Exemple didactique d'application de la norme NF EN 62061.

J. Baudoin, J.P. Bello

Institut National de Recherche et de Sécurité

Exemple didactique d'application de la norme NF EN 62061

NS 305 NOTE SCIENTIFIQUE ET TECHNIQUE

Exemple didactique d'application de la norme NF EN 62061

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

NS 305
août 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
Centre de Lorraine : 1, rue du Morvan CS 60027 54519 Vandœuvre-les-Nancy cedex • Tél. 03 83 50 20 00

Résumé :

Les concepteurs d'installations automatisées doivent de plus en plus souvent intégrer des composants complexes tels que des Automates Programmables Industriels dédiés à la Sécurité (APIdS) ou des Réseaux de Terrain dédiés à la Sécurité (RTdS), pour traiter des fonctions de sécurité.

Parmi les référentiels disponibles pour la conception des machines, la norme NF EN 62061 est adaptée pour concevoir un circuit de commande de machine intégrant des fonctions de sécurité utilisant des technologies électriques/électroniques/électroniques programmables. Elle décrit les principes généraux de conception des systèmes de commande électriques relatifs à la sécurité (SRECS).

Ce document a été élaboré pour répondre aux industriels qui s'interrogent sur la façon d'appliquer les nouveaux concepts qu'introduit cette norme.

La première partie du document intitulée : Guide de conception d'un SRECS, apporte des éclairages sur certaines parties de la norme et propose également des outils 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. Des phases de conception significatives sont décrites, en faisant ressortir les détails et commentaires jugés nécessaires pour assimiler les principes préconisés par la norme.

Ce document n'a pas pour objectif de se substituer à la norme NF EN 62061 car il n'en reprend pas le contenu. Il a surtout vocation à faciliter la lecture et l'application de cette norme ainsi que son appropriation par les concepteurs en s'appuyant sur des exemples concrets.

Abstract:

The designers of automated systems must increasingly integrate complex components such as Programmable Logic Controllers dedicated to safety or fieldbus dedicated to safety for processing safety functions.

Among the available standards for machine design, NF EN 62061 is suitable for designing a machine control circuit incorporating functional safety of safety-related electrical, electronic and programmable electronic control systems. It describes the general principles of design of Safety Related Electrical Control Systems (SRECS).

This document has been developed to meet industrial wondering about how to apply the new concepts introduced by this standard.

The first part of the document entitled: Guide to design a SRECS, sheds light on some parts of the standard and also offers tools to facilitate the understanding and use, but also the choices that designers will have to make.

The second part consists of a practical case of a safety function implemented by INRS based on the standard and the tools of the guide. Significant phases of design are described, highlighting details and comments deemed necessary to assimilate the principles advocated by the standard.

This document is not intended to replace the standard NF EN 62061 as it doesn't include its whole content. It mainly aims to facilitate the reading and application of this standard and its use by designers based on concrete examples.

SOMMAIRE GENERAL

PREAMBULE **5**

GUIDE DE CONCEPTION D'UN SRECS **6**

1 PRESENTATION GENERALE DE LA NORME NF EN 62061 8
2 TERMES ET DEFINITIONS 12
3 ILLUSTRATION DE LA DEMARCHE 13
4 PLAN DE SECURITE FONCTIONNELLE 15
5 PHASE PREPARATOIRE A LA CONCEPTION DU SRECS 15
6 INTEGRITE DE SECURITE SYSTEMATIQUE DU SRECS (*§ 6.4*) 17
7 FORMALISATION DES SRCF ET DU SRECS 18
8 SPECIFICATIONS ET CHOIX / CONCEPTION DES SOUS-SYSTEMES (*§ 6.7*) 23
9 EVALUATION DU SIL FINAL DES SRCF (§6.6.3) 41
10 LOGICIEL RELATIF AUX SRCF – CONCEPTION ET DEVELOPPEMENT (*§ 6.10 ET 6.11*) 42
11 INTEGRATION ET TESTS DU SRECS (*§ 6.12*) 44
12 INSTALLATION ET VALIDATION DU SRECS (*§6.13 ET § 8*) 44
13 INFORMATIONS POUR L'UTILISATION (*§ 7*), MODIFICATION (*§ 9*) ET DOCUMENTATION DU SRECS (*§ 10*) 46

BIBLIOGRAPHIE 47

EXEMPLE DE CONCEPTION D'UN SRECS **48**

ANNEXE A - DESCRIPTION DE LA PRESSE PLIEUSE 50
ANNEXE B - DETAIL DES FONCTIONS DE SECURITE ET DELIMITATION DU SRECS 57
ANNEXE C - FORMALISATION DES SRCF 63
ANNEXE D - SPECIFICATION ET CHOIX / CONCEPTION D'UN SOUS-SYSTEME 76
ANNEXE E - EVALUATION DU SIL FINAL DE LA SCRF C 94
ANNEXE F - EXTRAIT DES PLANS DE TESTS DE VALIDATION DU SRECS DE LA PRESSE PLIEUSE HYDRAULIQUE 95

Préambule

Les industriels gèrent de plus en plus souvent leurs installations automatisées à l'aide de systèmes de commande programmables. La problématique consiste à intégrer des composants complexes tels que des Automates Programmables Industriels dédiés à la Sécurité (APIdS), des Réseaux de Terrain dédiés à la Sécurité (RTdS), des capteurs et des actionneurs pour traiter à la fois des fonctions de commande « standard » et des fonctions de sécurité d'une installation. De fait, ces industriels doivent s'inscrire dans un cycle complet de conception du système de commande, et endosser le rôle d'intégrateur de composants dédiés ou non à la sécurité.

L'évolution de la normalisation dans ce domaine les conduit à appliquer, soit la norme NF EN 62061 [1], soit la norme NF EN ISO 13849-1 [2] ; la norme NF EN 62061 traitant exclusivement des technologies électriques/électroniques/électroniques programmables. Ces deux normes sont par ailleurs harmonisées et donnent présomption de conformité à la directive « machines » 2006/42/CE [3].

La norme NF EN 62061 décrit des mesures à mettre en œuvre pour la spécification, la conception et la validation de Systèmes de Commande Electriques Relatifs à la Sécurité [c] (SRECS), devant traiter des risques significatifs d'une machine. Elle introduit des principes permettant à un SRECS de satisfaire à un comportement attendu, par exemple la commande de l'arrêt d'un mouvement dangereux d'une machine. Pour concevoir un système sûr, elle considère le problème de façon globale en traitant de l'intégrité de sécurité systématique [h] et de l'intégrité de sécurité du matériel [l], laquelle tient compte de l'architecture mise en œuvre lors de la conception, mais également de la probabilité de défaillance du matériel utilisé. Ce dernier critère fait peur aux concepteurs de machines, peu habitués à l'utilisation et au calcul de ce genre de paramètre. Ce document montrera que les a priori à ce sujet ne sont pas fondés car il s'agit d'un paramètre qui ne pose pas de problème majeur à être évalué en suivant les prescriptions de la norme et dont l'évaluation ne représente qu'une petite partie du cycle de conception d'un SRECS.

Ce document a pour objectif de guider les concepteurs de SRECS dans son utilisation et de les aider à appréhender les notions nouvelles que la norme introduit. Il est basé sur un cas pratique traité par l'INRS.

Ce document a été rédigé suite à une étude menée à l'INRS pour développer l'ensemble du système de commande d'une presse plieuse en suivant les prescriptions de la norme NF EN 62061, sans mener d'analyse critique du contenu de la norme.

Ce document traite, chronologiquement, des différentes étapes qui ont été nécessaires à la conception du circuit de commande d'une presse plieuse intégrant des fonctions de sécurité. Seules les préconisations applicables à la conception du circuit de commande de la machine prises en exemple ou qui méritaient des précisions ont été reprises.

Les exemples décrits dans ce document peuvent être transposés à d'autres types de machines.

Avertissement

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

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

Guide de conception d'un SRECS

SOMMAIRE du GUIDE

1 PRESENTATION GENERALE DE LA NORME NF EN 62061 8

1.1 DOMAINE D'APPLICATION DE LA NORME 8
1.2 DEMARCHE DE CONCEPTION 10

2 TERMES ET DEFINITIONS 12

3 ILLUSTRATION DE LA DEMARCHE 13

4 PLAN DE SECURITE FONCTIONNELLE 15

5 PHASE PREPARATOIRE A LA CONCEPTION DU SRECS 15

5.1 INFORMATIONS DONT LE CONCEPTEUR DU SRECS DOIT DISPOSER 15
5.1.1 Informations fonctionnelles et de sécurité 15
5.1.2 Informations liées à l'appréciation des risques 15
5.2 PRINCIPES GENERAUX DE CONCEPTION D'UN CIRCUIT DE COMMANDE INTEGRANT DES FONCTIONS DE SECURITE 16
5.2.1 Séparation des fonctions de commande, des fonctions de sécurité 16
5.2.2 Gestion des priorités entre les fonctions de commande « standard » et les fonctions de sécurité 16
5.2.3 Spécification des fonctions de sécurité 16
5.3 DELIMITATION DU SRECS DANS LE CIRCUIT DE COMMANDE COMPLET 16

6 INTEGRITE DE SECURITE SYSTEMATIQUE DU SRECS (*§ 6.4*) 17

6.1 EVITEMENT DES DEFAILLANCES SYSTEMATIQUES DU MATERIEL (*§ 6.4.1*) 17
6.2 MAITRISE DES ANOMALIES SYSTEMATIQUES *(§ 6.4.2*) 17
6.3 COMPATIBILITE ELECTROMAGNETIQUE – IMMUNITE (*§ 6.4.3*) 18

7 FORMALISATION DES SRCF ET DU SRECS 18

7.1 IDENTIFICATION DES FONCTIONS DE COMMANDE RELATIVES A LA SECURITE (SRCF) 18
7.2 SPECIFICATIONS DES EXIGENCES FONCTIONNELLES DES SRCF 18
7.3 SPECIFICATIONS DES EXIGENCES D'INTEGRITE DE SECURITE DES SRCF 21
7.4 CONCEPTION D'UNE SRCF 22
7.4.1 Analyse/décomposition d'une SRCF en blocs fonctionnels 22
7.4.2 Attribution de sous-systèmes aux blocs fonctionnels d'une SRCF 22
7.4.3 Anticipation de la structure et de la composition du SRECS pour une conception plus rationnelle des SRCF23

8 SPECIFICATIONS ET CHOIX / CONCEPTION DES SOUS-SYSTEMES (*§ 6.7*) 23

8.1 INFORMATIONS NECESSAIRES POUR LE CHOIX OU LA CONCEPTION D'UN SOUS-SYSTEME 24
8.2 CHOIX D'UN COMPOSANT « TYPE » DU COMMERCE POUR L'INTEGRALITE D'UN SOUS SYSTEME (*§ 6.7.3*) 26
8.3 CONCEPTION D'UN SOUS-SYSTEME « PARTICULIER » 26
8.4 DETERMINATION DU SIL POUVANT ETRE REVENDIQUE PAR UN SOUS-SYSTEME 29
8.4.1 Détermination du SIL vis-à-vis des contraintes architecturales du sous-système (§ 6.7.6) 30
8.4.2 Détermination du SIL vis-à-vis de la PFHD du matériel (§ 6.7.8) 34
8.4.3 Détermination du SIL vis-à-vis des exigences pour l'intégrité de sécurité systématique des sous-systèmes (§ 6.7.9) 38
8.5 PRECONISATIONS CONCERNANT LES FONCTIONS DE DIAGNOSTIC 40
8.5.1 Comportement d'un SRECS suite à la détection d'une anomalie 40
8.5.2 Préconisations de réalisation des fonctions de diagnostic 40

8.5.3 Exemples de fonctions de diagnostic et de réaction à une anomalie 41

9 EVALUATION DU SIL FINAL DES SRCF (§6.6.3) 41

10 LOGICIEL RELATIF AUX SRCF – CONCEPTION ET DEVELOPPEMENT (*§ 6.10 ET 6.11*) 42

11 INTEGRATION ET TESTS DU SRECS (*§ 6.12*) 44

12 INSTALLATION ET VALIDATION DU SRECS (*§6.13 ET § 8*) 44

12.1 INSTALLATION 45
12.2 VALIDATION (*§ 8*) 45

13 INFORMATIONS POUR L'UTILISATION (*§ 7*), MODIFICATION (*§ 9*) ET DOCUMENTATION DU SRECS (*§ 10*) 46

BIBLIOGRAPHIE 47

1 Présentation générale de la norme NF EN 62061

L'INRS a déjà présenté la norme NF EN 62061 dans sa publication réf. PR 34 [4].

Ce document ne rappelle donc ici que les points importants concernant cette norme.

1.1 Domaine d'application de la norme

La norme NF EN 62061 décrit des mesures à mettre en œuvre pour la spécification, la conception et la validation de SRECS, devant traiter des risques significatifs d'une machine. Elle ne traite donc pas des autres types d'énergie, pneumatique ou autres.

La stratégie de conception retenue, par la norme, privilégie une approche d'intégration de dispositifs existants ou de composants de sécurité, conçus sur la base d'autres textes de normes comme par exemple la CEI 61508 [13]. Pour être capable de se suffire à elle-même, elle donne aussi la méthodologie pour concevoir des sous-systèmes simples lorsque leur utilisation est nécessaire en complément de ceux vendus "sur étagère". De fait, elle est donc bien adaptée aux pratiques en usage dans le domaine manufacturier. En effet, les fabricants de composants mettent sur le marché de nombreux "sous-systèmes" de caractéristiques connues, capables de traiter des fonctions de machines, charge ensuite aux concepteurs de machines de les intégrer pour développer leurs logiques de commande.

