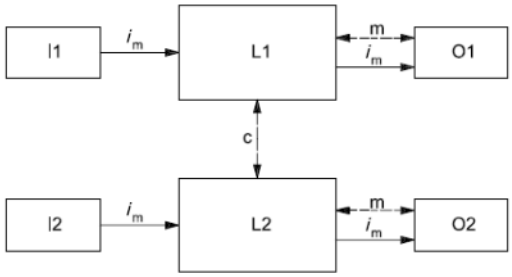
Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

La spécification de la SRP/CSa est déduite de celle de la SC/FS (Tableau 2).

Spécification de la SRP/CS Entrée	
	Nom : SRP/CSa
Conditions d'activation	Active en permanence
Interface	Entrée : - Actionneur du dispositif de verrouillage du protecteur (ex. came d'actionnement). Sortie : - 2 signaux électriques, chacun représentatif de l'état du protecteur fermé ou non fermé, fournis aux bornes du dispositif de verrouillage.
Moyens d'interconnexion (i_{ab})	Entre SPR/CSa et SPR/CSb : câbles électriques soumis aux contraintes environnementales extérieures au coffret électrique.
Description	Cette SRP/CS est conçue en deux canaux compte tenu du fait que la catégorie 3 est visée. Chaque canal génère en sortie un état logique « 0 » lorsque le protecteur est non fermé, et un état logique « 1 » lorsque le protecteur est fermé.
Priorités	Sans objet
Temps de réaction maximal	La somme des temps des SPR/CS ne doit pas dépasser le temps de réaction maximal spécifié pour le SC/FS (80 ms).
Taux de demande	La fréquence d'ouverture du protecteur est estimée à 10 fois par heure par période de 8 h à raison de 220 j/an.
Conditions d'ambiance	Degré de protection minimal IP 65

Tableau 4 : Spécification de la SRP/CSa

L'architecture retenue comme base de conception est celle de la figure 11 de la norme (voir Extrait 3)



Les traits interrompus représentent la détection de défaut raisonnablement praticable.

Légende

i_m	moyens de connexion
c	surveillance croisée
I1, I2	dispositifs d'entrée, par exemple détecteur
L1, L2	logique
m	surveillance
O1, O2	dispositifs de sortie, par exemple contacteur principal

Figure 11 — Architecture désignée pour la catégorie 3

Extrait 3 : Figure 11 de la norme NF EN ISO 13849-1

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

Mise en œuvre de l'architecture retenue.

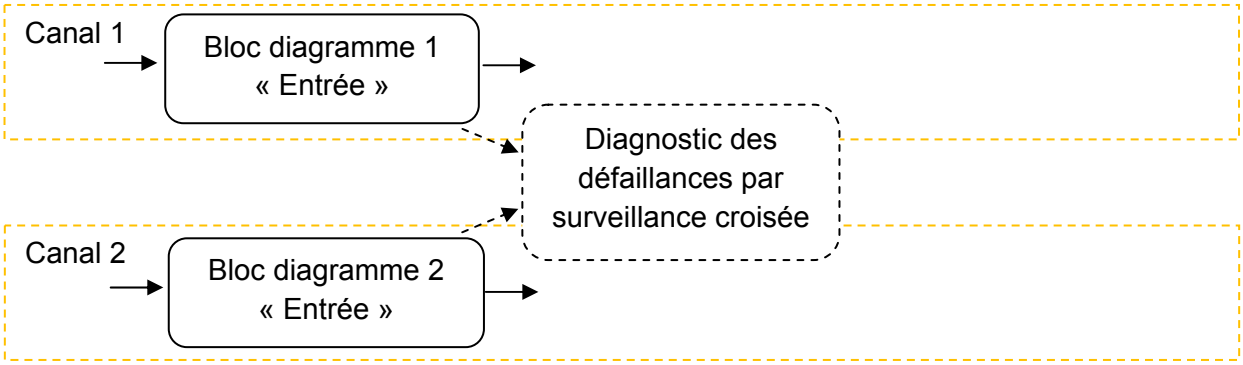
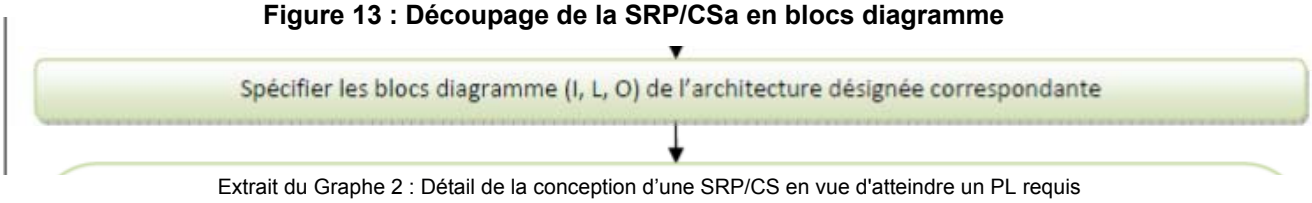
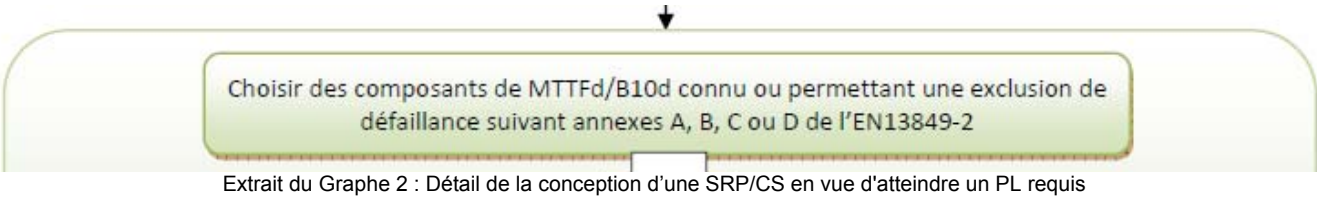


Figure 13 : Découpage de la SRP/CSa en blocs diagramme



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Chaque bloc assure unitairement l'intégralité de la fonction de chacun des canaux décrits dans la spécification de la SRP/CSa. Il n'y a donc pas lieu de re-spécifier à nouveau chacun des blocs, il suffit de reprendre les éléments de la spécification de la SRP/CSa.



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Choix du matériel pour le bloc diagramme 1

Le choix suivant est effectué (voir Figure 14) :

Interrupteur de position électromécanique « S1 » à galet avec 1 contact de type « O » à action directe d'ouverture (conforme à l'EN60947-5-1).

Il sera actionné suivant le mode positif et monté suivant les préconisations de son fabricant.

Pour le composant choisi, le temps de réponse est nul.

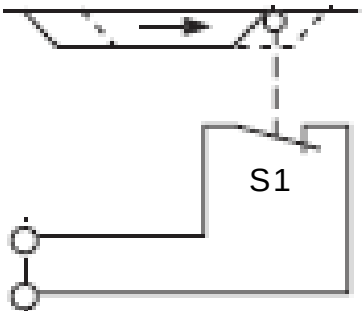


Figure 14 : Interrupteur S1
(représentation protecteur fermé)

Choix du matériel pour le bloc diagramme 2

Le choix suivant est effectué (voir Figure 15) :

Interrupteur de position électromécanique « S2 » à galet avec 1 contact de type « F ».

Il sera monté suivant les préconisations de son fabricant.

Pour le composant choisi, le temps de réponse est nul.

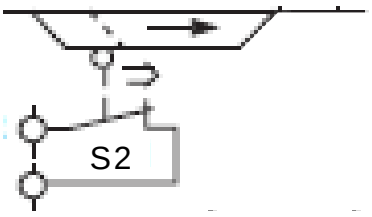
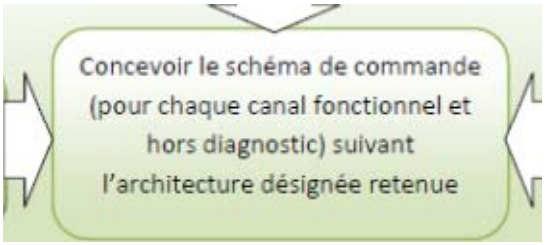


Figure 15 : Interrupteur S2
(représentation protecteur fermé)

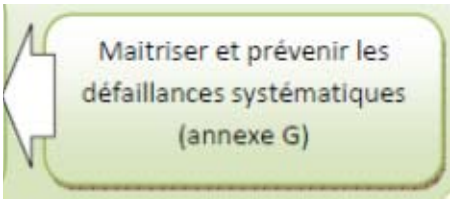
Conception du canal fonctionnel suivant l'architecture désignée de catégorie 3 retenue pour la SRP/CS



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

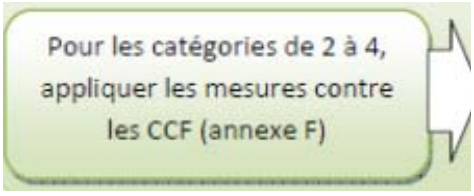
Les canaux 1 et 2 sont respectivement constitués de « **S1** » et « **S2** ».