La Figure 1 montre l'imbrication d'un SRECS dans le système de commande d'une machine ainsi que le champ d'application couvert par la norme NF EN 62061.

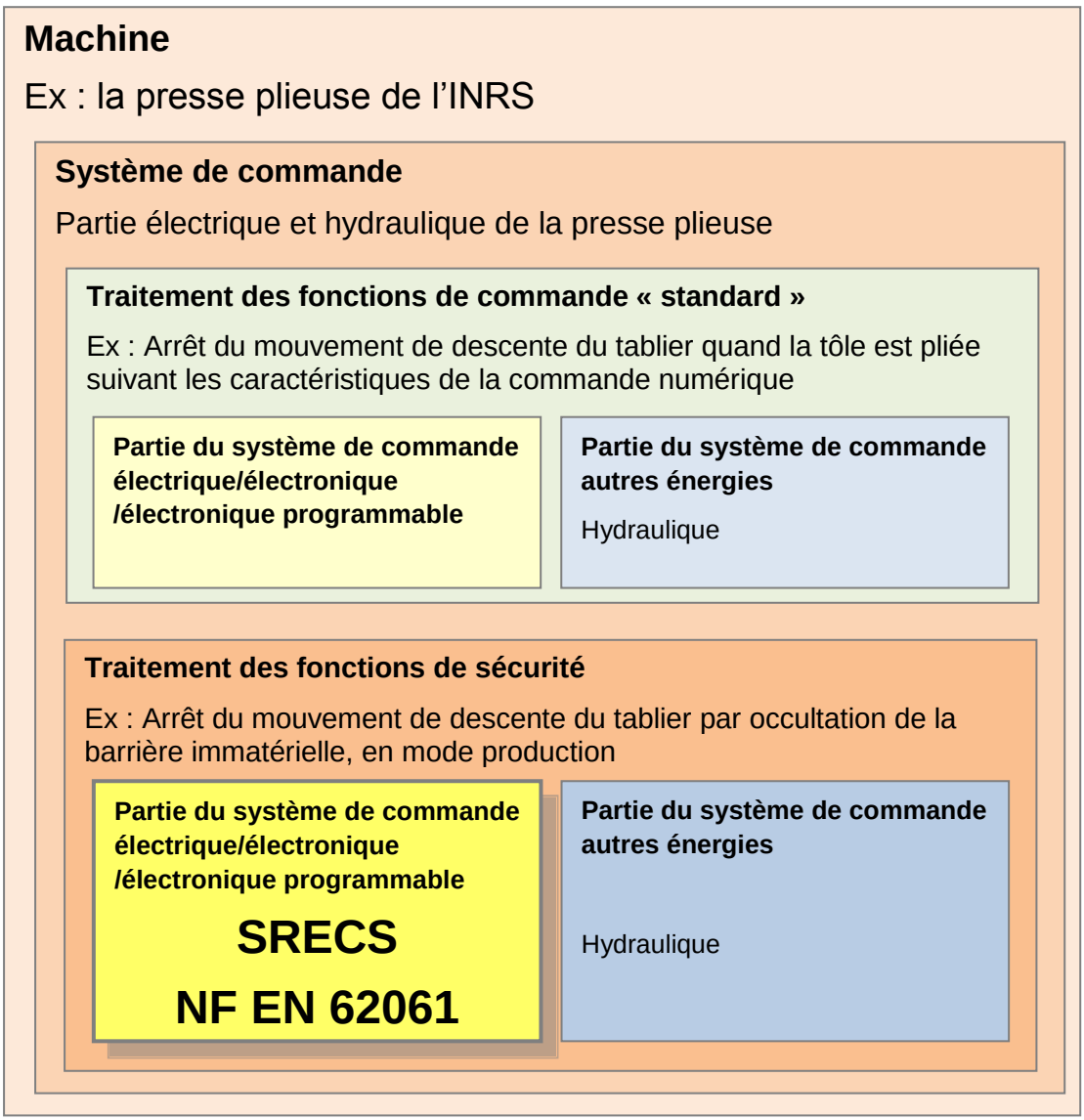


Figure 1 : Exemple de mise en évidence de l'imbrication du SRECS dans le système de commande d'une machine et détermination du champ d'application couvert par la norme NF EN 62061

1.2 Démarche de conception

La Figure 2 montre l'organisation proposée par la norme NF EN 62061 des principales activités de conception d'un SRECS.

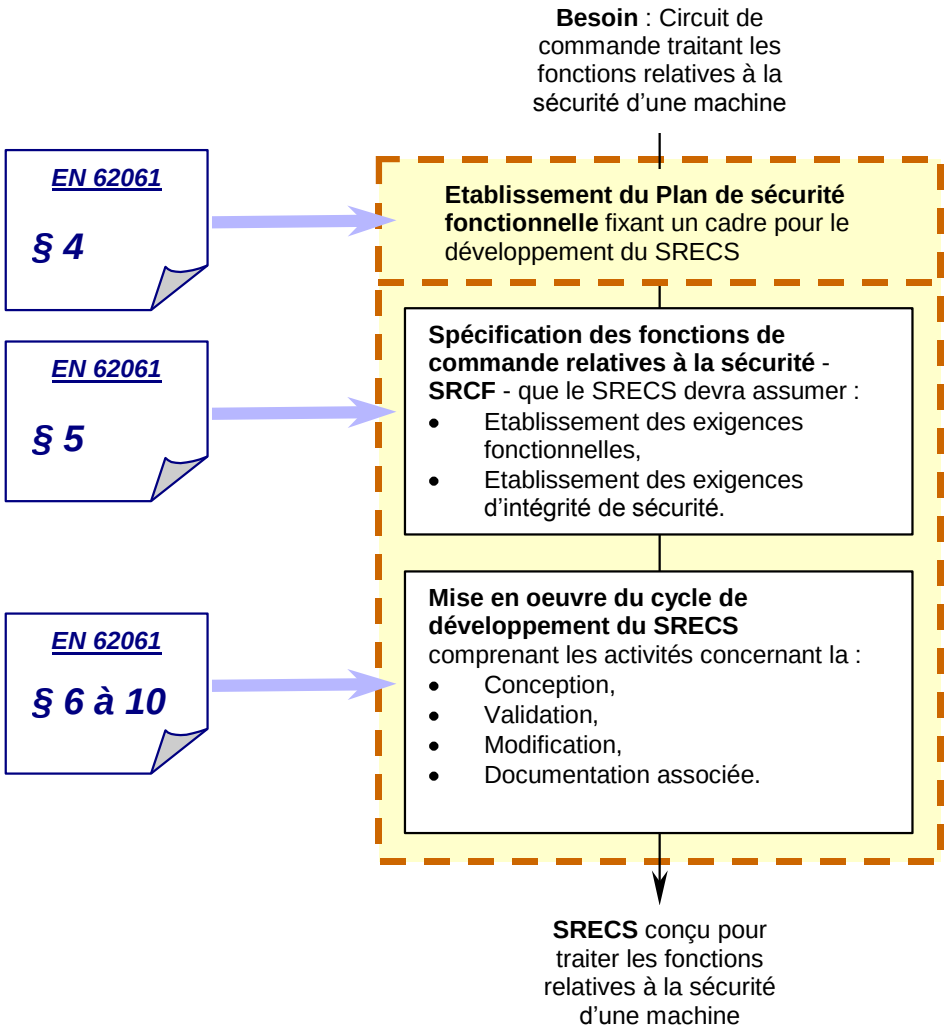


Figure 2 : Organisation des activités de conception d'un SRECS

En premier lieu, la norme impose au concepteur de formaliser clairement le processus de conception du SRECS, préalablement à toute tâche de conception et de tenir à jour le document correspondant nommé « plan de sécurité fonctionnelle » tout au long du processus.

Spécification des fonctions de commande relatives à la sécurité [e] **(SRCF)**

La première activité consiste à spécifier les SRCF à réaliser en donnant, pour chacune de ces fonctions, les exigences fonctionnelles et les exigences d'intégrité de sécurité.

La norme introduit des principes permettant à un SRECS de satisfaire à un comportement « sûr » spécifié en termes de niveau d'intégrité de sécurité [d] SIL, ce dernier étant déterminé suite à une estimation des risques.

Développement du SRECS

Les exigences fonctionnelles et d'intégrité de sécurité exprimées pour les SRCF devront, en s'appuyant sur la norme NF EN 62061, être traduites pour le SRECS sous la forme d'exigences :

- pour l'intégrité de sécurité matérielle :
    - contraintes architecturales,
    - exigences pour la probabilité de défaillance dangereuse aléatoire.
- pour l'intégrité de sécurité systématique :
    - exigences pour l'évitement des défaillances systématiques du matériel,
    - exigences pour la maîtrise des anomalies systématiques,
    - prescriptions d'immunité CEM.
- pour définir son comportement lors de la détection d'une anomalie,
- pour la conception et le développement du logiciel relatif à la sécurité.

Concernant la partie matérielle, le processus consiste à concevoir le SRECS en traitant chacune des SRCF qui lui sont confiées, en respectant les préconisations de la norme pour atteindre le SIL requis. Pour cela, ces fonctions seront conçues en plusieurs étapes qui peuvent être présentées succinctement de la façon suivante :

- Phase de réflexion
    - Les SRCF sont analysées et décomposées en Blocs Fonctionnels [f] (BF)
- Phase d'application
    - Attribution des BF à des Sous-Systèmes [g] (SS)
    - Choix ou conception des sous-systèmes (composants)
    - Mise en œuvre des sous-systèmes
    - Evaluation du SIL final pour chaque SRCF.

La Figure 3 représente schématiquement ces différentes phases.

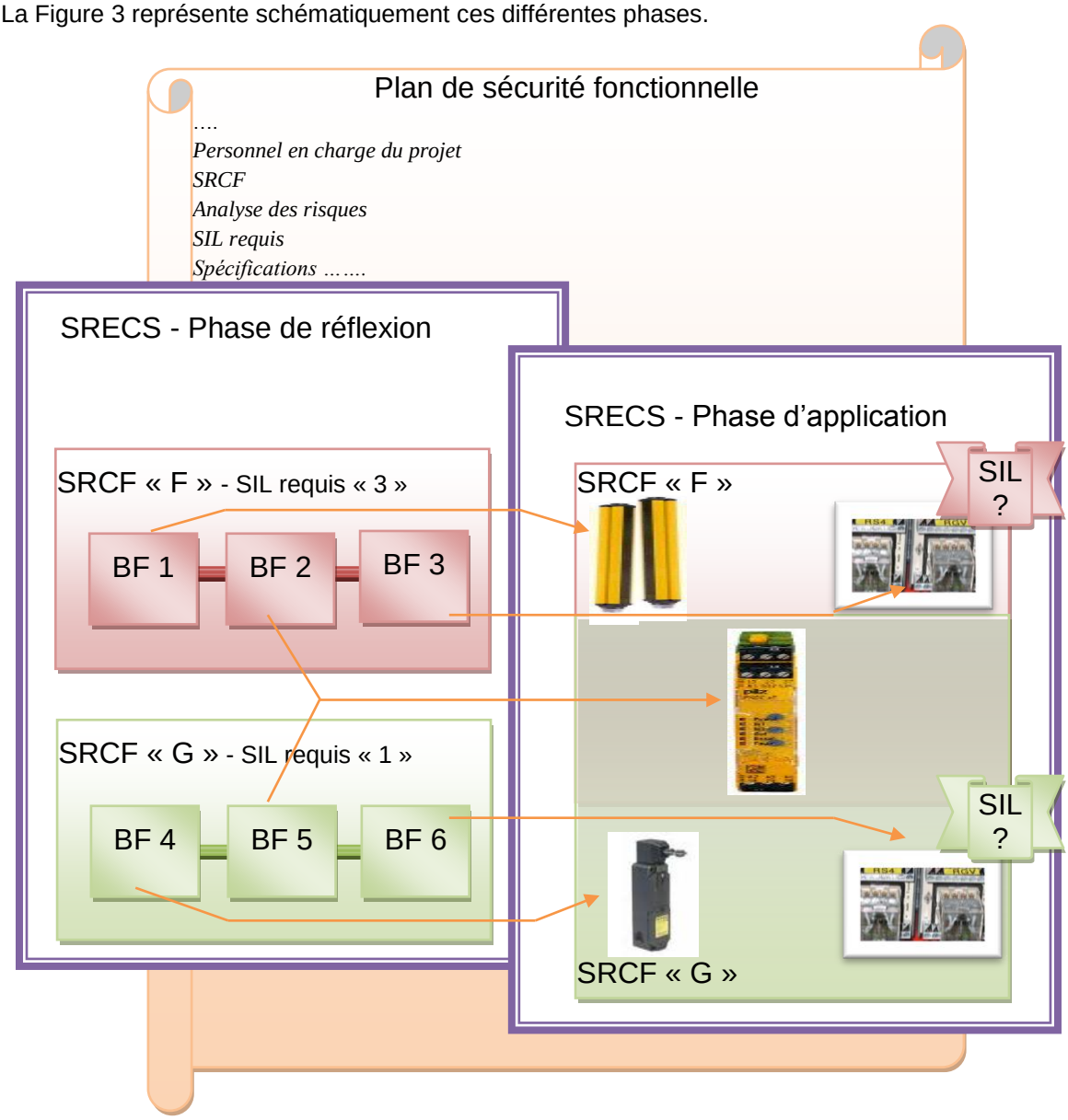


Figure 3 : Représentation schématique des différentes phases de conception d'un SRECS

Enfin, comme cela se faisait déjà avant la parution de cette norme, des phases de validation, de mise en service et de documentation du SRECS sont prévues.

2 Termes et définitions

Note : les définitions issues du chapitre 3 de la norme NF EN 62061 sont reproduites en caractères italiques.

[a] Fonction de commande, appelée également fonction « standard »
Fonction qui évalue les informations ou signaux d'entrée du système de commande et génère des actions ou informations de sortie. Une fonction de commande n'a pas d'influence sur la sécurité des opérateurs.

[b] Fonction de sécurité
Fonction d'une machine dont la défaillance peut provoquer un accroissement immédiat du (des) risque(s).

[c] Système de commande électrique relatif à la sécurité SRECS[1]
Système de commande électrique d'une machine dont la défaillance peut provoquer un accroissement immédiat du (des) risques(s). Le terme électrique recouvre les technologies électrique, électronique ou électronique programmable.

[d] Niveau d'intégrité de sécurité SIL[2]
L'intégrité de sécurité est le moyen qui permettra de satisfaire les objectifs fixés relativement à la sécurité fonctionnelle d'une entité. Cette intégrité de sécurité est quantifiée en 3 niveaux, de 1 à 3, lorsqu'elle est associée à la réduction du risque « machines ». Plus le niveau d'intégrité de sécurité de l'entité est élevé, plus la probabilité d'une défaillance dangereuse de cette entité dans l'exécution de la SRCF requise est faible.

[e] Fonction de commande relative à la sécurité SRCF[3]
Fonction de commande mise en œuvre par un SRECS avec un niveau d'intégrité spécifié, prévue pour maintenir la condition de sécurité de la machine ou empêcher un accroissement immédiat du (des) risque(s). On notera que la notion de SRCF est attachée au SRECS, donc à la partie électrique d'une fonction de sécurité. De ce fait, une SRCF ne constituera qu'une partie d'une fonction de sécurité si des technologies autres qu'électrique sont utilisées pour réaliser cette fonction.

[f] Bloc fonctionnel
Un bloc fonctionnel est le *plus petit élément d'une SRCF dont la défaillance peut entraîner une défaillance de la SRCF.*

[g] Sous-système
Un sous-système est une *entité de la conception de l'architecture générale du SRECS dans laquelle une défaillance d'un sous-système quelconque entraînera une défaillance d'une SRCF.*

[h] Intégrité de sécurité systématique
Partie de l'intégrité de sécurité d'un SRECS ou de ses sous-systèmes qui se rapporte à sa résistance aux défaillances systématiques (défaillances reliées de façon déterministe à une certaine cause) dans un mode dangereux.

[i] Fonction de diagnostic du SRECS
Fonction prévue pour détecter les anomalies dans un SRECS et fournir une activité ou une information de sortie déterminée en cas de détection d'une anomalie.

[j] Dispositif de verrouillage
Dispositif électromécanique destiné à empêcher les mouvements dangereux de la machine de s'accomplir tant qu'un protecteur n'est pas fermé.

[k] Probabilité de défaillance dangereuse par heure PFH_D
Probabilité moyenne de défaillance dangereuse en 1 h.

[l] Intégrité de sécurité du matériel
Partie de l'intégrité de sécurité d'un SRECS ou de ses sous-systèmes comprenant les exigences relatives à la fois à la probabilité de défaillance aléatoire du matériel et de contraintes architecturales.

3 Illustration de la démarche

Le graphe Figure 4 illustre, dans un ordre chronologique, toutes les phases de la démarche à mettre en œuvre pour la conception d'un SRECS.

[1] SRECS : Safety-Related Electrical Control System
[2] SIL : Safety Integrity Level
[3] SRCF : Safety-Related Control Function

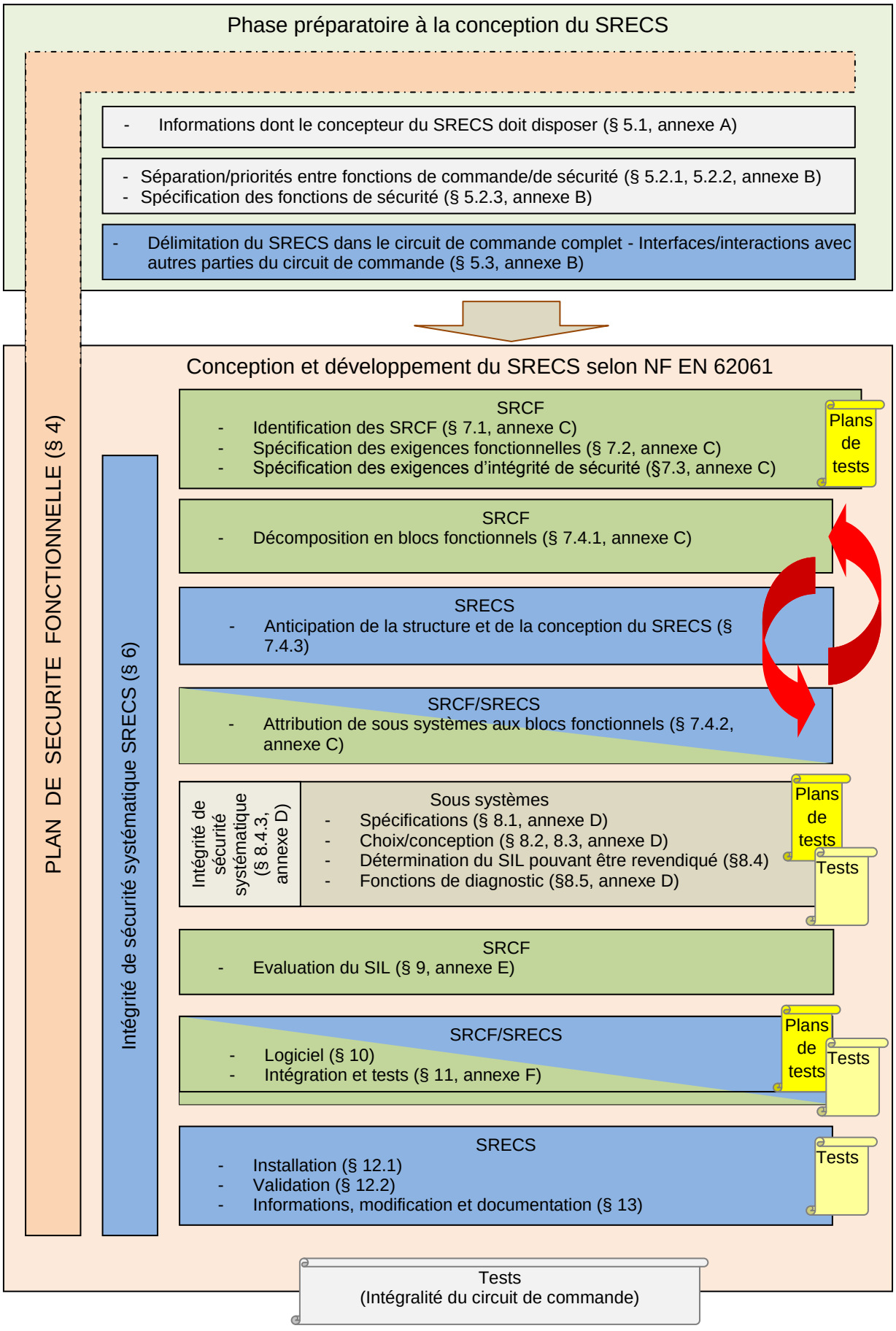


Figure 4 : Illustration graphique de la démarche

4 Plan de sécurité fonctionnelle

La norme NF EN 62061 prévoit la mise en place d'un cadre pour développer le SRECS dans des conditions rigoureuses, pour assurer une traçabilité la plus précise possible et faire vivre le SRECS pour ses évolutions futures.

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

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

Le concepteur ne doit pas négliger d'établir un plan de vérification (***§ 4.2.1.g***[4]) et un plan de validation (***§ 4.2.1.h***), sachant qu'il n'est pas facile de les détailler au départ de la conception d'un SRECS, mais qu'ils doivent évoluer au cours du développement.

Dans le cas de la machine prise en exemple dans ce document, il était quasi impossible de définir la stratégie technique de validation du SRECS au début du projet, car certains des tests dépendaient du matériel mis en œuvre dans le SRECS et celui-ci a naturellement été déterminé en cours du cycle de conception.

5 Phase préparatoire à la conception du SRECS

5.1 Informations dont le concepteur du SRECS doit disposer

Avant de se lancer dans la conception proprement dite du SRECS, il est nécessaire de rassembler un certain nombre d'informations, ou à défaut de compléter celles manquantes par un travail préparatoire afin de disposer, le moment venu, de toutes les informations nécessaires conformément aux préconisations du ***§ 5***.

5.1.1 Informations fonctionnelles et de sécurité

Il est primordial de spécifier toutes les caractéristiques fonctionnelles et de sécurité de la machine pour laquelle l'étude du SRECS est prévue. Elles sont indispensables pour produire les spécifications des exigences fonctionnelles et d'intégrité de sécurité des SRCF. Ces informations sont tirées du cahier des charges ou de la description fonctionnelle de la machine.

5.1.2 Informations liées à l'appréciation des risques

Les éléments de l'appréciation des risques, utilisés lors de la phase de conception de la machine pour le choix des mesures de protection adaptées seront également utiles pour la détermination du niveau de sécurité des fonctions de sécurité assumées par le SRECS. Les éléments utiles sont notamment : la nature du phénomène dangereux (principalement écrasement/sectionnement/coupure pour les risques mécaniques des machines) avec identification de la partie du corps lésée, la gravité du dommage, la fréquence d'accès de l'opérateur à la zone dangereuse (zone d'évolution de l'élément mobile dangereux) etc.

[4] Les références notées en ***italique-gras*** renvoient aux § concernés de la norme NF EN 62061

5.2 Principes généraux de conception d'un circuit de commande intégrant des fonctions de sécurité

5.2.1 Séparation des fonctions de commande, des fonctions de sécurité

Le système de commande d'une machine remplit généralement deux types de fonctions :

- les fonctions de commande « standard » [a] qui participent au fonctionnement de la machine pour assurer sa tâche de production ou pour permettre de la régler et qui n'ont pas de rapport avec la sécurité opérateur. Ces fonctions gèrent généralement les mouvements de la machine tels que montée, descente, avant, arrière, etc.,
- les fonctions de sécurité [b] qui ne sont pas indispensables au fonctionnement de la machine, mais qui sont nécessaires pour gérer la sécurité des opérateurs. Ces fonctions sont généralement liées à la sollicitation d'un protecteur, d'un dispositif de protection ou d'un moyen de prévention. Les fonctions de sécurité peuvent être facilement déduites de la description des modes de marche et de protection contenue dans le cahier des charges du système de commande de la machine, d'où l'intérêt de réaliser cette phase avec précision et en amont (cf. § 7.1 de ce document).

Ces deux types de fonctions peuvent agir indépendamment sur des actionneurs différents, c'est le cas par exemple lorsque la fonction de commande agit sur les mouvements d'un vérin et la fonction de sécurité agit sur l'alimentation en énergie de la machine. Elles peuvent aussi agir de manière concomitante sur le même actionneur. C'est le cas notamment lorsque la fonction de commande agit sur le mouvement d'un actionneur et la fonction de sécurité a pour rôle d'arrêter ou de maintenir à l'arrêt ce même mouvement.

5.2.2 Gestion des priorités entre les fonctions de commande « standard » et les fonctions de sécurité

La notion de priorité intervient uniquement lorsque des fonctions de commande « standard » et des fonctions de sécurité agissent sur le même actionneur ou la même interface de commande de cet actionneur. Dans ce cas, il faut prendre des dispositions pour que les fonctions de sécurité restent toujours prioritaires sur les ordres provenant des fonctions de commande « standard ».

Cette priorité devra être gérée par une partie du système de commande relative à la sécurité. Lors de la délimitation du SRECS, il faudra définir si cette priorité est gérée par le SRECS ou en dehors du SRECS (par des fonctions de sécurité basées sur des technologies autres qu'électriques).

5.2.3 Spécification des fonctions de sécurité

Lorsque les fonctions de sécurité ont été identifiées, séparées dans la mesure du possible des fonctions de commande, et que leurs liens ou priorités vis-à-vis des autres fonctions ont été clairement établis, il est temps de rédiger les spécifications des exigences de sécurité pour tracer toutes les informations recueillies et tout le travail préparatoire effectué propre à chacune de ces fonctions.

Ces spécifications fonctionnelles et de sécurité concernent l'ensemble de la fonction de sécurité, du capteur jusqu'à l'actionneur final, comprenant le cas échéant la partie électrique/électronique qui sera traitée par le SRECS ainsi que les autres parties du circuit de commande gérées par d'autres énergies.

Note : Dans le cas où l'ensemble de la fonction de sécurité est gérée par le SRECS, cas d'un circuit de commande tout électrique, ces spécifications seront intégralement reprises pour la SRCF.