Défaillances systématiques (Voir annexe A de ce document)



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Mesures prévues contre les CCF et notation (voir Tableau 5)



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

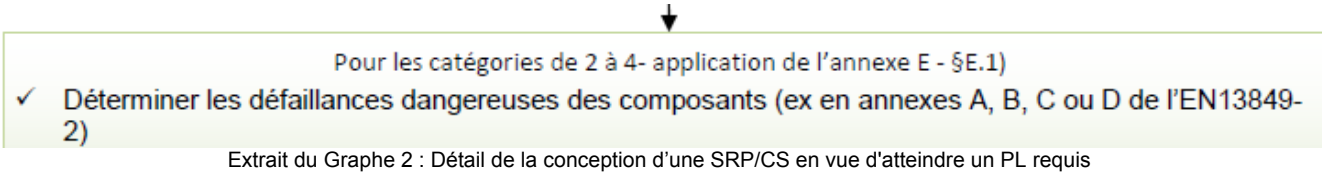
Tableau 5 : Notation des mesures contre les CCF pour la SRP/CSa

N°	Notation des mesures contre les CCF (annexe F – Informative - de la norme)	
1	**Séparation/Isolement**	
	Séparation physique entre les voies de signaux **– Score atteint**	***15***
	Séparation par mise en œuvre d'un câble propre à chacun des interrupteurs de position	***x***
2	**Diversité**	
	Différents principes de conception/technologies ou physiques sont utilisés **– Score atteint**	***20***
	Principe d'actionnement différent pour les interrupteurs	***x***
3	**Conception/application/expérience**	
3.1	Protection contre surtension, surpression, surintensité, etc. **– Score atteint**	***15***
	Défaut des entrées pris en compte par le module	***x***
3.2	Utilisation de composants éprouvés **– Score non atteint**	***0***
	Pas de mise en œuvre de composant éprouvé	**N**
4	**Appréciation /analyse**	
	Analyse et prise en compte des modes de défaillance et de leurs effets pour prévenir les CCF à la conception **– Score atteint**	***5***

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

N°	Notation des mesures contre les CCF (annexe F – Informative - de la norme)	
	Pour les interrupteurs : cause commune mécanique inexistante (principes d'actionnement différents par des cames inverses) – composants séparés	***x***
5	**Compétence/formation**	
	Score atteint	***5***
6	**Environnement**	
6.1	Prévention de la contamination et de la CEM contre les CCF **– Score atteint**	***25***
	Electromécanique non sensible à CEM	***x***
6.2	Autres influences **– Score atteint**	***10***
	Exigences environnementales prise en compte dans les choix des interrupteurs (vibrations, humidité, température, choc) suivant les contraintes de l'application	***x***
	Score total	***95***
Le score total est ≥ 65 : Les mesures mises en œuvre satisfont les exigences		

Analyse des modes de défaillance de chacun des canaux et de leurs conséquences



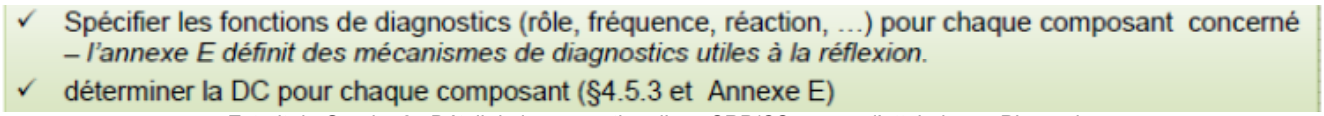
Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Composant	Type de défaillance retenu	Conséquence	Conclusion sur la potentialité du danger résultant (pour la SRP/CS) mouvement dangereux : **D** mouvement non dangereux : **ND**
Interrupteur **S1**	Soudure du contact de type « O »	Contact ne s'ouvre pas	D
	Rupture du contact de type « O »	Contact ouvert	ND
	Système d'actionnement bloqué « actionné »	Contact ouvert	ND
	Système d'actionnement bloqué « non actionné » ou rupture	Contact ne s'ouvre pas	D
Interrupteur **S2**	Soudure du contact de type « F »	Contact ne s'ouvre pas	D
	Rupture du contact de type « F »	Contact ouvert	ND
	Système d'actionnement bloqué « actionné »	Contact ne s'ouvre pas	D
	Système d'actionnement bloqué « non actionné » ou rupture	Contact ouvert	ND

Tableau 6 : Analyse des modes de défaillance des composants de la SRP/CSa

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

Spécification des diagnostics et détermination du DC



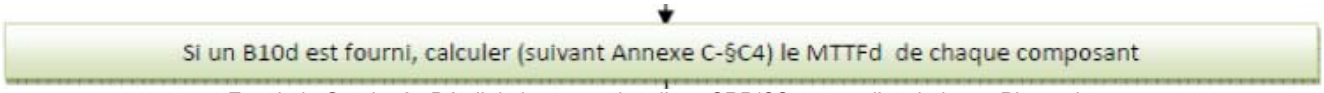
Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Composant et rappel des défauts potentiellement dangereux	**Diagnostic prévu** (en se basant sur l'annexe E de la norme)	**DC de chaque composant** (d'après annexe E de la norme)
Interrupteur « **S1** » ou « **S2** » Défaillance prise en compte : Contact ne s'ouvre pas	***Entrée*** *- Surveillance croisée des entrées sans test dynamique*	99 % (voir note)
Note : Valeur retenue compte tenu que tous les défauts potentiellement dangereux sont détectés et que la fréquence de diagnostic est jugée importante (essais effectués systématiquement à chaque ouverture du protecteur, soit 10 fois par heure par période de 8 h à raison de 220 j/an)		

Tableau 7 : Mesures mises en œuvre pour les diagnostics et estimation de la DC

Composant	**Spécification et taux d'essais**
Interrupteur « **S1** » et « **S2** »	La surveillance croisée des 2 interrupteurs est effectuée systématiquement à chaque ouverture du protecteur, par la SRP/CSb (module).

Tableau 8 : Spécification de la fonction de diagnostic de la SRP/CSa



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Détermination du $MTTF_d$ des composants uniques

Le calcul du $MTTF_d$ de chaque composant est effectué en appliquant la formule de la Figure 7 page 19

Rappel : La fréquence d'ouverture du protecteur est estimée à 10 fois par heure par période de 8 h à raison de 220 j/an - fréquence de sollicitation = 10 fois par heure (3 600sec), d'où t_{cycle} = 3 600/10 = 360 s

Composant	**h_{op} (h)**	**d_{op}**	**n_{op} calculé**	**t_{cycle} (s)**	**B_{10d} constructeur**	**B_{10d} par défaut** (annexe C de la norme)	**$MTTF_d$ calculé (ans)**	**$MTTF_d$ constructeur (ans)**	**$MTTF_d$ par défaut** (annexe C de la norme) **(ans)**
S1	8	220	17600	360	50 000 000	/	28409		
S2	8	220	17600	360	50 000 000	/	28409		

Tableau 9 : Détermination du $MTTF_d$ de chaque composant de la SRP/CSa

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

Application de la « méthode bloc »

Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Dans le cas présent (Figure 16), chaque canal est constitué d'un composant unique

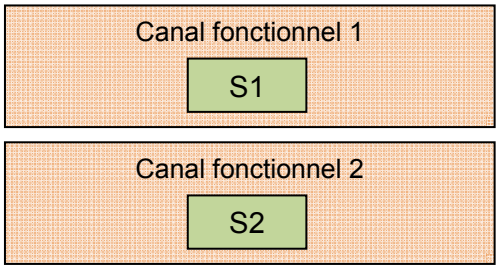
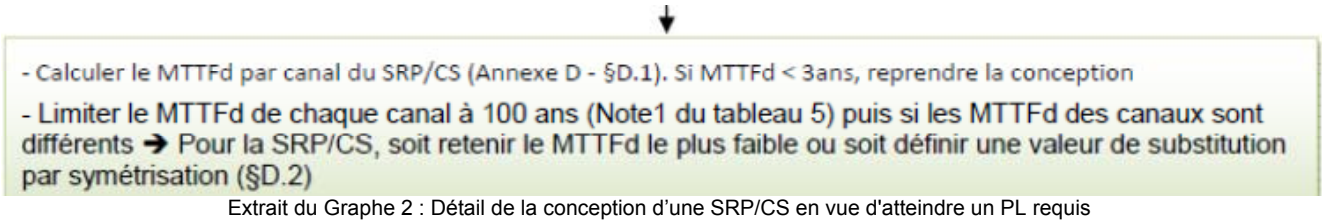
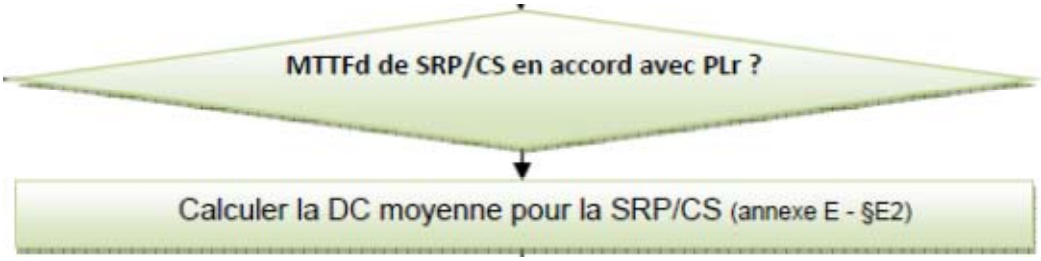


Figure 16 : Schéma identifiant les parties relatives à la sécurité de la SRP/CSa



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

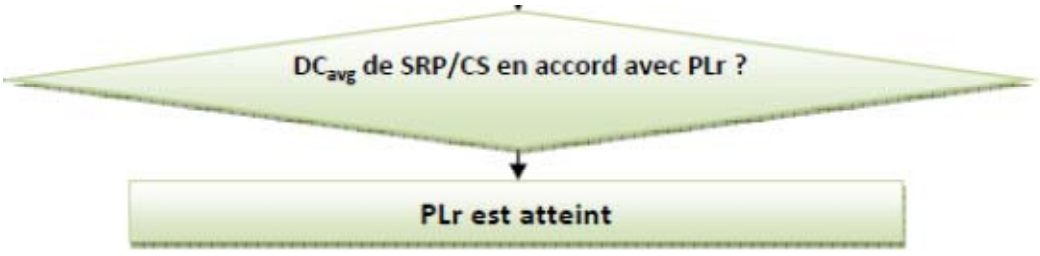
Pour chaque canal : le calcul donne $MTTF_d$ = 28409 ans, limité à 100 ans (Note 1 tableau 5 de la norme).
Pour la SRP/CSa, les deux canaux étant symétriques, **le $MTTF_d$ par canal est égal à 100 ans**.
$MTTF_d$ élevé qui répond au PLd requis.



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Les DC de S1 et S2 sont de 99 %, les $MTTF_d$ de S1 et S2 sont de 100 ans, donc le calcul donne :

$$DC_{avg} = \frac{\frac{DCS1}{MTTFdS1} + \frac{DCS2}{MTTFdS2}}{\frac{1}{MTTFdS1} + \frac{1}{MTTFdS2}}$$ **= 99 % soit DC_{avg} élevée qui répond au PLd requis.**



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

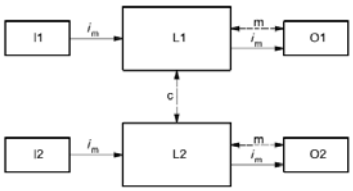
<table>
<tr><th colspan="4">Tableau récapitulatif SRP/CSa</th></tr>
<tr><th>Données</th><th colspan="2">Exigences requises</th><th>Résultats obtenus</th></tr>
<tr><td rowspan="8">Exigences pour un PLd avec usage de la catégorie 3</td><td colspan="2">Respect exigences de Cat B</td><td>OK</td></tr>
<tr><td>30 ans ≤ $MTTF_d$ ≤ 100 ans
(donc $MTTF_d$ = « Elevé »)</td><td>10 ans ≤ $MTTF_d$ ≤ 100 ans
(donc $MTTF_d$ ≥ « moyen »)</td><td>$MTTF_d$ canal = 100 ans
$MTTF_d$ Elevé</td></tr>
<tr><td>DC_{avg} ≥ 60 %
(donc DC_{avg} ≥ « Faible »)</td><td>DC_{avg} ≥ 90 %
(donc DC_{avg} ≥ « Moyenne »)</td><td>DC_{avg} = 99 %
DC_{avg} Elevée</td></tr>
<tr><td colspan="2">CCF : score ≥ 65</td><td>Score = 95</td></tr>
<tr><td colspan="2">Composant et principes de sécurité éprouvés
Défaut unique = état sûr</td><td>OK
OK</td></tr>
<tr><td colspan="2">Essais : si possible, dès ou avant prochaine sollicitation</td><td>Essais : à chaque sollicitation</td></tr>
<tr><td colspan="2">Si défaut détecté : conduire à état sûr (arrêt)</td><td>Si défaut détecté :
Etat sûr = arrêt</td></tr>
<tr><td colspan="2"> 
</td><td>Catégorie 3</td></tr>
<tr><td>Prise en compte des fautes systématiques</td><td colspan="2">Annexe G</td><td>OK</td></tr>
<tr><td>Logiciel</td><td colspan="2">§ 4.6 et annexe J</td><td>Sans objet</td></tr>
<tr><td colspan="3">Conclusion : PL « d » obtenu ?</td><td>OUI</td></tr>
</table>

Tableau 10 : Récapitulatif des résultats obtenus pour la SRP/CSa

Note : Compte tenu de l'ensemble des résultats obtenus, la SRP/CSa satisfait les préconisations minimales requises pour revendiquer un PL « e ». Cette revendication d'un PL supérieur à celui nécessaire pour satisfaire le PL_r du SC/FS peut être utile dans le cas de combinaison de SRP/CS (voir tableau 11 de la norme).

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

A5.2 Conception de la SRP/CSb

Pour la SRP/CSb, un module de sécurité apte à atteindre un PL « e » sera mis en œuvre, car c'est le niveau de performance le plus couramment disponible sur le marché pour ce type de composant (les modules de PL « d » sont rares). L'étude consistera à intégrer ce module pour assurer que le PL « e » est atteint pour cette SRP/CS.

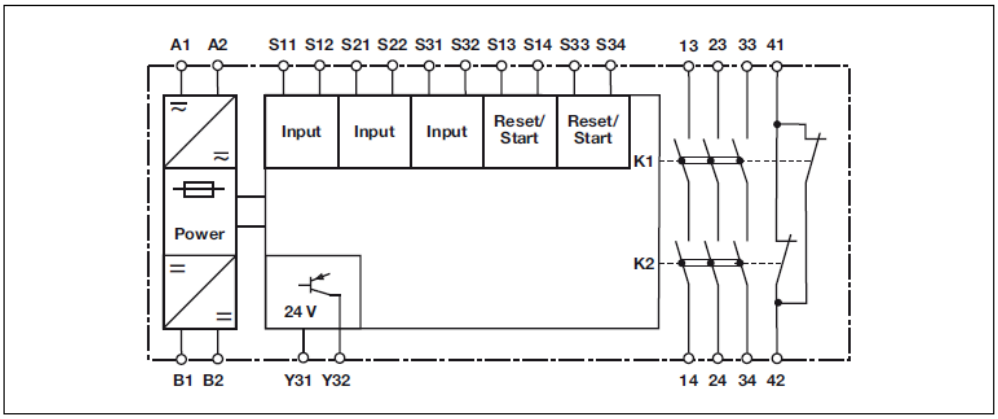
Spécification de la SRP/CS Traitement	
	Nom : SRP/CSb
Conditions d'activation	Active en permanence
Interface	Entrée : - 2 signaux électriques de sortie de la SRP/CSa Sortie : - 2 signaux électriques
Moyens d'interconnexion (i_{ab},i_{bc})	Entre SPR/CSa et SPR/CSb : traité dans la SPR/CSa. Entre SPR/CSb et SPR/CSc : traité dans la SPR/CSc.
Description	Cette partie consiste à traiter la redondance du dispositif de verrouillage. Chaque signal de sortie est à l'état logique « 0 » lorsque l'une des deux entrées est à l'état « 0 » et à l'état logique « 1 » lorsque les deux entrées sont à l'état « 1 ».
Priorités	Sans objet
Temps de réaction maximal	La somme des temps des SPR/CS ne doit pas dépasser le temps de réaction maximal spécifié pour le SC/FS (80 ms).
Taux de demande	Le module commute à chaque sollicitation du protecteur. La fréquence de commutation du module est estimée à 10 fois par heure par période de 8 h à raison de 220 j/an.
Conditions d'ambiance	Degré de protection minimal IP 65

Tableau 11 : Spécification de la SRP/CSb

Le choix se porte sur un module du commerce revendiquant un niveau de performance « jusqu'à PLe », dont la description du fonctionnement répond aux spécifications fonctionnelles exprimées dans le Tableau 11.

Pour que la SRP/CSb, et donc le module, atteigne effectivement un PLe, les prescriptions du constructeur rappelées dans les Figure 17 et Figure 18 sont respectées.

Schéma de principe



jusqu'à PL e selon l'EN ISO 13849-1

Description du fonctionnement

- Commande par 1 canal : pas de redondance dans le circuit d'entrée, les mises à la terre dans les circuits de réarmement et d'entrée sont détectées.
- Commande à 2 canaux d'entrée avec détection des courts-circuits : circuit d'entrée redondant, reconnaissant
  - les mises à la terre dans le circuit de réarmement et le circuit d'entrée
  - les courts-circuits dans le circuit d'entrée ainsi que dans le circuit de réarmement lors d'un réarmement auto-contrôlé.
  - les courts-circuits entre les circuits d'entrée.
- Réarmement automatique : l'appareil est activé dès que le circuit d'entrée est fermé.
- Réarmement auto-contrôlé : l'appareil est activé lorsque le circuit d'entrée est fermé et lorsque le circuit de réarmement se ferme après l'écoulement du temps d'attente (voir les caractéristiques techniques)
- Augmentation possible du nombre de contacts et du pouvoir de coupure des contacts de sécurité instantanés par le raccordement de blocs d'extension de contacts ou de contacteurs externes.

Légende

- Power : tension d'alimentation
- Reset/Start : circuit de réarmement S13-S14, S33-S34
- Input : circuit d'entrée S11-S12, S21-S22, S31-S32
- Output safe : contacts de sécurité 13-14, 23-24, 33-34
- Output aux : contacts d'information 41-42
- Out semi : état de commutation des canaux 1/2 de la sortie statique
- ①: réarmement automatique
- ②: réarmement auto-contrôlé
- t_1 : temps de montée
- t_2 : temporisation à la retombée
- t_3 : temps de remise en service
- t_4 : temps d'attente

Câblage

Important :

- Respectez impérativement les données indiquées dans la partie "Caractéristiques techniques".
- Les sorties 13-14, 23-24, 33-34 sont des contacts de sécurité, la sortie 41-42 est un contact d'information (par exemple pour l'affichage).
- Protection des contacts de sortie par des fusibles (voir les caractéristiques techniques) pour éviter leur soudage.
- Calcul de la longueur de câble max. I_{max} sur le circuit d'entrée :

Déf systématiques

$$I_{max} = \frac{R_{lmax}}{R_l / km}$$

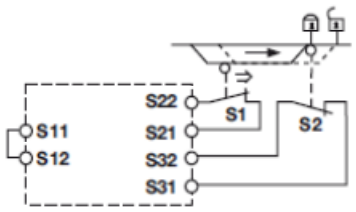
R_{lmax} = résistance max. de l'ensemble du câblage (voir les caractéristiques techniques)
R_l /km = résistance du câblage/km

- Utilisez uniquement des fils de câblage en cuivre résistant à des températures de 60/75 °C.
- Assurez-vous du pouvoir de coupure des contacts de sortie en cas de charges capacitives ou inductives.