5.3 Délimitation du SRECS dans le circuit de commande complet

Comme évoqué précédemment, le circuit de commande d'une machine est constitué de fonctions de commande et de fonctions de sécurité. De plus, comme c'est souvent le cas, les machines de l'industrie utilisent, en plus de l'énergie électrique/électronique, d'autres énergies telles que

l'hydraulique, le pneumatique, etc. dont la technologie n'est pas prise en compte par la norme NF EN 62061 (voir Figure 1).

Avant d'appréhender la conception du SRECS, il faut donc :

- avoir une vue globale de l'architecture du système de commande de la machine dans lequel sera inclus le SRECS,
- séparer les fonctions de sécurité des fonctions de commande mais également identifier et spécifier précisément toutes les interfaces ainsi que toutes les relations de priorité ou de simultanéité pouvant exister entre ces différentes fonctions,
- délimiter les parties du système de commande relatif à la sécurité utilisant de l'énergie électrique qui vont constituer le SRECS, de celles utilisant une autre énergie en identifiant clairement les interfaces qui peuvent exister entre elles,
- prendre en compte le fait qu'aucun composant électrique, électronique et électronique programmable ne devra être inséré entre l'interface de sortie de la SRCF (limite du SRECS) et l'actionneur (hors SRECS) de l'élément mobile sur lequel doit agir la SRCF ; dans le cas contraire, le niveau d'intégrité de la ou des SRCF concernées pourrait être dégradé.

L'annexe B de ce document illustre cette étape de la conception.

6 Intégrité de sécurité systématique du SRECS (*§ 6.4*)

Le concepteur doit prendre connaissance des principes généraux liés à l'intégrité de sécurité systématique du SRECS très tôt dans le cycle de développement, car ils ont un impact important sur les mesures techniques et organisationnelles à mettre en œuvre.

La définition de l'intégrité de sécurité systématique est rappelée en ***§ 3.2.22***.

L'annexe G de la norme NF EN ISO 13849-1 apporte également des précisions sur les mesures techniques pouvant être mises en œuvre pour maitriser les défaillances systématiques.

6.1 Evitement des défaillances systématiques du matériel (*§ 6.4.1*)

La définition des défaillances systématiques est rappelée en ***§ 3.2.45***.

Les mesures préconisées par la norme ont pour objectif que le SRECS ne soit pas affecté par des défaillances reliées de façon déterministe à une certaine cause. Parmi ces causes, il y a les erreurs humaines lors de la phase de conception (***§ 6.4.1***), notamment au niveau du choix des sous-systèmes, de leur assemblage et interconnexion, de leur compatibilité, de la prise en compte de leur comportement prévisible vis-à-vis de l'environnement extérieur.

Les mesures proposées par la norme (***§ 6.4.1***) ont pour but d'éliminer ces causes, ce qui passe notamment par le respect du plan de sécurité fonctionnelle. Il est explicitement rappelé que les concepteurs devront respecter la norme NF EN 60204-1 [7], qui contient un ensemble de règles déjà appliquées par les concepteurs de systèmes de commande électrique relatifs à la sécurité.

Le ***§ 6.4.1.2*** liste des mesures de revue de conception, de mise œuvre de matériel d'aide à la conception et de simulation dont au moins une doit être appliquée.

6.2 Maitrise des anomalies systématiques *(§ 6.4.2*)

Les mesures préconisées ont pour but de réaliser ou maintenir un état sûr du SRECS lorsque des anomalies systématiques de fonctionnement surviennent, telles que des coupures ou des variations de l'alimentation en énergie, des interférences, des erreurs de processus de communication.

A titre d'exemples, quelques unes des mesures mises en œuvre pour la presse plieuse citée dans ce document sont décrites ci-après :

- les alimentations électriques sont équipées de dispositifs de protection contre les surintensités, calibrés en fonction des circuits alimentés,
- le régime de mise à la terre de l'alimentation en énergie du SRECS est réalisé pour que les SRCF ne soient pas affectées par une mise à la masse accidentelle d'un conducteur actif,
- les ordres d'autorisation des mouvements potentiellement dangereux sont donnés par apport de tension et ceux d'arrêt par coupure de tension,
- les SRCF sont conçues pour commander un arrêt des mouvements correspondants potentiellement dangereux suite à une baisse ou une coupure d'alimentation en énergie électrique,
- le rétablissement de l'alimentation en énergie électrique, suite à une baisse ou une coupure de tension, ne donne pas d'autorisation de mouvement sans un ré-actionnement des ordres de commande,
- le temps de réponse du SRECS ne dépasse pas la valeur spécifiée pour les SRCF même en cas de défaut de communication entre les différents sous-systèmes,
- une coupure ou une erreur de communication entre les différents sous-systèmes mène à une commande d'arrêt des mouvements potentiellement dangereux,
- le diagnostic des éléments de sous-système réagit à chaque sollicitation de la SRCF,
- les SRCF commandent un arrêt des mouvements potentiellement dangereux en cas de courts-circuits entre les conducteurs des câbles de raccordement qui sont mobiles et exposés à des risques de détérioration mécanique.

6.3 Compatibilité électromagnétique – immunité (*§ 6.4.3*)

Ce paragraphe de la norme ne nécessite pas d'être précisé et la note qu'il contient précise bien l'objectif visé. Il convient de prendre en considération le comportement du SRECS en réponse à un phénomène électromagnétique pour toutes les valeurs données en ***annexe E*** de la norme.

7 Formalisation des SRCF et du SRECS

7.1 Identification des Fonctions de Commande Relatives à la Sécurité (SRCF)

Les fonctions de sécurité identifiées lors de la phase préparatoire mettent en œuvre plusieurs types d'énergie (électrique, hydraulique). Comme le SRECS ne prend en compte que la partie traitée en technologie électrique, électronique,…, il faut donc extraire des fonctions de sécurité celles qui seront traitées en tout ou partie par le SRECS. Ces dernières sont nommées « fonctions de commande relatives à la sécurité » (SRCF).

Certaines priorités entre fonctions mises en évidence lors de la spécification des fonctions de sécurité ne seront pas reprises par les SRCF compte tenu de l'architecture adoptée pour le circuit de commande et des limites définies pour le SRECS.

7.2 Spécifications des exigences fonctionnelles des SRCF

Le ***§ 5.2.3.1*** liste les informations à fournir pour spécifier les exigences fonctionnelles de chaque SRCF qui seront nécessaires pour leur conception.

Ces spécifications sont en partie tirées de celles des fonctions de sécurité correspondantes.

Le Tableau 1 liste les informations à renseigner pour spécifier une SRCF.

Spécification des exigences fonctionnelles de la SRCF	
N°	**Nom de la SRCF**
x	**Intitulé de la fonction**
Conditions d'activation de la SRCF	
Interface de la SRCF	
Description de la SRCF	
Priorité par rapport à d'autres fonctions simultanées	
Autres SRCF agissant sur la même interface de sortie	
Temps de réaction maximal de la SRCF	
Fréquence de fonctionnement de la SRCF	
Réaction aux fautes/Conditions de redémarrage	
Conditions d'ambiance	
Taux de cycles de manœuvres, catégorie d'utilisation pour les dispositifs électromécaniques	

Tableau 1 : Spécifications des exigences fonctionnelles d'une SRCF

Quelques remarques concernant les différentes informations

Important : Les spécifications des exigences fonctionnelles des SRCF sont la base de la conception du SRECS. En effet, elles vont être utiles, depuis la définition de l'architecture, en passant notamment par le choix du matériel, jusqu'à la validation des SRCF et du SRECS.

Condition d'activation de la SRCF

Cette information est importante pour les SRCF qui ne sont pas actives en permanence, par exemple uniquement dans un mode de marche particulier mis en service par un sélecteur de cycle.

Interface de la SRCF

Il n'est pas toujours évident de renseigner précisément les paramètres d'entrée et de sortie dès la spécification fonctionnelle de la SRCF. Certains renseignements devront alors être précisés au cours de la phase de conception du SRECS, par exemple lors du choix du matériel.

Néanmoins, il faudra s'assurer qu'aucun composant électrique, électronique et électronique programmable ne soit inséré entre l'interface de sortie de la SRCF (limite du SRECS) et l'actionneur (hors SRECS) de l'élément mobile sur lequel doit agir la SRCF.

Description de la SRCF

Elle doit faire clairement apparaître :

- le déclencheur de la fonction ou l'interface avec le déclencheur si celui-ci ne fait pas partie du SRECS. Dans le cas de la sollicitation d'un protecteur mécanique mobile par exemple, l'interface à prendre en compte sera l'information du capteur de position du protecteur),
- l'état du déclencheur qui active la SRCF (ouvert-fermé, libre-occulté),
- le résultat attendu, en étant le plus précis possible,

- l'organe ou l'interface, lorsque le SRECS ne réalise pas l'intégralité de la fonction de sécurité, sur lequel agit la SRCF.

Priorité par rapport à d'autres fonctions simultanées

Dans certains cas où plusieurs fonctions de commande « standard » ou SRCF, actives simultanément, pourraient engendrer des conflits au niveau des ordres de commande générés, il est nécessaire de définir des priorités au niveau de la spécification afin d'anticiper ces conflits. Des priorités spécifiées au niveau de la fonction de sécurité ne seront reprises au niveau de la SRCF que si elles sont traitées par le SRECS.

Autres SRCF agissant sur la même interface de sortie

Dans le cas ou plusieurs SRCF doivent agir sur la même interface de sortie, il est nécessaire de le préciser dés la spécification des SRCF concernées. Cette spécificité sera prise en compte lors de la conception de l'architecture du SRECS sous forme de blocs fonctionnels dédiés. En effet, une fonction logique devra être prévue pour permettre à ces SRCF d'agir conjointement sur cette interface.

Temps de réaction maximal de la SRCF

Il faut renseigner ce paramètre avec le temps de réaction maximal de la SRCF, vu du SRECS, compris entre les deux interfaces de la fonction. Ce temps doit être déduit du temps de réaction maximal attendu de la fonction de sécurité, toutes énergies confondues.

Fréquence de fonctionnement

La fréquence de fonctionnement, ou de sollicitation de la SRCF, doit être évaluée compte tenu de l'usage normal de la machine. Certaines SRCF sont sollicitées cycliquement (cas par exemple d'une barrière immatérielle d'une presse travaillant au coup par coup ; la barrière est franchie à chaque cycle pour retirer la tôle), d'autres beaucoup moins fréquemment.

Réaction aux fautes

Il faut détailler le comportement attendu de la SRCF en présence d'un dysfonctionnement dans son traitement. Il faut également s'intéresser aux autres contraintes, par exemple les conditions de redémarrage d'une machine suite à une détection d'anomalie ayant eu pour effet de commander un arrêt.

Conditions d'ambiance

Les contraintes liées à l'environnement de la machine doivent être détaillées afin de prendre les mesures adéquates au niveau de la conception et la réalisation du SRECS. Il s'agit par exemple de la température, l'humidité, les poussières, les vibrations et autres nuisances. Lorsqu'elle existe, ces préconisations sont généralement tirées de la norme de type C correspondant à la machine à concevoir.

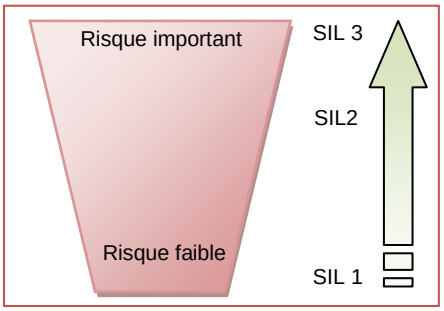
Taux de cycles de manœuvres, catégorie d'utilisation pour les dispositifs électromécaniques

Il est très rare de pouvoir renseigner ces paramètres dès la spécification fonctionnelle de la SRCF, car ces renseignements sont techniques et dépendent du matériel mis en œuvre. Ils pourront être précisés au cours de la phase de conception du SRECS.

7.3 Spécifications des exigences d'intégrité de sécurité des SRCF

La norme NF EN 62061 spécifie les exigences d'intégrité de sécurité en termes de SIL.

Rappel : L'intégrité de sécurité est le moyen qui permettra de satisfaire les objectifs fixés relativement à la sécurité fonctionnelle d'une entité. Cette intégrité de sécurité est quantifiée en 3 niveaux, de 1 à 3, lorsqu'elle est associée à la réduction du risque « machines ». Le comportement d'une SRCF de SIL 3 est plus sûr, vis-à-vis des conséquences d'éventuelles défaillances aléatoires ou systématiques, que celui d'une SRCF de SIL 1.



Lors de la conception du SRECS, les mesures mises en œuvre devront permettre d'atteindre au moins le SIL requis de chacune des SRCF.

Attribution d'un SIL en suivant une norme « produit »

Lorsque le concepteur choisit de suivre une norme « produit », appelée également norme de type « C » dans le domaine des machines et que celle-ci spécifie un SIL requis pour une SRCF, celui-ci est imposé et ne doit pas être remis en cause.

Attribution d'un SIL requis en suivant l'exemple de méthodologie de ***l'annexe A*** de la norme NF EN 62061

Dans le cas où il n'existe pas de norme produit attribuant un SIL requis à une SRCF, la norme NF EN 62061 préconise une méthode dans son ***annexe A***. Une estimation des risques détermine le niveau de contribution du SRECS vis-à-vis des risques à couvrir. Cette estimation ne se substitue pas à l'évaluation des risques « amont » réalisée au niveau de la machine pour déterminer les moyens de protection à mettre en œuvre. Cependant, elle en reprend les paramètres communs tels que la gravité du dommage par exemple.