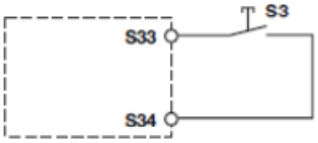
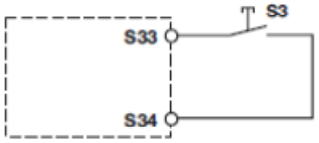
Figure 17 : Extrait de la notice constructeur du module de sécurité

Le schéma de raccordement recommandé, prenant en compte les éventuels courts-circuits des entrées (exigence de comportement en présence de défaut exprimée au niveau de la SRP/CSa) et retenu pour respecter un PLe est le suivant :

▸ Circuit d'entrée

Circuit d'entrée	monocanal	à deux canaux
Protecteur mobile **avec** détection des courts-circuits entre les canaux Type de raccordement retenu pour l'entrée dans la notice du fabricant		

▸ Circuit de réarmement

Circuit de réarmement	Câblage de la arrêt d'urgence (monocanal) Protecteur mobile (monocanal)	Câblage de la arrêt d'urgence (à deux canaux) Protecteur mobile (à deux canaux)
Réarmement automatique	Type de raccordement retenu pour le réarmement dans la notice du fabricant	
Réarmement auto-contrôlé		

▸ Boucle de retour

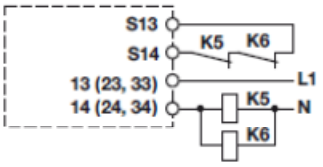
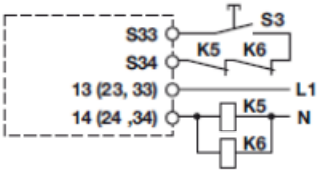
Boucle de retour	Réarmement automatique	Réarmement auto-contrôlé
Contacts des contacteurs externes		

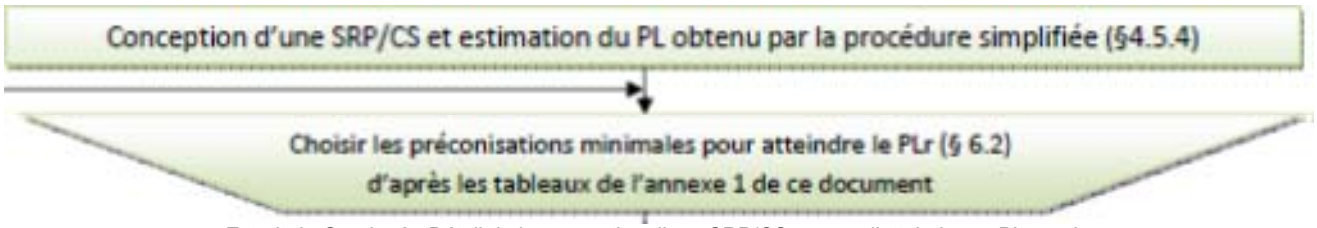
Figure 18 : Extrait de la notice constructeur du module de sécurité

Défaillances systématiques (Voir annexe A de ce document)

La prévention et la maîtrise des défaillances systématiques est obtenue par le respect de la notice de mise en œuvre du module de sécurité et notamment par :

- la mise en place de fusibles correctement calibrés sur l'alimentation des contacts de sorties,
- le respect de la charge admissible sur les contacts de sortie (pouvoir de coupure),
- le respect de la longueur et de la nature des câbles d'acquisition des signaux d'entrée du module,
- le positionnement du module dans un coffret électrique d'IP > 65.

A5.3 Conception de la SRP/CSc



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

La SRP/CSc doit être conçue pour atteindre au moins un PL « d » en respectant les critères correspondants, synthétisés dans le Tableau 12 extrait de l'annexe 1 de ce document. La catégorie 3 est retenue.

nisations minimum pour un PL « d » – Suivant tab[redacted]t pour utilisation d[redacted]océdure s

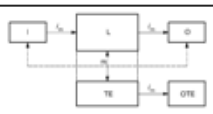
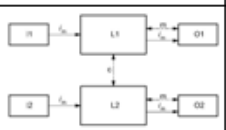
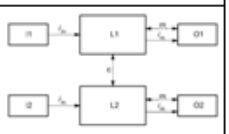
Catégories autorisées	Cat 2 *§ 6.2.5*	Cat 3 *§ 6.2.6*	Cat 3 *§ 6.2.6*
Respect autre catégorie	Respect exigences de Cat B	Respect exigences de Cat B	Respect exigences de Cat B
MTTFd par canal fonct. *§4.5.2*	30ans ≤ MTTFd ≤ 100 ans (donc MTTFd = « Elevé »)	30ans ≤ MTTFd ≤ 100 ans (donc MTTFd = « Elevé »)	10ans ≤ MTTFd ≤ 100 ans (donc MTTFd ≥ « moyen »)
DC_{avg} mini *§4.5.3 et Annexe E*	DC_{avg} ≥ 90% (donc DC_{avg} ≥ « Moyenne »)	DC_{avg} ≥ 60% (donc DC_{avg} ≥ « Faible »)	DC_{avg} ≥ 90% (donc DC_{avg} ≥ « Moyenne »)
CCF *Annexe F*	score ≥ 65	score ≥ 65	score ≥ 65
Spécificités	- Composants et principes de sécurité éprouvés (§ 6.2.4) - $MTTFd_{uc}$ à considérer (§ 4.5.4)	- Composant et principes de sécurité éprouvés (§ 6.2.4) - Défaut unique = état sûr	- Composant et principes de sécurité éprouvés (§ 6.2.4) - Défaut unique = état sûr
Contrôle des fonctions - périodicité	Démarrage machine, et périodiquement (automatique ou manuel), et Taux de demande ≤ 1/100 du taux d'essais	Si possible, dès ou avant prochaine sollicitation	Si possible, dès ou avant prochaine sollicitation
Contrôle des fonctions - réaction	Si défaut détecté : Conduire à état sûr (arrêt) Ou avertissement de danger	Si défaut détecté : Conduire à état sûr (arrêt)	Si défaut détecté : Conduire à état sûr (arrêt)
Architecture désignée			
fautes systématiques	Annexe G	Annexe G	Annexe G

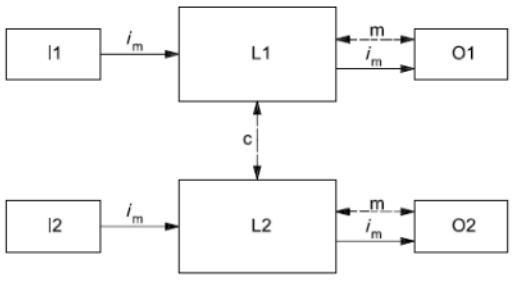
Tableau 12 : Préconisations minimales pour atteindre un PL « d »

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

Spécification de la SRP/CS Sortie	
	Nom : SRP/CSc
Conditions d'activation	Active en permanence
Interface	Entrée : - 2 signaux électriques de sortie de la SRP/CSb Sortie : - orifices de commande du moteur hydraulique.
Moyens d'interconnexion (i_{bc})	Entre SRP/CSb et SRP/CSc : câbles électriques soumis aux contraintes environnementales extérieures au coffret électrique.
Description	Cette partie consiste à arrêter et empêcher l'alimentation en fluide hydraulique du moteur si l'une des entrées est à l'état « 0 » et à autoriser l'alimentation en fluide hydraulique du moteur si les deux entrées sont à l'état « 1 ».
Priorités	Par rapport aux ordres hydrauliques de commande standards.
Temps de réaction maximal	La somme des temps des SPR/CS ne doit pas dépasser le temps de réaction maximal spécifié pour le SC/FS (80 ms).
Taux de demande	Les composants mis en œuvre commutent à chaque sollicitation du protecteur. La fréquence de commutation des composants est estimée à 10 fois par heure par période de 8 h à raison de 220 j/an.
Conditions d'ambiance	Degré de protection minimal IP 65

Tableau 13 : Spécification de la SRP/CSc

L'architecture retenue comme base de conception est fixée par la norme (cf. figure 11), voir Extrait 4.



Les traits interrompus représentent la détection de défaut raisonnablement praticable.

Légende

i_m	moyens de connexion
c	surveillance croisée
I1, I2	dispositifs d'entrée, par exemple détecteur
L1, L2	logique
m	surveillance
O1, O2	dispositifs de sortie, par exemple contacteur principal

Figure 11 — Architecture désignée pour la catégorie 3

Extrait 4 : Figure 11 de la norme NF EN ISO 13849-1

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

Mise en œuvre de l'architecture retenue.

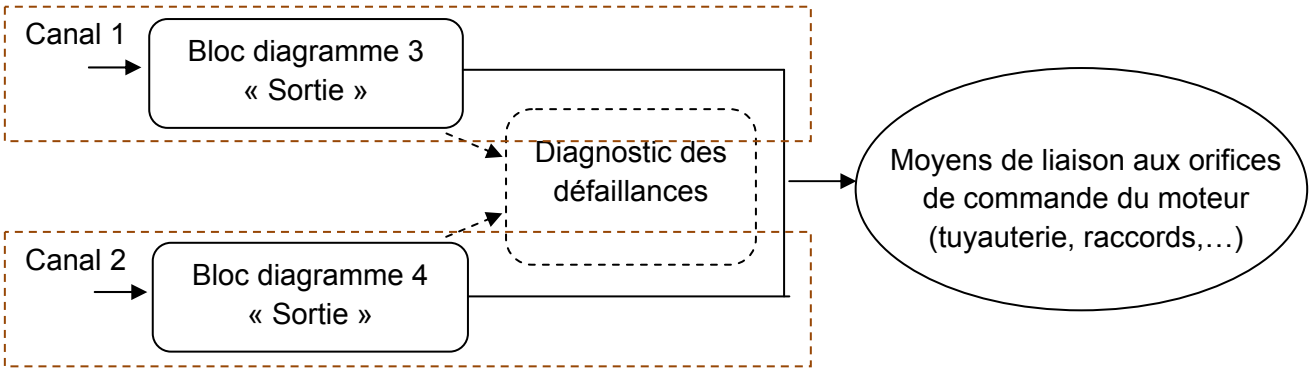
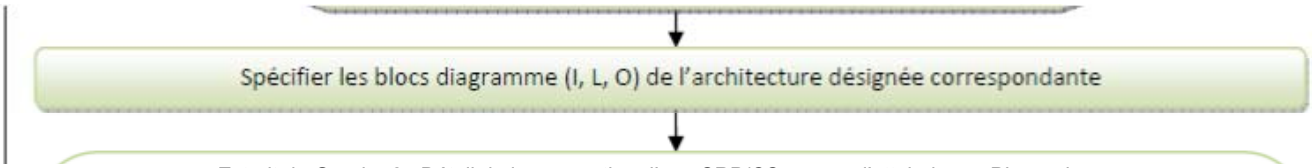
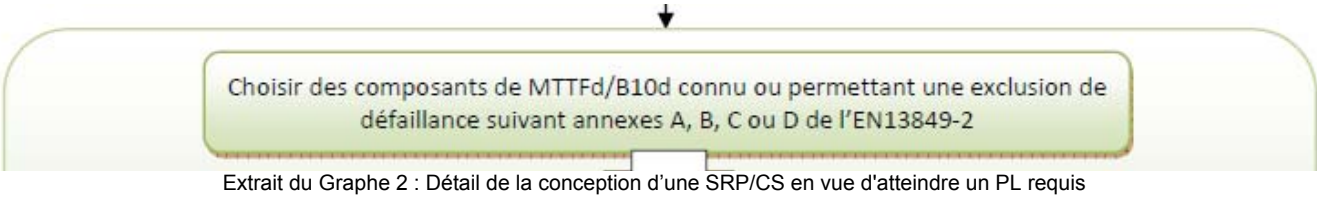


Figure 19 : Découpage de la SRP/CSc en blocs diagramme



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Chaque bloc assure unitairement l'intégralité de la fonction de chacun des canaux décrits dans la spécification de la SRP/CSc. Il n'y a donc pas lieu de spécifier à nouveau chacun des blocs, il suffit de reprendre les éléments de la spécification de la SRP/CSc.



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Choix du matériel identique pour les blocs diagramme 3 et 4

Le choix suivant est effectué (voir Figure 20) :

Deux distributeurs hydrauliques 4/2 (4 orifices/2 positions).

Lorsque leurs bobines sont alimentées électriquement, ils commutent l'alimentation hydraulique depuis EVD vers le moteur.

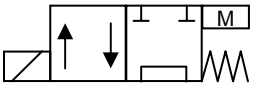
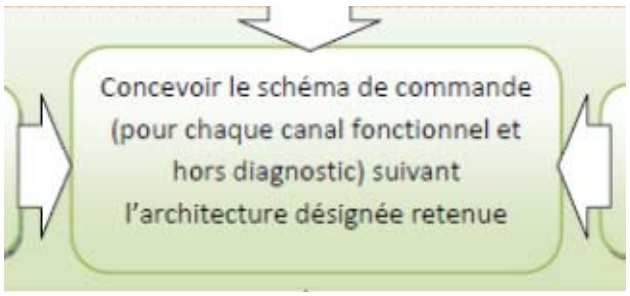


Figure 20 : Distributeur hydraulique 4/2

Lorsque leurs bobines ne sont plus alimentées, ils arrêtent les mouvements de rotation du moteur quelle que soit la position du distributeur de commande directionnel du moteur hydraulique EVD et ils dérivent l'alimentation hydraulique vers le réservoir.

Pour les composants choisis, le temps de réponse est 30 ms.

Conception du canal fonctionnel suivant l'architecture désignée de catégorie 3 retenue pour la SRP/CS



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Les canaux 1 et 2 sont respectivement constitués de « **EVS1** » et « **EVS2** ».

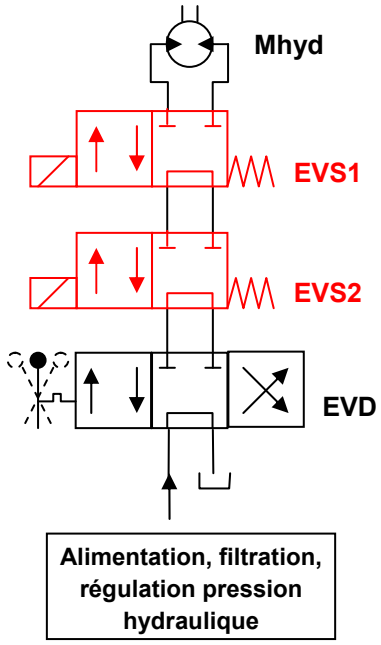
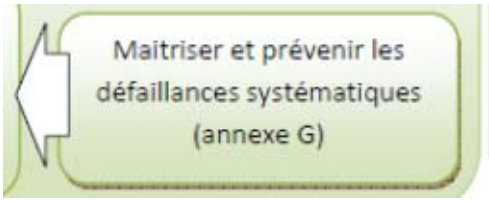


Figure 21 : Schéma hydraulique envisagé

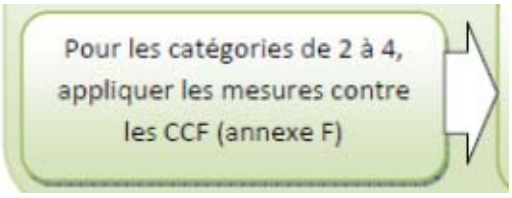
Défaillances systématiques (Voir annexe A de ce document)



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Les éléments pris en compte doivent inclure également les moyens de liaison aux orifices de commande du moteur (tuyauterie, raccords,…).

Mesures prévues contre les CCF et notation (voir Tableau 14)

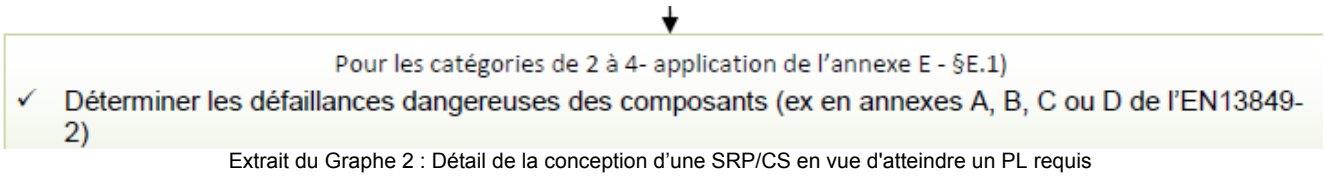


Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Tableau 14 : Notation des mesures contre les CCF pour la SRP/CSc

N°	Notation des mesures contre les CCF (annexe F – Informative - de la norme)	
1	**Séparation/Isolement**	
	Séparation physique entre les voies de signaux **– Score atteint**	***15***
	Séparation par mise en œuvre d'un câble d'alimentation propre à chacun des distributeurs hydrauliques	***x***
2	**Diversité**	
	Différents principes de conception/technologies ou physiques sont utilisés **– Score non atteint**	***0***
	/	**N**
3	**Conception/application/expérience**	
3.1	Protection contre surtension, surpression, surintensité, etc. **– Score atteint**	***15***
	Protection électrique (surintensité) assurée au niveau de l'alimentation des sorties du module (SRP/CSb) *Protection hydraulique (surpression) assurée au niveau de l'alimentation hydraulique*	***x***
3.2	Utilisation de composants éprouvés **– Score atteint**	***5***
	Utilisation de composants hydrauliques conçus selon des principes de sécurités éprouvés	***x***
4	**Appréciation/analyse**	
	Analyse et prise en compte des modes de défaillance et de leurs effets pour prévenir les CCF à la conception **– Score atteint**	***5***
	La principale possibilité de CCF des distributeurs hydrauliques est liée à la qualité du fluide hydraulique. Elle est prise en compte par une prévention de la contamination du fluide hydraulique (voir 6.1)	***x***
5	**Compétence/formation**	
	Score atteint	***5***
6	**Environnement**	
6.1	Prévention de la contamination et de la CEM contre les CCF **– Score atteint**	***25***
	Commande électromécanique, des distributeurs hydrauliques, non sensible à CEM *Alimentation hydraulique filtrée au niveau du médium sous pression*	***x***
6.2	Autres influences **– Score atteint**	***10***
	Exigences environnementales prise en compte dans les choix des distributeurs hydrauliques (vibrations, humidité, température, choc) suivant les contraintes de l'application.	***x***
	Score total	***80***
Le score total est ≥ 65 : Les mesures mises en œuvre satisfont les exigences		

Analyse des modes de défaillance de chacun des canaux et de leurs conséquences :

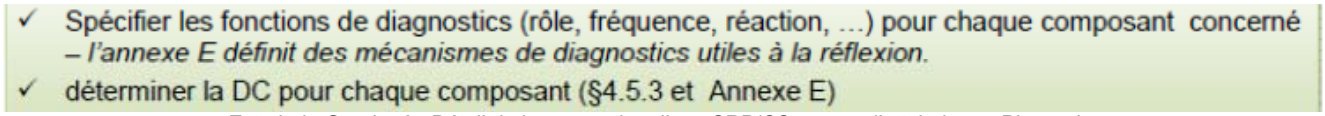


Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Composant	**Type de défaillance retenu**	**Conséquence**	**Conclusion sur la potentialité du danger résultant (pour la SRP/CS)** mouvement dangereux : **D** mouvement non dangereux : **ND**
Distributeur hydraulique **EVS1**	Blocage mécanique, rupture ressort	Distributeur reste actionné	D
	Blocage mécanique ou coupure bobine	Distributeur au repos	ND
Distributeur hydraulique **EVS2**	Blocage mécanique, rupture ressort	Distributeur reste actionné	D
	Blocage mécanique ou coupure bobine	Distributeur au repos	ND

Tableau 15 : Analyse des modes de défaillance des composants de la SRP/CSc

Spécification des diagnostics et détermination du DC :



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Composant **et rappel des défauts potentiellement dangereux**	**Diagnostic prévu** (en se basant sur annexe E de la norme)	**DC de chaque composant** (d'après annexe E de la norme)
Distributeur hydraulique **EVS1** ou **EVS2** Défaillance prise en compte : Distributeur reste actionné	***Dispositif de sortie*** *- Surveillance directe de la position électrique des distributeurs de commande*	99 %

Tableau 16 : Mesures mises en œuvre pour les diagnostics et estimation de la DC

Composant	**Spécification et taux d'essais**
Distributeur hydraulique **EVS1** ou **EVS2**	La surveillance directe de la position électrique des distributeurs de commande est effectuée systématiquement à chaque sollicitation des distributeurs hydrauliques et donc à chaque ouverture du protecteur, par la SRP/CSb (module).