Important : Une fois le SIL requis déterminé, il n'est plus possible de le modifier en cours de conception du SRECS mais il faut en assumer les conséquences, en particulier les mesures associées pour le respecter. Il faut donc apporter une grande attention à la phase de détermination du SIL requis.

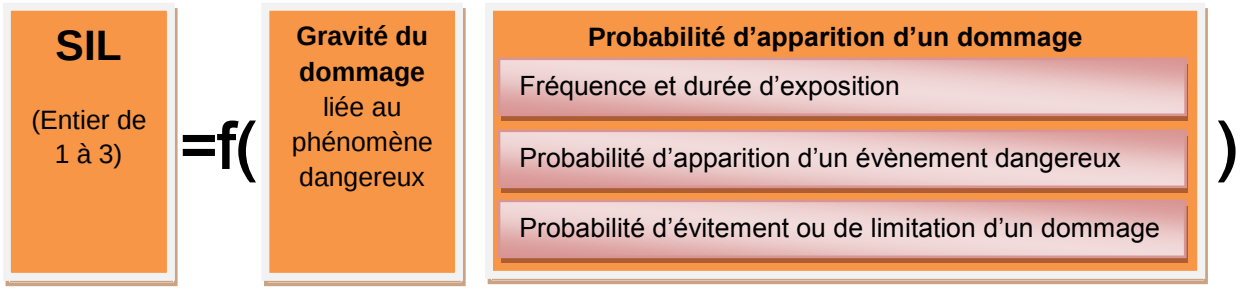


Figure 5 : Paramètres utilisés dans l'estimation du risque

7.4 Conception d'une SRCF

Le concepteur, qui a procédé aux phases décrites précédemment, doit déterminer les différentes parties matérielles dont il a besoin pour réaliser les SRCF. La norme lui préconise de procéder par itérations successives, en commençant par une décomposition des SRCF en « blocs fonctionnels », qui seront ensuite attribués à des « sous-systèmes ». Il doit mener cette réflexion jusqu'à un niveau lui permettant d'attribuer à chacun de ces sous-systèmes, un matériel du commerce directement adapté aux besoins exprimés ou une partie matérielle qu'il aura à concevoir.

7.4.1 Analyse/décomposition d'une SRCF en blocs fonctionnels

Tout d'abord la SRCF doit être analysée du point de vue fonctionnel, sans sauter d'étapes et sans passer trop vite à un assemblage de « composants ». La SRCF doit être décomposée en une structure de blocs fonctionnels (***§ 6.6.2.1.1 et 6.6.2.1.2***) de telle manière que la défaillance de chacun des blocs fonctionnels entraîne une défaillance de la SRCF. Le respect de cette exigence est impératif pour être en mesure d'utiliser les formules simplificatrices proposées par la norme pour les évaluations probabilistes.

Cette structure doit être décrite pour chaque SRCF et doit permettre d'en satisfaire toutes ses spécifications. Elle ne doit pas inclure de bloc fonctionnel participant aux fonctions de diagnostic ; lorsque celles-ci sont nécessaires, elles seront traitées séparément des SRCF (***§ 6.6.2.1.1 - Note 3***).

La forme la plus rationnelle se décline en au moins trois blocs fonctionnels. Cependant, la norme ne fixe pas le nombre de blocs fonctionnels, car il peut être nécessaire d'en utiliser plus ou moins.

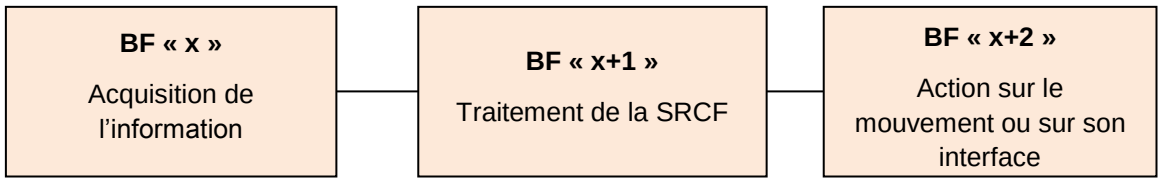


Figure 6 : Exemple de découpage en blocs fonctionnels d'une SRCF

Chaque bloc fonctionnel doit être spécifié en termes d'exigences fonctionnelles propres à ce bloc (par exemple les informations d'entrée, la logique interne et les informations de sortie du bloc) et d'exigences d'intégrité de sécurité communes à toute la SRCF (***§ 6.6.2.1.6***).

Chaque BF doit être identifié (par ex. par un N°) et la SRCF à laquelle il participe doit être facilement identifiable.

La décomposition en blocs fonctionnels s'effectue, autant que possible, sans a priori sur le matériel qui sera mis en œuvre, sauf pour certains composants qui sont imposés par le cahier des charges.

7.4.2 Attribution de sous-systèmes aux blocs fonctionnels d'une SRCF

Cette étape consiste à passer d'une structure en blocs fonctionnels à une structure en sous-systèmes en attribuant les blocs fonctionnels à des sous-systèmes (***§ 6.6.2.1.3***). Elle consiste à passer de la phase théorique de décomposition en blocs fonctionnels vers la phase d'attribution du matériel adéquat.

Il faut avant tout rappeler la définition d'un sous-système au sens de la norme (***§ 3.2.5***), qui le définit comme étant « *une entité de l'architecture générale du SRECS dans laquelle une défaillance d'un sous-système quelconque entraînera une défaillance d'une SRCF* ».

Chaque sous-système doit atteindre un SIL au moins équivalent à celui requis pour la SRCF concernée.

L'architecture du SRECS, et donc de chaque SRCF doit être documentée, par exemple sous une forme graphique, et décrire tous les sous-systèmes ainsi que les relations qui les lient (***§ 6.6.2.1.5***).

La norme impose qu'un bloc fonctionnel ne soit attribué qu'à un seul sous-système. Cependant, plusieurs blocs fonctionnels peuvent être attribués à un même sous-système (***§ 6.6.2.1.3***).Il faut bien se rappeler de cette possibilité, car pour ne pas dépasser la probabilité de défaillance dangereuse d'une SRCF imposée par son SIL requis, il faut souvent limiter le nombre de sous-systèmes utilisés ou mettre en œuvre des composants ayant une PFH_D faible. Les composants électroniques hautement intégrés, peu influencés par la fréquence de sollicitation de la SRCF ont généralement une PFH_D faible, ce qui n'est pas le cas, par exemple, pour la majorité des composants électromécaniques.

Chacun des sous-systèmes doit être choisi ou conçu pour pouvoir respecter :

- au moins le SIL requis pour la SRCF,
- et les spécifications fonctionnelles du bloc fonctionnel correspondant, tout en prenant en compte les spécificités du matériel utilisé pour le sous-système lui-même, ainsi que les caractéristiques des sous-systèmes qui ont des interactions avec lui (entrées/sorties, paramétrages, type de raccordement recommandé,…).

Note sur l'attribution des sous-systèmes

La norme ne préconise pas de méthode pour guider le concepteur dans l'attribution d'un même sous-système à un ou plusieurs blocs fonctionnels. A cette étape, le concepteur doit connaître (par expérience ou après recherche documentaire) les caractéristiques du matériel existant qui potentiellement répondrait aux spécifications des blocs fonctionnels auxquels ce matériel est destiné et au SIL requis pour la SRCF. Cette connaissance lui permettra de déterminer l'architecture en sous-systèmes la mieux adaptée. Dans le cas contraire, plusieurs itérations peuvent être nécessaires.

7.4.3 Anticipation de la structure et de la composition du SRECS pour une conception plus rationnelle des SRCF

Anticiper sur la structure et la composition du SRECS, notamment en faisant ressortir les relations entre les différentes SRCF, peut permettre de rationaliser la phase de conception des SRCF, en réduisant le nombre d'itérations dans cette phase. C'est le cas par exemple :

- si un même matériel est envisagé pour des SRCF de SIL différent, le choix s'orientera d'office vers un composant d'un SIL au moins égal au plus élevé parmi les SRCF,
- si le choix a priori est d'utiliser un APIdS pour le traitement logique des SRCF : la décomposition en blocs fonctionnels pourra s'effectuer avec un nombre de blocs fonctionnels réduit dès lors que ceux-ci sont destinés à être attribués au sous-système APIdS. En effet, ce genre de composant permet de réaliser de multiples fonctions logiques dans un même sous système.
- lorsque le concepteur a une idée préconçue d'un composant dédié à la sécurité qu'il veut utiliser et que ce composant intègre des fonctions de sécurité dont les spécifications fonctionnelles sont déterminés (bloc logique, module logiciel constructeur d'un APIdS,…) : il est alors conseillé de prendre connaissance de ses spécifications avant de commencer la conception des SRCF, pour en tenir compte lors de cette phase.

8 Spécifications et choix / conception des sous-systèmes (*§ 6.7*)

Pour un sous-système donné, le concepteur aura le choix entre utiliser un composant du commerce répondant seul à ses spécifications ou concevoir un sous-système par assemblage de plusieurs composants.

8.1 Informations nécessaires pour le choix ou la conception d'un sous-système

Il faut, dans un premier temps, définir les informations nécessaires pour le choix ou la conception du sous-système, ensuite recueillir l'ensemble des informations nécessaires à son évaluation et à son usage, soit auprès du fabricant du ou des composants attribué(s) au sous-système ou du concepteur du sous-système. Ces informations comprennent :

- Le SIL requis du sous-système qui devra être supérieur ou égal au plus élevé des SIL requis revendiqué par les SRCF qui utilisent ce sous-système (***§ 6.7.2.2- i***).
- La spécification fonctionnelle des fonctions et interfaces du sous système (***§ 6.7.2.2- a***)
    - Une description fonctionnelle du sous-système. Un sous-système pouvant traiter plusieurs BF différents, il faut penser à respecter toutes les spécifications fonctionnelles des BF concernés.
    - Les caractéristiques principales, d'entrée, de sortie, de temps de réponse,...
    - Un rappel des conditions environnementales (***§ 6.7.2.2- h***) (ex. température, humidité, vibrations,…) qu'il convient de respecter.
    - Eventuellement la probabilité de défaillance dangereuse par heure [k] **PFH_D** à ne pas dépasser, par exemple si le concepteur connaît la **PFH_D** des autres sous-systèmes et qu'il a par déduction une valeur maximale à ne pas dépasser pour respecter le SIL requis de la SRCF.

Elles sont récapitulées dans les lignes 1 à 8 du Tableau 2. Pour qu'un sous-système puisse être retenu définitivement, il faut qu'il réponde aux caractéristiques définies ci-avant et que les informations listées dans la dernière colonne du Tableau 2 soient fournies, conformément au ***§ 6.7.2.2*** de la norme.

Il s'agit d'informations, qui intègrent le rappel de certaines hypothèses ou caractéristiques prises en considération lors de la conception des sous-systèmes par leur concepteur.

Informations			
N°	Type	**Requises** pour le choix ou la conception d'un SS	**A fournir** par le fabricant/concepteur du SS (données réelles détaillées)
1	SIL	Minimum requis	Maxi revendiqué (***§6.7.2.2- g, h et i***),
2	Fonction(s)	Description fonctionnelle du sous-système	Description
3	Entrée(s)	Caractèristiques des interfaces du sous-système	Caractéristiques détaillées
4	Sortie(s)	caractèristiques des interfaces du sous-système	Caractéristiques détaillées
5	Temps de réponse	Valeur maximale requise	Valeur maximale revendiquée (cf. P1)
6	Conditions environnementales (ex. température, humidité, vibrations,…)	Minimum requis	Maximal revendiqué
7	Fréquence de fonctionnement du sous-système	Suivant spécification de la ou des SRCF auquel le SS est attribué	Maximal revendiqué

Informations			
N°	Type	**Requises** pour le choix ou la conception d'un SS	**A fournir** par le fabricant/concepteur du SS (données réelles détaillées)
8	PFH_D	A spécifier éventuellement, mais dans la limite de la valeur autorisée pour le SIL requis	Valeur
9	Environnement et conditions de fonctionnement qu'il convient d'observer (***§6.7.2.2- c***) (afin de maintenir la validité des taux de défaillance estimés dus aux défaillances aléatoires de matériel)	Sans objet	Description (cf. P2)
10	Durée de vie du sous-système qu'il convient de ne pas dépasser (***§ 6.7.2.2- c***) (afin de maintenir la validité des taux de défaillance estimés dus à des défaillances aléatoires du matériel)	Sans objet	Valeur (cf. P2)
11	Tests et/ou exigences de maintenance à respecter (***§ 6.7.2.2- d***)	Sans objet	Description (cf. P3)
12	Diagnostic(s) qu'il est prévu de confier à un autre sous-système (***§ 6.7.2.2- e***)	Sans objet	Description
13	Limitations afin d'éviter les défaillances systématiques (***§ 6.7.2.2- h***)	Sans objet	Description (cf. P4)
14	Les informations nécessaires à l'identification de la configuration du matériel et du logiciel (***§ 6.7.2.2- j***)	Sans objet	Description
15	Probabilité d'erreur de transmission dangereuse dans le cas de processus de communication de données numériques (***§ 6.7.2.2- k***)	Sans objet	Valeur

Tableau 2 : Récapitulatif des caractéristiques utiles pour un sous-système

- Cf. P1 – Temps de réponse

Le fabricant doit fournir cette valeur ou les moyens de la déterminer comme c'est le cas pour un APIdS pour lequel le temps de réponse dépend de certains paramètres liés au temps d'exécution des fonctions à traiter. Il est préférable de choisir un matériel pour lequel son fabricant est capable de fournir des outils - simples à utiliser et ergonomiques - pour évaluer « a priori » son temps de réponse maximal et pour vérifier « a posteriori » le temps de réponse maximal obtenu à partir des données et paramètres réels utilisés. L'idéal serait de disposer d'un composant, capable de fournir automatiquement la valeur de son temps réponse maximal, l'ayant lui-même déterminé suivant les caractéristiques et/ou le paramétrage réel du matériel mis en œuvre.