Tableau 17 : Spécification de la fonction de diagnostic de la SRP/CSc

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Détermination du $MTTF_d$ des composants uniques

Dans le cas présent, en l'absence de données « constructeur », le $MTTF_d$ pour chaque composant est déterminé d'après les valeurs typiques du tableau C.1 de la norme soit 150 ans pour EVS1 et EVS2.

Application de la « méthode bloc »

Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Dans le cas présent (Figure 22), chaque canal est constitué d'un composant unique

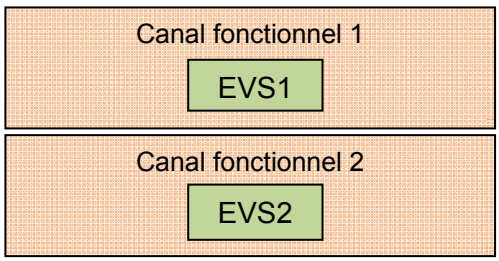
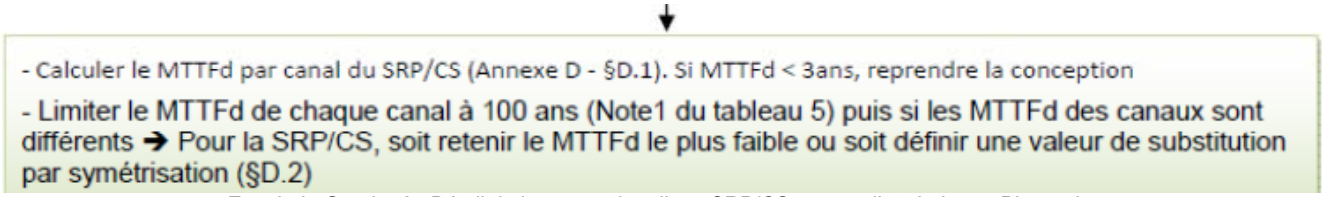
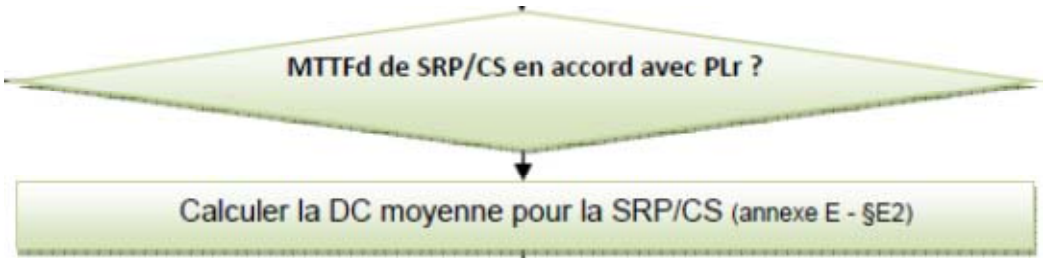


Figure 22 : Schéma identifiant les parties relatives à la sécurité de la SRP/CSc



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

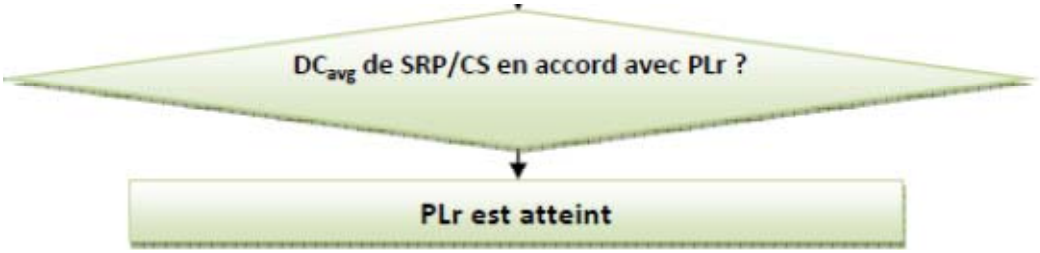
Pour chaque canal : $MTTF_d$ = 150 ans, limité à 100 ans (Note 1 tableau 5 de la norme)
Pour la SRP/CSc, les deux canaux étant symétriques **le $MTTF_d$ par canal est égal à 100 ans**.
$MTTF_d$ élevé qui répond au PLd requis.



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

Les DC de EVS1 et EVS2 sont de 99 %, les $MTTF_d$ de EVS1 et EVS2 sont de 100 ans, donc le calcul donne :

$$DC_{avg} = \frac{\frac{DCEVS1}{MTTFdEVS1} + \frac{DCEVS2}{MTTFdEVS2}}{\frac{1}{MTTFdEVS1} + \frac{1}{MTTFdEVS2}}$$ **= 99 % soit DC_{avg} élevée qui répond au PLd requis.**



Extrait du Graphe 2 : Détail de la conception d'une SRP/CS en vue d'atteindre un PL requis

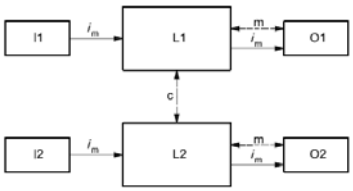
<table>
<tr><th colspan="4">Tableau récapitulatif SRP/CSc</th></tr>
<tr><th>Données</th><th colspan="2">Exigences requises</th><th>Résultats obtenus</th></tr>
<tr><td rowspan="8">Exigences pour un PLd avec usage de la catégorie 3</td><td colspan="2">Respect exigences de Cat B</td><td>OK</td></tr>
<tr><td>30 ans ≤ $MTTF_d$ ≤ 100 ans
(donc $MTTF_d$ = « Elevé »)</td><td>10 ans ≤ $MTTF_d$ ≤ 100 ans
(donc $MTTF_d$ ≥ « Moyen »)</td><td>$MTTF_d$ canal = 100 ans
$MTTF_d$ Elevé</td></tr>
<tr><td>DC_{avg} ≥ 60 %
(donc DC_{avg} ≥ « Faible »)</td><td>DC_{avg} ≥ 90 %
(donc DC_{avg} ≥ « Moyenne »)</td><td>DC_{avg} = 99 %
DC_{avg} Elevée</td></tr>
<tr><td colspan="2">CCF : score ≥ 65</td><td>Score = 80</td></tr>
<tr><td colspan="2">Composant et principes de sécurité éprouvés
Défaut unique = état sûr</td><td>OK
OK</td></tr>
<tr><td colspan="2">Essais : Si possible, dès ou avant prochaine sollicitation</td><td>Essais : à chaque sollicitation</td></tr>
<tr><td colspan="2">Si défaut détecté : Conduire à état sûr (arrêt)</td><td>Si défaut détecté :
Etat sûr = arrêt</td></tr>
<tr><td colspan="2"> 
</td><td>Catégorie 3</td></tr>
<tr><td>Prise en compte des fautes systématiques</td><td colspan="2">Annexe G</td><td>OK</td></tr>
<tr><td>Logiciel</td><td colspan="2">§ 4.6 et annexe J</td><td>Sans objet</td></tr>
<tr><td colspan="3">Conclusion : PL « d » obtenu ?</td><td>OUI</td></tr>
</table>

Tableau 18 : Récapitulatif des résultats obtenus pour la SRP/CSc

Note : Compte tenu de l'ensemble des résultats obtenus, la SRP/CSc satisfait les préconisations minimales requises pour revendiquer un PL « e ». Cette revendication d'un PL supérieur à celui nécessaire pour satisfaire le PL_r du SC/FS peut être utile dans le cas de combinaison de SRP/CS (voir tableau 11 de la norme).

Exemple de conception d'un SC/FS de PL_r « d » - Catégorie 3

A6. Résultats finaux pour le SC/FS

A6.1 Détermination du PL du SC/FS

Le PL de chacune des SRP/CS ayant été déterminé dans les paragraphes A5.1, A5.2 et A5.3, le PL global du SC/FS est déterminé en utilisant le tableau 11 de la norme.

Pour le SC/FS considéré, la combinaison des SRP/CS est représentée Figure 23

Figure 23 : Combinaison des SRP/CS pour atteindre le PL global

Le **PL_{low}** parmi les SRP/CS est PL **d**, ce qui concerne 2 SRP/CS.