- Cf. P2 – Environnement, conditions de fonctionnement et durée de vie

Ces informations sont surtout importantes pour les sous-systèmes intégrant des composants électromécaniques. Par exemple, lors de la détermination du taux de défaillance pris en compte pour la détermination du SIL d'un sous-système, le nombre d'opérations par heure des composants est pris en compte. Les conditions de fonctionnement qu'il convient

d'observer ne doivent pas aller au-delà de cette valeur, sinon le SIL annoncé par le concepteur du sous-système n'est plus garanti.

- cf. P3 - Tests et/ou exigences de maintenance à respecter

C'est le cas par exemple lorsque la PFH_D est largement dépendante des tests périodiques (c'est-à-dire des essais prévus pour révéler les défauts non détectés par les fonctions de diagnostic – voir avant-propos de la norme NF EN 62061).

- cf. P4 - Limitations à observer afin d'éviter les défaillances systématiques

Par exemple, pour tenir compte des caractéristiques d'entrée/sortie du sous-système, leurs éventuelles spécificités de raccordement,…

8.2 Choix d'un composant « type » du commerce pour l'intégralité d'un sous système (*§ 6.7.3*)

Un composant « type » est un composant qui, d'après les informations fournies par son fabricant, répond seul aux spécifications du sous-système.

Deux cas peuvent se présenter pour un composant « type » :

- un composant tel qu'un APIdS ou un module de sécurité du commerce, conçu et fabriqué pour pouvoir assurer des fonctions de sécurité et dont les caractéristiques de SIL et de PFH_D sont fournies,
- un composant pour lequel le SIL (dont la PFH_D) n'est pas fourni, mais les données pour le déterminer sont fournies. Il s'agit par exemple d'un composant électromécanique, dont le SIL va dépendre des spécifications du sous système auquel il va être affecté. Pour déterminer ce SIL, le concepteur du SRECS doit tenir compte de :
  - la fréquence de fonctionnement du sous-système par exemple,
  - et de l'influence des modes de défaillances possibles du composant sur le comportement de la ou des SRCF concernée(s).

  Lorsque le concepteur doit déterminer lui-même le SIL du sous-système (dont la PFH_D), il lui faudra recueillir les informations listées dans le Tableau 2. Pour déterminer le SIL auquel peut prétendre ce sous-système, il faut mener les analyses décrites en § 8.4 de ce document.

Il arrive parfois qu'un composant du commerce remplisse une fonction équivalente à celle qui est spécifiée pour le sous-système à réaliser, mais d'une manière différente de celle qui a été spécifiée. Il faut alors reprendre l'analyse fonctionnelle pour harmoniser les spécifications du bloc fonctionnel et du sous-système concernés avec celles du composant retenu.

La norme ne traite pas du SIL des composants complexes, mais préconise que celui-ci soit déterminé conformément aux prescriptions des CEI 61508-2 et CEI 61508-3 pour autant qu'elles soient applicables (***§ 6.7.3.2*** *de la norme NF EN 62061*).

8.3 Conception d'un sous-système « particulier »

Dès que le besoin de développer une architecture de sous-système, par association d'éléments de sous-systèmes apparaît, il faut alors respecter les préconisations du ***§ 6.7.4*** de la norme qui fixe les règles correspondantes.

La ***figure 4*** du ***§ 6.7.4.3*** de la norme, rappelée ci-après, décrit le processus à suivre et illustre les diverses possibilités de conception et de développement des sous-systèmes.

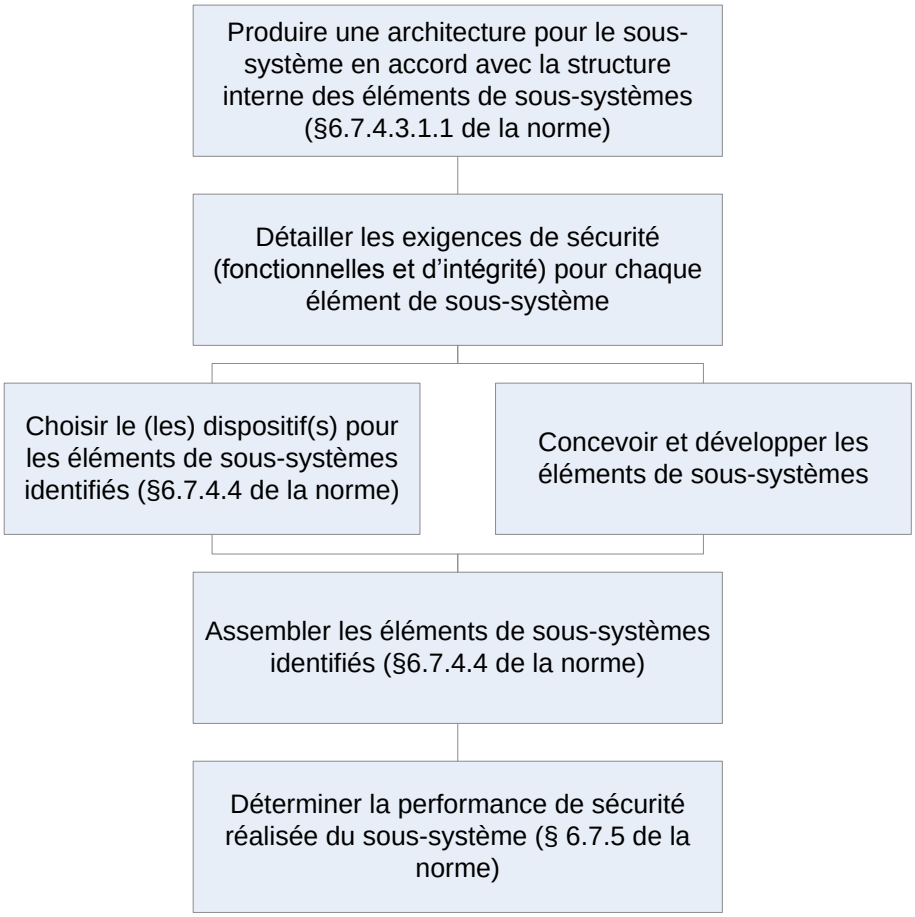


Figure 4 de la norme – Diagramme de conception et développement d'un sous système

Rappel : Un élément de sous-système est « *une partie d'un sous-système comprenant un composant unique ou un quelconque groupe de composants* » (***§ 3.2.6***).

La conception d'un sous-système « particulier » s'applique, par exemple, pour réaliser un sous-système d'acquisition d'information (dispositif de verrouillage électrique d'un protecteur) ou un sous-système d'interface de sortie (pour commander un circuit de puissance ou un circuit de commande utilisant une énergie autre qu'électrique).

Important : Les préconisations de la norme NF EN 62061 ne sont applicables qu'aux sous-systèmes de faible complexité, les sous-systèmes « complexes » devant suivre les règles de la norme CEI 61508.

Choix de l'architecture d'un sous-système (*§ 6.7.4.3*)

La norme NF EN 62061 envisage 4 types d'architectures « A » à « D », pour la conception d'un sous-système, qui se distinguent par leur tolérance aux anomalies du matériel et par la présence ou non de fonction de diagnostics. Elle ne préconise pas de méthode pour le choix direct de l'architecture qui conviendrait le mieux. La démarche préconisée par la norme étant itérative elle permet de partir d'un sous-système de conception simple, par exemple d'architecture « A », pour ensuite le faire évoluer autant que cela soit nécessaire, jusqu'à aboutir par exemple à une architecture « C » ou d'une architecture « B » vers « D » pour atteindre le SIL requis du sous-système.

Un concepteur « expérimenté » passera certainement vite au choix de l'architecture adéquat sans procéder à toutes les itérations.

Les représentations logiques des différentes architectures de la norme sont rappelées ci-dessous accompagnées de précisions complémentaires.

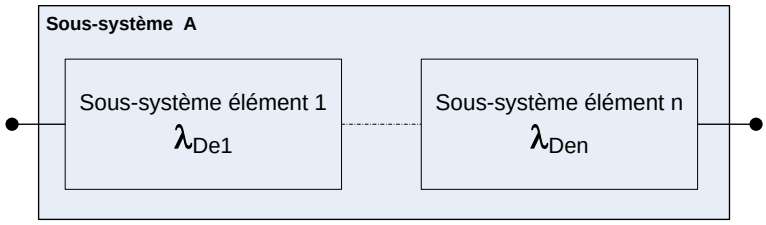


Figure 7 : Représentation logique d'un sous système de type A

Pour réaliser ce sous-système, plusieurs éléments de sous-système (1 à n) sont nécessaires pour assurer sa spécification fonctionnelle. Dans cette architecture de type A, toute défaillance dangereuse d'un élément de sous-système entraîne une défaillance de la SRCF.

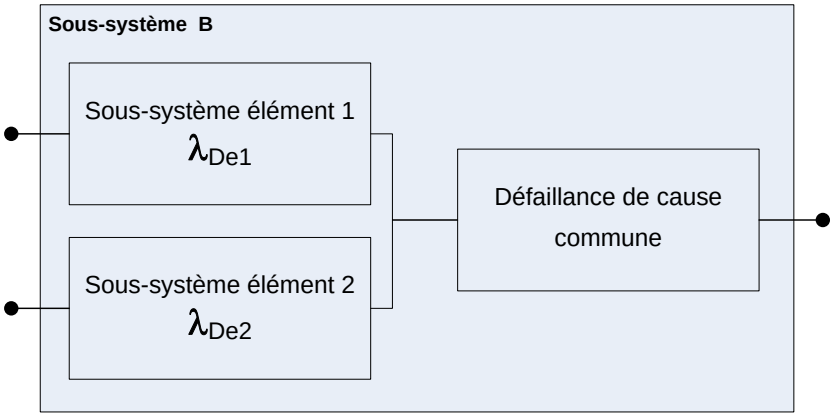


Figure 8 : Représentation logique d'un sous système de type B

Cette architecture est utilisée en cas de redondance (homogène ou hétérogène) d'un élément de sous-système. Dans cette architecture de type B, une défaillance dangereuse unique de tout élément du sous-système n'entraîne pas une défaillance de la SRCF.

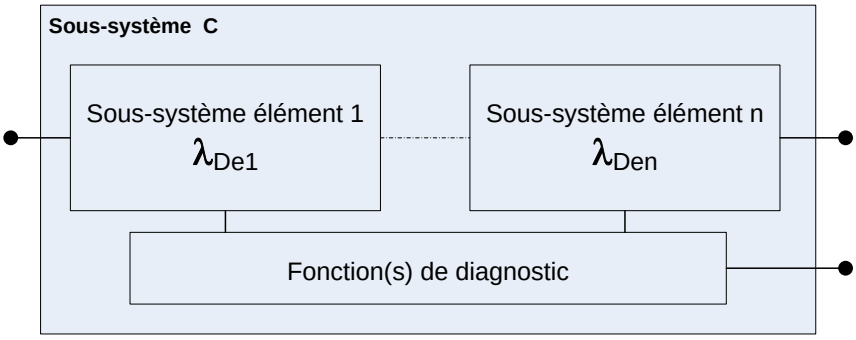


Figure 9 : Représentation logique d'un sous-système de type C

Pour réaliser ce sous-système, plusieurs éléments de sous-système (1 à n) sont nécessaires pour assurer sa spécification fonctionnelle et une fonction de diagnostic est nécessaire. Dans cette architecture de type C, toute défaillance dangereuse non détectée, d'un élément de sous-système, conduit à une défaillance dangereuse de la SRCF. Lorsqu'une défaillance dangereuse d'un élément de sous-système est détectée, la(les) fonction(s) de diagnostic déclenche(nt) une fonction réaction à la défaillance dangereuse.