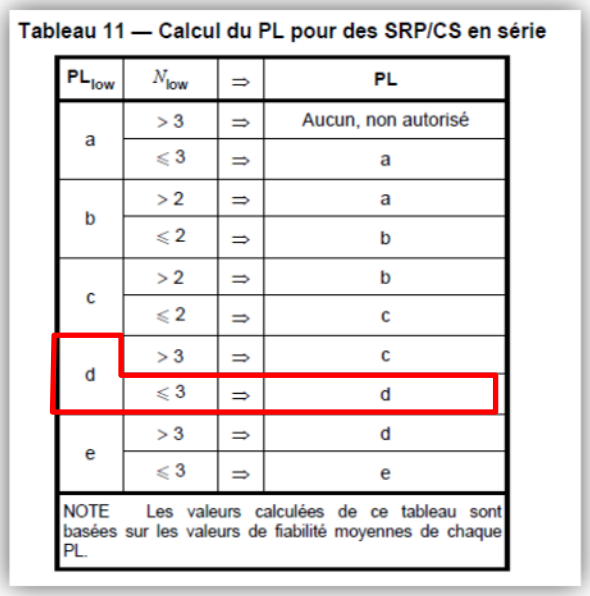


Tableau 11 — Calcul du PL pour des SRP/CS en série

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

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

Figure 24 : Exploitation du tableau 11 de la norme NF EN ISO 13849-1

D'après le tableau 11 de la norme, **le PL du SC/FS est : PL d**

A6.2 Temps de réaction du SC/FS

Le temps de réaction est déterminé en prenant en compte le temps de réponse des différentes SRP/CS constituant le SC/FS.

Temps de réponse	SRP/Csa	SRP/CSb	SRP/CSc	SC/FS
	0	30 ms	30 ms	60 ms

Tableau 19 : Temps de réaction du SC/FS

Le temps de réaction de 60 ms est acceptable car il est inférieur à 80 ms, temps de réaction spécifié pour le SC/FS dans le Tableau 2.

A6.3 Schéma final du SC/FS

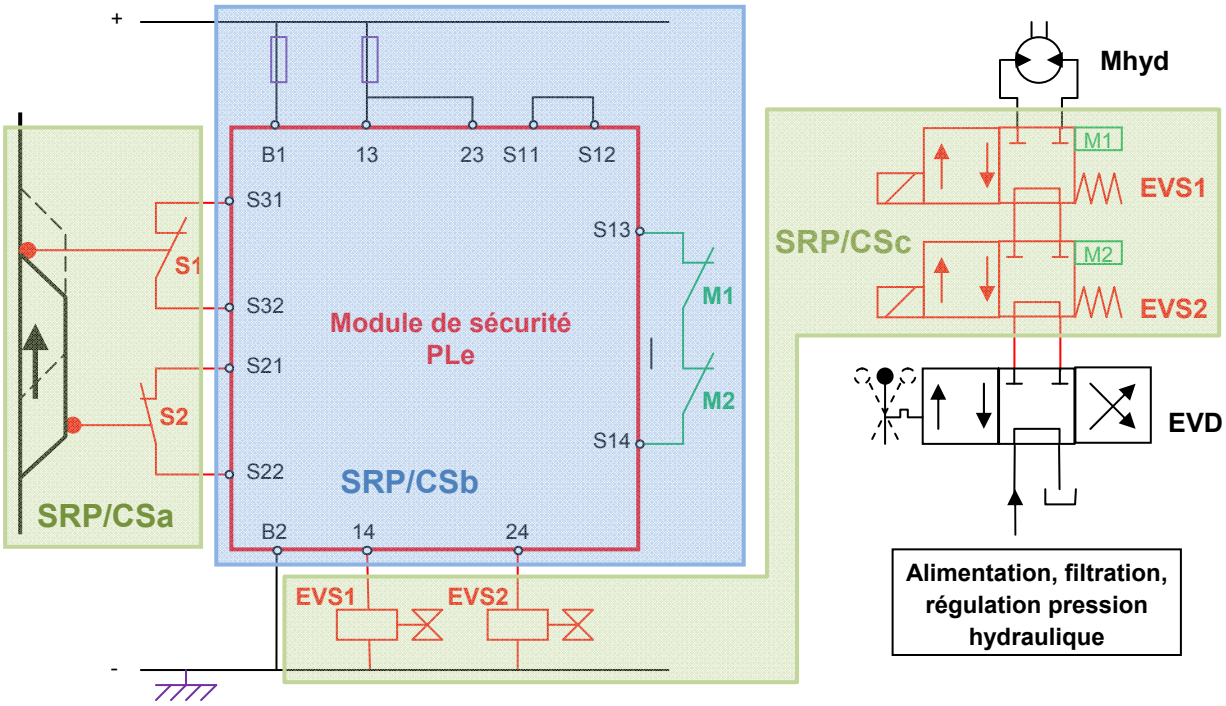


Figure 25 : Schéma final du SC/FS

Annexe A - Défaillances systématiques de toutes les SRP/CS du SC/FS « Arrêt du moteur hydraulique par protecteur »

Le Tableau 20 décrit les mesures mises en œuvre pour couvrir les défaillances systématiques propres à cet exemple de SRP/CS. Toutes les exigences de la norme NF EN ISO 13849-1 sont rappelées dans l'encadré de couleur. Certains principes de sécurité listés dans l'ISO 13849-2 ainsi que la référence aux tableaux des annexes applicables à cet exemple sont rappelés.

Les mesures mises en œuvre sont notées en vert.

Les défaillances systématiques sont prises en compte comme décrit ci-après, en considérant chaque SRP/CS (« a », « b », « c »).

Tableau 20 : Prise en compte des défaillances systématiques

N°	Défaillances systématiques (annexe G – Informative - de la norme)				
	SRP/CSa « a » – SRP/CSb « b »– SRP/CSc « c » **=>**		***a***	***b***	***c***
G.1 Généralités *L'ISO 13849-2 fournit une liste complète de mesures qu'il convient d'appliquer contre les défaillances systématiques telles que les principes de sécurité de base et les principes de sécurité éprouvés.*					
G.2 Exigences pour la maîtrise des défaillances systématiques *Il convient d'appliquer les mesures suivantes*					
G2.1	- *Utilisation de la désactivation énergétique (voir l'ISO 13849-2)* *Il convient de concevoir les parties des systèmes de commande relatives à la sécurité (SRP/CS) de sorte qu'il soit possible d'atteindre ou de maintenir un état sûr de la machine en cas de perte de puissance du système.*		***x***	***x***	***x***
	Ex. « Principes de sécurité de base » électriques (cf. Tableau D.1 de l'ISO 13849-2) **et hydrauliques** (cf. Tableau C.1 de l'ISO 13849-2)				
	Utilisation du principe de désactivation énergétique	L'ouverture du protecteur provoque l'ouverture des contacts des interrupteurs de position S1 et S2 qui se traduit par l'ouverture des contacts (de type F) du module de sécurité qui désexcite les bobines EVS1 et EVS2	***x***	***x***	***/***
		Les distributeurs hydrauliques EVS1 et EVS2 sont à rappel par ressort. Leur désexcitation provoque une coupure ou mise à la bâche du fluide. Une perte de puissance de l'alimentation hydraulique (sous-pression) n'est pas dangereuse. Une coupure de pression mène à un état sûr (arrêt du mouvement dangereux)	***/***	***/***	***x***
G2.2	- *Mesures visant à maîtriser les effets des coupures de tension, variations de tension, surtensions, sous-tensions* *Il convient de prédéterminer le comportement des SRP/CS en cas de coupure de tension, de variations de tension, de surtension et de sous-tension de sorte que les SRP/CS puissent réaliser ou maintenir un état sûr de la machine (voir également la CEI 60204-1 et la CEI 61508-7:2000, A.8).*		***x***	***x***	***x***
	Ex. « Principes de sécurité de base » électriques (cf. Tableau D.1 de l'ISO 13849-2)				

N°	Défaillances systématiques (annexe G – Informative - de la norme)					
	SRP/CSa « a » – SRP/CSb « b »– SRP/CSc « c » **=>**			***a***	***b***	***c***
	Utilisation du principe de la désactivation énergétique	Les variations de tension sont contrôlées par le module de sécurité et conduisent à une ouverture des sorties de sécurité en cas de dépassement des limites		***x***	***x***	***x***
	Protection contre un redémarrage intempestif	En cas de rétablissement de l'alimentation, la fermeture des sorties de sécurité du module impose la fermeture préalable du protecteur. Donc pas de risque		***x***	***x***	***x***
G2.3	- *Mesures visant à maîtriser ou à éviter les effets de l'environnement physique (par exemple la température, l'humidité, l'eau, les vibrations, les poussières, les substances corrosives, les interférences électromagnétiques et leurs effets)* *Il convient de prédéterminer le comportement des SRP/CS en réponse aux effets de l'environnement physique de sorte que les SRP/CS puissent réaliser ou maintenir un état sûr de la machine (voir également, par exemple, la CEI 60529, la CEI 60204-1).*			***x***	***x***	***x***
	Ex. « Principes de sécurité de base » électriques (cf. Tableau D.1 de l'ISO 13849-2) **et hydrauliques** (cf. Tableau C.1 de l'ISO 13849-2)					
	Résistance aux contraintes de l'environnement	Pour les interférences électromagnétiques et leurs effets	Matériels électromécaniques utilisés non sensibles à ces rayonnements	***x***	***/***	***x***
			Module de sécurité – respect des exigences par son fabricant et par le respect de la notice pour sa mise en œuvre.	***/***	***x***	***/***
		Pour l'humidité, l'eau, les poussières	IP 65 pour l'interrupteur de position et le distributeur hydraulique. Matériel prévu pour un usage industriel	***x***	***/***	***x***
			Le module de sécurité IP 40 est placé dans un coffret électrique qui respecte un IP 65	***/***	***x***	***/***
		Vibrations et chocs	Non significatifs pour cette machine	***/***	***/***	***/***
G2.4	- *Une surveillance de la séquence de programme doit être utilisée pour les SRP/CS contenant un logiciel pour détecter une séquence de programme défectueuse.* *Une séquence de programme défectueuse existe si les éléments individuels d'un programme (par exemple : modules logiciels, sous-programmes ou ordres) sont traités selon une séquence erronée ou pendant un laps de temps incorrect ou si l'horloge du processeur est défaillante (voir la CEI 61508-7:2001, A.9)*			***/***	***/***	***/***
	Sans objet : aucune SRP/CS ne comporte de logiciel			***/***	***/***	***/***
G2.5	- *Mesures visant à maîtriser les effets des erreurs et d'autres effets résultant de tout processus de communication de données (voir la CEI 61508-2:2000, 7.4.8)*			***/***	***/***	***/***
	Sans objet : Toutes les informations des SRP/CS sont traitées en logique câblée.			***/***	***/***	***/***
	En outre, il convient d'appliquer une ou plusieurs des mesures suivantes en tenant compte de la complexité de la SRP/CS et de son PL					
G2.6.1	- *détection de défaillance par surveillance en ligne*			***/***	***/***	***x***