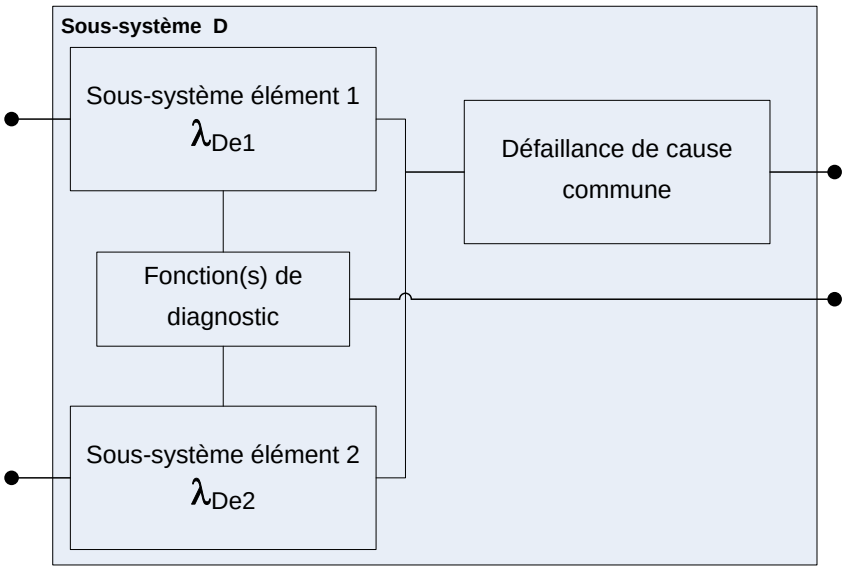


Figure 10 : Représentation logique d'un sous-système de type D

Cette architecture est utilisée en cas de redondance (homogène ou hétérogène) d'un élément de sous-système nécessitant une fonction de diagnostic. Dans cette architecture de type D, une défaillance dangereuse unique de tout élément du sous-système n'entraîne pas une défaillance de la SRCF. Lorsqu'une défaillance dangereuse d'un élément de sous-système est détectée, la(les) fonction(s) de diagnostic déclenche(nt) une fonction réaction à la défaillance dangereuse.

Note : Les représentations logiques des architectures « A » à « D » ne doivent pas être interprétées comme leur réalisation physique.

Le ***§ 6.7.4.3.1*** décrit le processus de conception de l'architecture d'un sous-système. Pour déterminer le SIL auquel peut prétendre un sous-système, il faut mener les analyses décrites en § 8.4.de ce document.

8.4 Détermination du SIL pouvant être revendiqué par un sous-système

Pour atteindre un SIL requis, un sous-système est soumis au respect :

- des contraintes architecturales, traitées en § 8.4.1,
- des probabilités de défaillance dangereuse par heure (PFHD) définies dans le tableau 3 de la norme NF EN 62061 et traitées en § 8.4.2,
- des exigences d'intégrité de sécurité systématique, traitées en § 8.4.3.

Ces différents critères doivent être, suivant les cas, définis, estimés ou calculés par le concepteur. La Figure 11 fait le bilan des éléments nécessaires pour la détermination du SIL d'un sous-système.

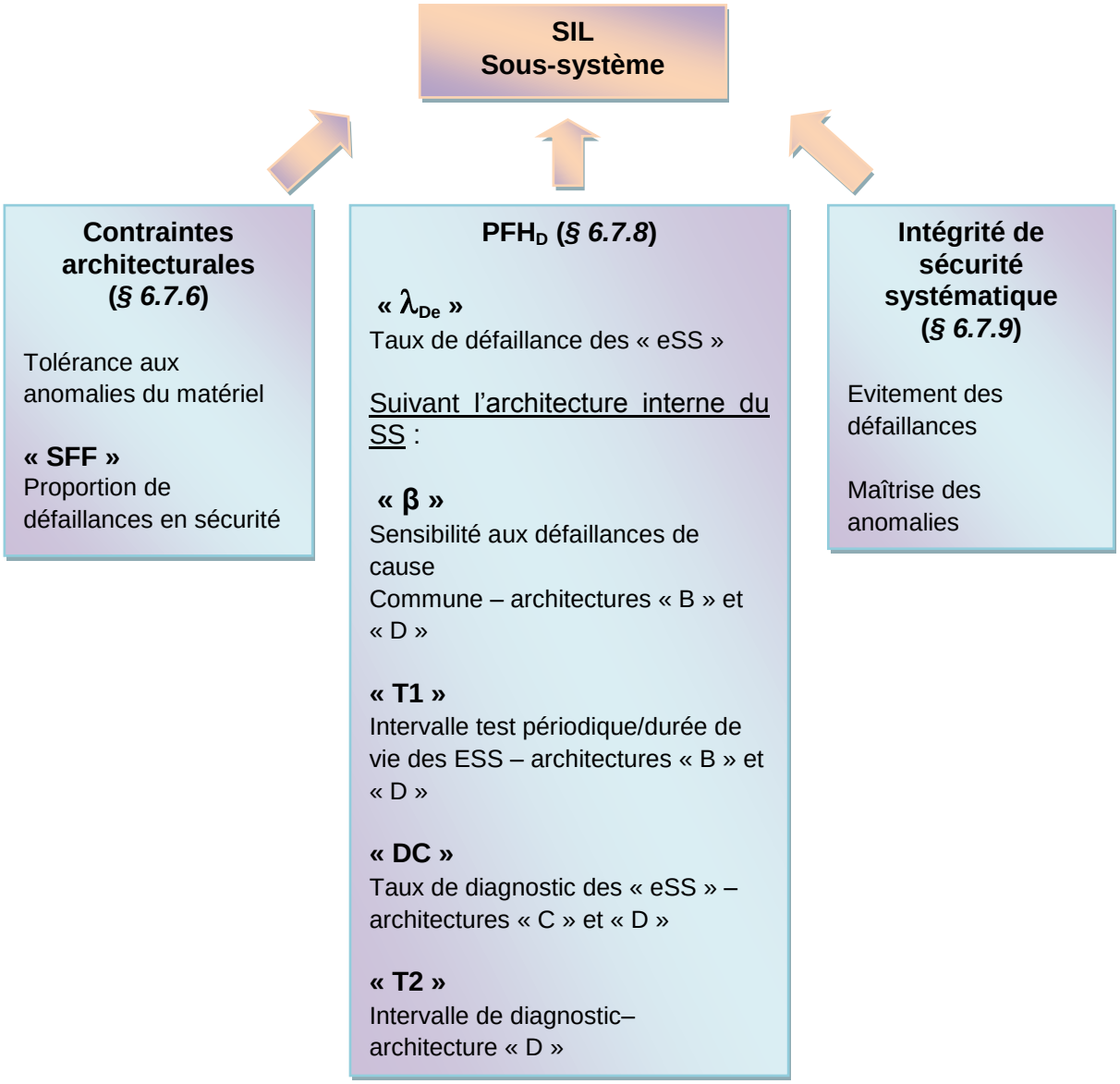


Figure 11 : Bilan des éléments nécessaires pour la détermination du SIL d'un sous-système

Note : La norme NF EN 62061 : 2005 comporte une erreur dans sa version française concernant la définition du paramètre T2. La définition donnée dans ce document est issue de la version en langue anglaise.

8.4.1 Détermination du SIL vis-à-vis des contraintes architecturales du sous-système (*§ 6.7.6*)

Ce SIL tient compte de :

- la tolérance aux anomalies du matériel,
- et de la proportion de défaillances en sécurité du sous-système « SFF[5] ».

a) Tolérance aux anomalies du matériel

Le ***§ 6.7.6.1*** décrit comment évaluer le comportement du sous-système en présence d'une anomalie. En résumé, une tolérance aux anomalies du matériel de valeur « N » signifie que N+1 anomalies sont susceptibles de provoquer la perte de la SRCF.

[5] SFF : Safe Failure Fraction

Important : Lors de la détermination de la tolérance aux anomalies, il ne faut pas prendre en compte les mesures pouvant maîtriser l'effet d'une anomalie, donc ne pas prendre en compte l'effet d'une fonction de diagnostic [i] par exemple.

Il faut donc recenser les modes de défaillances possibles du sous-système et le cas échéant de ses éléments de sous-système puis analyser leurs conséquences sur le comportement de la SRCF.

b) Proportion de défaillances en sécurité « SFF »

Rappel : La SFF représente la « *proportion du taux global des défaillances d'un sous-système qui n'entraînent pas une défaillance dangereuse* ».

C'est un paramètre à estimer suivant toutes les préconisations du ***§ 6.7.7*** (y compris l'exception mentionnée dans ce ***§*** de la norme) en prenant notamment en compte les modes de défaillances répertoriés du (des) composant(s) utilisé(s) pour le sous-système ou les éléments de sous-système. Normalement, leur fabricant devrait être en mesure de fournir les modes de défaillances possibles. Dans le cas contraire, ***l'annexe D*** de la norme cite des exemples de rapports de modes de défaillance pour des composants électriques/électroniques.

Il faut déterminer le comportement de la SRCF pour chacune des défaillances du ou des composant(s) et les classifier de la manière suivante :

- les défaillances aux conséquences potentiellement dangereuses, qui peuvent empêcher la SRCF d'assurer sa fonction. Elles sont comptabilisées par :
    - le taux de défaillances dangereuses « λ_D » qui regroupe l'ensemble des défaillances dangereuses, détectées et non détectées par une fonction de diagnostic,
    - le taux de défaillances dangereuses détectées « λ_{DD} » qui comprend uniquement celles qui sont détectées par une fonction de diagnostic.
- les autres défaillances qui n'affectent pas la SRCF de manière dangereuse. Elles sont à comptabiliser dans le taux de défaillance en sécurité « λ_S ».

Le calcul de la proportion de défaillance en sécurité « SFF » s'effectue pour la totalité du sous-système en prenant en compte tous les éléments de sous-systèmes.

La SFF peut être calculée en utilisant la formule du ***§ 3.2.42*** :

$$\left(\sum\lambda_S + \sum\lambda_{DD} \right) / \left(\sum\lambda_S + \sum\lambda_D \right)$$

A cette étape du cycle de conception d'un sous-système, les valeurs des taux de défaillance (λ) ne sont pas connues et la formule précédente ne peut pas être utilisée en l'état. Comme les données fournies par les fabricants sont exprimées en proportion de défaillance (%d) (en sécurité, dangereuse ou détectée) par rapport au nombre total de défaillances, la SFF peut être calculée de la façon suivante :

SFF (à exprimer en %) $= [\sum \%d_S + \sum \%d_{DD}] / [\sum \%d_S + \sum \%d_D]$

Où

$\%d_S$ est le pourcentage de défaillance en sécurité par rapport au nombre total de défaillances.

$\%d_D$ est le pourcentage de défaillance dangereuse par rapport au nombre total de défaillances.

$\%d_{DD}$ est le pourcentage de défaillance dangereuse qui est détecté par les fonctions de diagnostic par rapport au nombre total de défaillances.

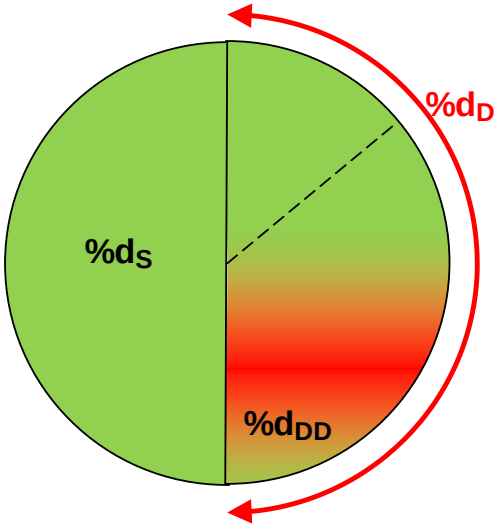


Figure 12

Ces différents paramètres peuvent être représentés comme dans l'exemple de la Figure 12.

Note : Les défaillances dangereuses non détectées n'étant pas utilisées dans les calculs, aucun symbole ne leur est attribué dans ce document.

c) Détermination du SIL vis-à-vis des contraintes architecturales

Le ***tableau 5*** de la norme permet de déterminer le SIL pouvant être revendiqué par une SRCF en fonction de la tolérance aux anomalies « N » et la proportion de défaillance en sécurité « SFF » des sous-systèmes qui la composent.

Pour les sous-systèmes conçus suivant la norme ISO 13849-1 :1999, le ***§ 6.7.6.5*** de la norme NF EN 62061 permet de déduire directement le SIL maximal pouvant être revendiqué, par l'intermédiaire de son ***tableau 6***.

Les résultats peuvent être consignés dans un tableau récapitulatif, tel que l'exemple proposé dans le Tableau 3, prédisposé pour être complété ultérieurement avec les autres paramètres à déterminer pour le sous-système.