N°	Défaillances systématiques (annexe G – Informative - de la norme)			
	SRP/CSa « a » – SRP/CSb « b »– SRP/CSc « c » **=>**	***a***	***b***	***c***
	Détection de défaillance des distributeurs hydrauliques **EVS1** et **EVS2** par monitoring **M1** et **M2**	***/***	***/***	***x***
G2.6.2	- *essais de matériel redondant*	***x***	***x***	***x***
	Contrôle de discordance des entrées S1 et S2 (SRP/CSa) via le module (SRP/CSb) Contrôle interne des deux voies du module (SRP/CSb) Contrôle de l'état des distributeurs hydrauliques EVS1 et EVS2 (SRP/CSc) via le module (SRP/CSb)	***x***	***x***	***x***
G2.6.3	- *diversité du matériel*	***/***	***/***	***/***
	Mesure non mise en œuvre			
G2.6.4	- *fonctionnement en mode positif*	***x***	***/***	***/***
	Interrupteur **S1** actionné suivant le mode positif	***x***	***/***	***/***
G2.6.5	- *contacts liés à action mécanique*	***/***	***/***	***/***
	Mesure non mise en œuvre			
G2.6.6	- *action d'ouverture directe*	***x***	***/***	***/***
	Contact de l'interrupteur **S1** à action directe d'ouverture	***x***	***/***	***/***
G2.6.7	- *mode de défaillance orienté*	***/***	***/***	***/***
	Mesure non mise en œuvre			
G2.6.8	- *surdimensionnement par un coefficient adapté, lorsque le fabricant peut démontrer que le déclassement améliorera la fiabilité — lorsque le surdimensionnement est adapté, il convient d'utiliser un coefficient de surdimensionnement d'au moins 1,5.*	***/***	***/***	***/***
	Mesure non mise en œuvre			
G2.7	*(Voir aussi l'ISO 13849-2:2003, D.3)*	***x***	***x***	***x***
	G.3 Exigences de prévention des défaillances systématiques *Il convient d'appliquer les mesures suivantes*			
G3.1	- *Utilisation de matériaux appropriés et de fabrication adéquate* *Sélection du matériau, des méthodes de fabrication et du traitement en tenant compte par exemple des contraintes, de la durabilité, de l'élasticité, des frottements, de l'usure, de la corrosion, de la température, de la conductivité et de la rigidité diélectrique.*	***x***	***/***	***x***
	Matériel électromécanique (composants et conducteurs) et hydraulique adapté à un usage industriel et à l'usage prévu pour cette application.	***x***	***/***	***x***
G3.2	- *Dimensionnement et forme appropriés* *Tenir compte par exemple des contraintes, de la déformation, de la fatigue, de la température, de l'état de surface, des tolérances et de la fabrication.*	***x***	***/***	***/***

N°	Défaillances systématiques (annexe G – Informative - de la norme)				
	SRP/CSa « a » – SRP/CSb « b »– SRP/CSc « c » **=>**		***a***	***b***	***c***
	Caractéristiques du système d'actionnement des interrupteurs adaptées aux mouvements du protecteur (angle d'attaque des galets des interrupteurs, alignement,…)		***x***	***/***	***/***
G3.3	- *Sélection, combinaison, dispositions, assemblage et installation corrects des composants, y compris le câblage, les branchements et toutes les interconnexions* *Appliquer les normes appropriées et les notes d'application du fabricant, par exemple fiches catalogues, instructions d'installation, spécifications et utilisation des bonnes pratiques d'ingénierie.*		***x***	***x***	***x***
	Respect des règles de l'art de la norme EN60204-1 *Respect de la notice du module* *Respect de la norme EN ISO 4413 :2010 pour le montage des composants hydrauliques*		***x***	***x***	***x***
	Ex. « Principes de sécurité de base » électriques (cf. Tableau D.1 de l'ISO 13849-2)				
	Circuit de protection adéquat	Une borne de chaque bobine d'électrovanne EVS1 et EVS2 ainsi qu'une borne d'alimentation du module sont reliées au circuit de protection.	***/***	***x***	***x***
	Surveillance de l'isolation	Un fusible est installé sur le conducteur qui n'est pas relié à la terre afin de couper automatiquement le circuit après un défaut de terre.	***/***	***x***	***x***
		Le module de sécurité prend en compte les défauts de mise à la terre des entrées.	***x***	***/***	***/***
	Protection contre un redémarrage intempestif	Dans cette application, le rétablissement de l'alimentation du circuit de commande ne crée pas de danger car le protecteur doit être fermé pour autoriser un redémarrage et tout risque est alors écarté.	***/***	***x***	***x***
	Protection du circuit de commande	Le circuit de commande électrique est protégé par la mise en place de fusibles adaptés et calibrés.	***x***	***x***	***x***
	Ex. « Principes de sécurité éprouvés » électriques (cf. Tableau D.2 de l'ISO 13849-2)				
	Distance de séparation	Séparation physique des bornes des conducteurs pouvant présenter des risques en cas de connexions imprévues.	***x***	***x***	***x***
	Ex. « Principes de sécurité de base » hydraulique (cf. Tableau C.1 de l'ISO 13849-2)				
	Limitation de la pression	Le circuit de commande hydraulique est protégé contre les surpressions par des moyens adaptés et calibrés.	***/***	***/***	***x***
	Evitement de manière suffisante de la contamination du fluide	Le système d'alimentation hydraulique est équipé d'une filtration adaptée et contrôlée régulièrement.	***/***	***/***	***x***
G3.4	- *Compatibilité* *Utiliser des composants à caractéristiques de fonctionnement compatibles.*		***x***	***x***	***x***
	Ex. « Principes de sécurité de base » électriques (cf. Tableau D.1 de l'ISO 13849-2) ***/*** **Mesure basée sur l'état de l'art**				

N°	Défaillances systématiques (annexe G – Informative - de la norme)				
	SRP/CSa « a » – SRP/CSb « b »– SRP/CSc « c » **=>**		**a**	**b**	**c**
	Compatibilité	Composants électriques compatibles avec les tensions et les courants utilisés. Composant hydraulique adapté aux pressions, débits de l'application.	**x**	**x**	**x**
G3.5	- *Résistance aux conditions d'environnement spécifiées* *Concevoir la SRP/CS de sorte qu'elle puisse fonctionner dans tous les environnements prévus et toutes les conditions défavorables prévisibles, par exemple température, humidité, vibration et interférence électromagnétique (EMI) (voir l'ISO 13849-2:2003, D.2).*		**x**	**x**	**x**
	Voir mesures prévues en G2.3		**x**	**x**	**x**
G3.6	- *Utilisation de composants conçus selon une norme appropriée et dont les modes de défaillance sont bien définis* *Pour réduire le risque de non-détection de défauts par l'utilisation de composants ayant des caractéristiques spécifiques (voir la CEI 61508-7:2000, B.3.3).*		**x**	**/**	**x**
	Contacts électromécaniques et distributeur hydraulique aux modes de défaillances connus		**x**	**/**	**x**
	En outre, il convient d'appliquer une ou plusieurs des mesures suivantes en tenant compte de la complexité de la SRP/CS et de son PL.				
G3.7.1	- *Revue de conception du matériel (par exemple par inspection ou par sondage)* *Pour que les revues et l'analyse révèlent les divergences entre la spécification et la mise en œuvre (voir la CEI 61508-7:2000, B.3.7 et B.3.8).*		**x**	**x**	**x**
G3.7.2	- *Outils de conception assistée par ordinateur capables de réaliser des simulations ou des analyses* *Exécuter la procédure de conception de façon systématique et inclure des éléments de construction automatiques appropriés qui sont déjà disponibles et vérifiés (voir la CEI 61508-7:2000, B.3.5).*		**/**	**/**	**/**
G3.7.3	- *Simulation* *Réaliser une inspection systématique et complète de la conception d'une SRP/CS en termes de performance fonctionnelle et de dimensionnement correct des composants (voir la CEI 61508-7:2000, B.3.6).*		**/**	**/**	**/**
	Compte tenu de la faible complexité de cette application, les analyses ont été effectuées sans outil de conception ou de simulation		**/**	**/**	**/**
	G.4 Mesures pour éviter les défaillances systématiques lors de l'intégration de SRP/CS *Il convient d'appliquer les mesures suivantes lors de l'intégration de SRP/CS :* - *essais fonctionnels* - *gestion de projet* - *documentation* *En outre, il convient d'appliquer l'essai «boîte noire», en tenant compte de la complexité de la SRP/CS et de son PL.*				
	***non traité dans ce document**		*	*	*