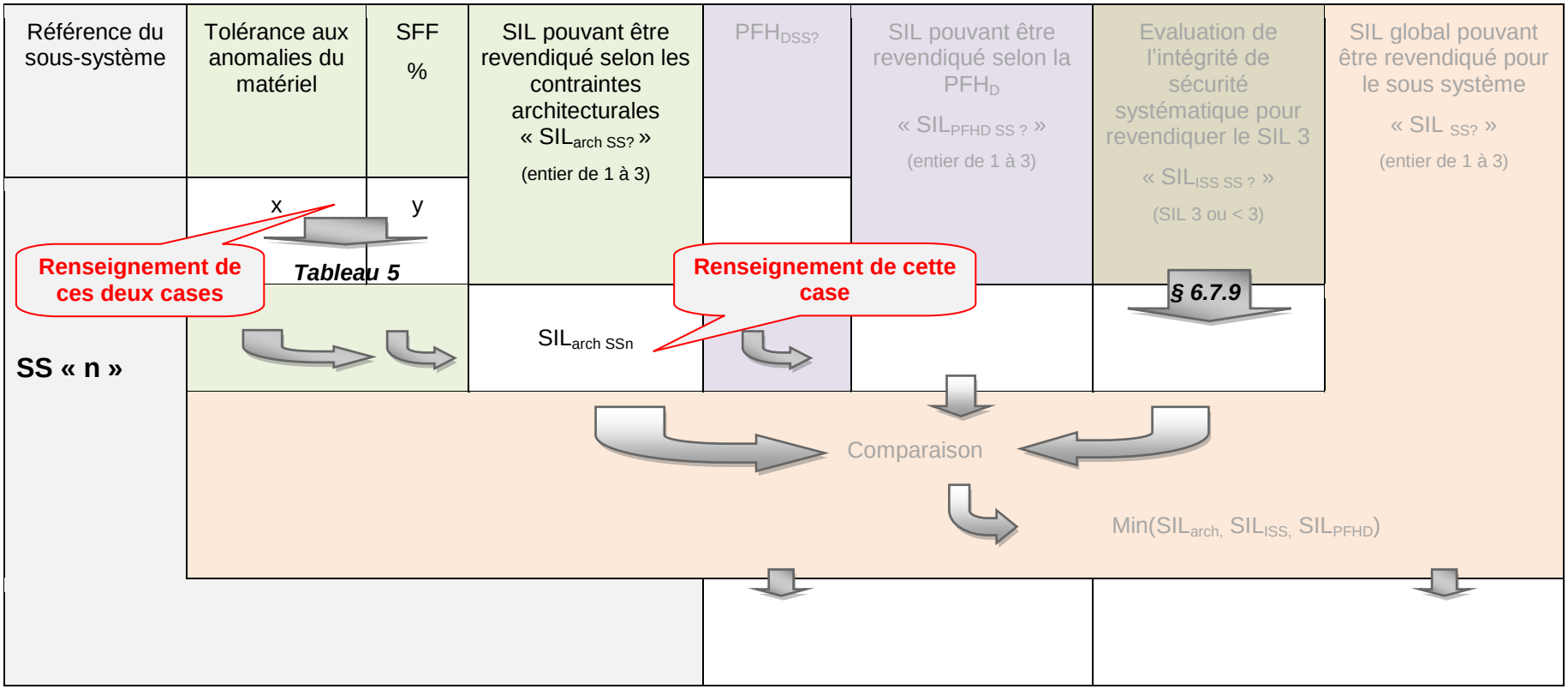


Tableau 3 : Récapitulatif du SIL pouvant être revendiqué pour un sous-système SS « n », renseigné selon les contraintes architecturales

8.4.2 Détermination du SIL vis-à-vis de la PFHD du matériel (§ 6.7.8)

Evaluation de la PFH_D pour des architectures basiques de sous-systèmes.

Parmi ses préconisations, la norme décrit, en ***§ 6.7.8.2.1***, pour les architectures basiques « A » à « D », une approche simplifiée pour l'estimation de la probabilité de défaillance dangereuse aléatoire du matériel des sous-systèmes. Ce type de défaillance est généralement dû à une panne ou une dégradation du matériel utilisé, un collage d'un contact électromécanique par exemple.

Pour chacune des architectures « A » à « D », évoquées en § 8.3 de ce document, une formule spécifique de calcul de la PFH_D est préconisée par la norme.

Une des difficultés actuelle réside dans le fait que les fabricants de matériels n'ont pas encore toutes les données nécessaires, concernant leurs composants, pour permettre d'effectuer les calculs de PFH_D définis dans cette norme. Il est conseillé de choisir des composants pour lesquels le fabricant est en mesure de fournir ces données, c'est le gage d'obtenir des résultats représentatifs du matériel réellement utilisé. Les valeurs par défaut, telles que celles qui sont fournies dans ***l'annexe D*** de la norme NF EN 62061, ne doivent être utilisées qu'en dernier recours.

Approche simplifiée pour l'estimation de la contribution des défaillances de cause commune (*§ 6.7.8.3*)

Le ***§ 6.7.8.3*** décrit les préconisations correspondantes. Il propose d'utiliser ***l'annexe F*** de la norme, pour déterminer le facteur « **β** » permettant de quantifier la sensibilité aux défaillances de cause commune d'un sous-système.

Les différents paramètres utiles pour les calculs et quelques formules pour les déterminer sont précisés dans le Tableau 4.

Abréviation	Dénomination	Commentaire	Origine F : Fabricant C : Calcul
λ_{De}	Taux de défaillance **dangereuse** d'un élément de sous-système Unité : défaillance par heure	Pour les composants électroniques : λ_{De} = 1/MTTFd	**C**
		Pour les composants électromécaniques : λ_{De} = 0,1xC/B10d	**C**
Suivant le type d'architecture « A » à « D » retenue			
β	Sensibilité aux défaillances de cause commune du sous-système	Voir méthodologie de ***l'annexe F (****informative)* de la norme	**C**
T1	Intervalle de test périodique ***(§ 3.2.37)*** du sous-système ou la durée de vie suivant la plus faible Unité : heure	(***§ 6.7.8.2.5***) L'intervalle de test périodique est fixé par le concepteur du sous système La durée de vie est une donnée du fabricant de l'élément de sous-système	**F/C**

Abréviation	Dénomination	Commentaire	Origine F : Fabricant C : Calcul
DC[6]	Couverture des diagnostics de l'élément de sous-système, lorsqu'une fonction de diagnostic est implantée	**DC** = λ_{DDe} / λ_{De} λ_{DDe} : Taux de défaillance dangereuse de l'élément de sous-système qui est détecté par les fonctions de diagnostic λ_{De} : Taux de défaillance dangereuse de l'élément de sous-système.	**C**
T2	Intervalle des diagnostics de l'élément de sous-système, lorsqu'une fonction de diagnostic est implantée. Unité : heure	(***§ 6.7.8.2.5***) Note : La norme NF EN 62061 : 2005 comporte une erreur dans sa version française concernant la définition du paramètre **T2**. La définition donnée dans ce document est issue de la version en langue anglaise	**C**
Formules pouvant être utiles pour la détermination des paramètres ci-dessus			
λ**e**	Taux de défaillance d'un élément de sous-système Unité : défaillance par heure	(***§ 6.7.8.2.1 – Note 3***) λ**e** = λ_{Se} + λ_{De} λ_{Se} : Taux de défaillance en sécurité de l'élément de sous-système λ_{De} : Taux de défaillance dangereuse de l'élément de sous-système	**C**
		Pour les composants électroniques (***§ 6.7.8.2.1 – Note 2***) : λ**e** = 1/MTTF	**C**
		Pour les composants électromécaniques (***§ 6.7.8.2.1 – Note 2***) : λ**e** = 0,1xC/B10	**C**
C	Nombre de cycles de manœuvres par heure	Dépend de la fréquence de sollicitation de la (des) SRCF mettant en œuvre le sous-système	**C**
MTTF	Durée moyenne de fonctionnement de l'élément avant défaillance (en heures)		**F**

[6] DC : Diagnostic Coverage

Abréviation	Dénomination	Commentaire	Origine F : Fabricant C : Calcul
MTTFd	Durée moyenne de fonctionnement de l'élément avant défaillance dangereuse (en heures)	Des valeurs typiques de MTTFd sont également disponibles dans les annexes C et D de la norme ISO 13849-1 :2006	**F/C**
B10	Nombre moyen de manœuvres au bout duquel 10 % des composants testés auront eu une défaillance	La définition donnée en ***§ 6.7.2.2.b – Note 1 et 6.7.4.4.2.c – Note 1*** mentionne un temps au lieu d'un nombre de manœuvres	**F**
B10d	Nombre moyen de manœuvres au bout duquel 10 % des composants testés auront eu une défaillance dangereuse.	a) Définition en § C.4.2 de l'annexe C de l'ISO 13849-1 :2006 **b)** Peut être calculé à partir du B10, à l'aide de la proportion de défaillance dangereuse de l'élément de sous-système (eSS) $B10d = B10 / \%d_{De}$ $\%d_{De}$: pourcentage de défaillance dangereuse de l'eSS **c)** Des valeurs typiques sont disponibles dans le tableau C1 de l'annexe C de la norme ISO 13849-1 :2006	**F/C**

Tableau 4 : Récapitulatif des éléments à considérer pour le calcul de la PFH_D

Après avoir effectué le calcul de la PFH_D, il faut prendre connaissance du SIL maximal pouvant être revendiqué par le sous-système, en se basant sur les critères du ***tableau 3*** de la norme intitulé : *« Niveaux d'intégrité de sécurité : valeurs cibles des défaillances pour les SRCF* ».

Si le sous-système ne permet pas d'atteindre le SIL requis, il faut recommencer le cycle de conception du sous-système, par exemple, en choisissant du matériel plus fiable, en améliorant son architecture, sa tolérance aux anomalies, les fonctions de diagnostics, l'immunité aux défaillances de cause commune, ou en jouant sur les autres paramètres entrant dans le calcul de la PFH_D.

Les résultats peuvent être consignés dans un tableau récapitulatif tel que l'exemple représenté dans le Tableau 5.

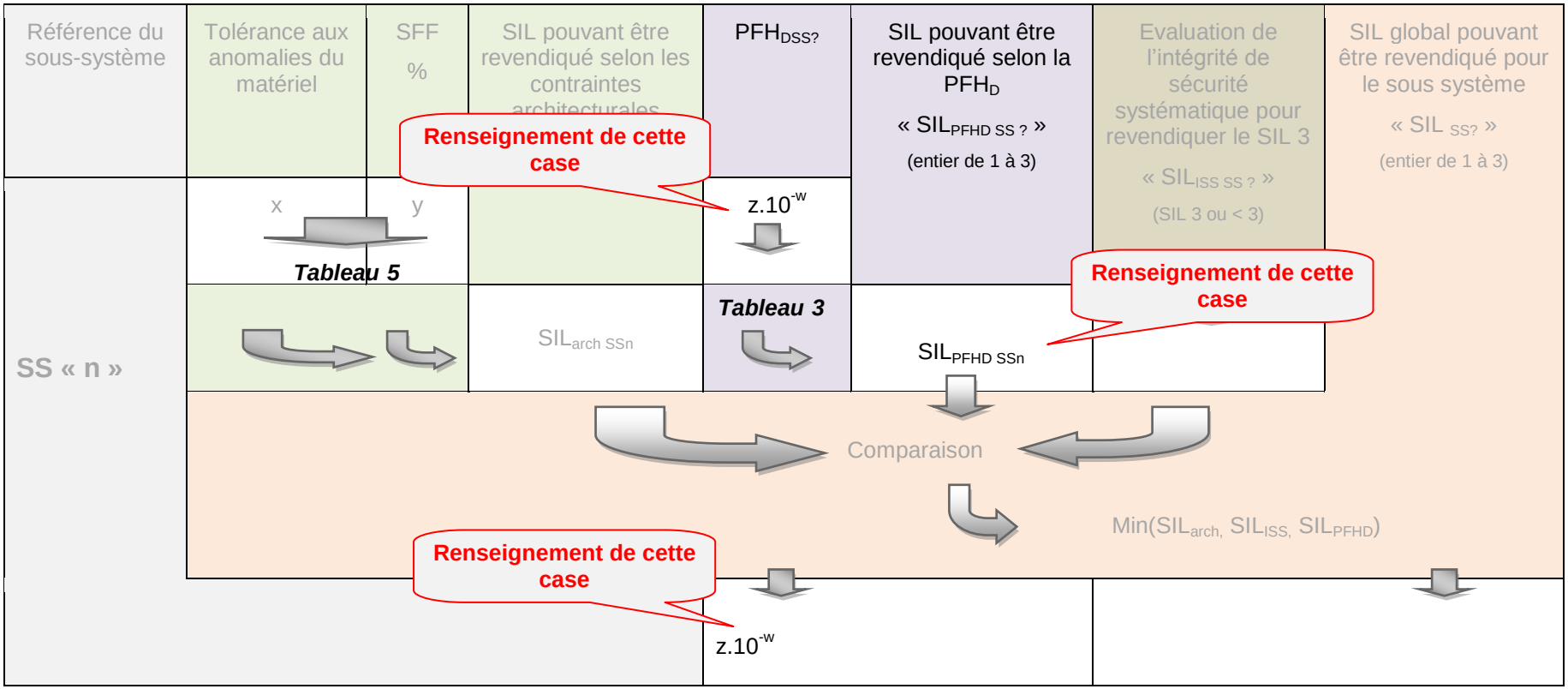


Tableau 5 : Récapitulatif du SIL pouvant être revendiqué pour un sous système SS « n », renseigné selon la PFH_D

8.4.3 Détermination du SIL vis-à-vis des exigences pour l'intégrité de sécurité systématique des sous-systèmes (§ 6.7.9)

Le ***§ 6.7.9*** de la norme n'apporte pas d'élément nouveau et ses préconisations visent le même objectif que le ***§ 6.4*** de la norme, concernant le SRECS, en les transposant au niveau du sous-système. Il est en effet logique que ce qui est requis pour le SRECS le soit également pour chacun des sous-systèmes qui le composent. Les commentaires et exemples du § 6 de ce document restent donc en grande partie valables pour la conception des sous-systèmes.

Le ***§ 6.7.9.1*** rappelle les règles de l'art dans la mise en œuvre de matériel d'automatisme pour que le matériel utilisé soit correctement choisi, assemblé, adapté à l'environnement, mais également pour s'assurer qu'une méthode et/ou des outils appropriés sont mis en œuvre par l'équipe de conception pour éviter les défaillances systématiques.

Le ***§ 6.7.9.2*** préconise des mesures pour maîtriser les anomalies systématiques.

Le respect des exigences des ***§ 6.7.9.1*** et ***6.7.9.2*** entraîne la possibilité pour le sous-système de revendiquer, vis-à-vis de la prise en compte des défaillances systématiques, un SIL de niveau 3. Par contre, la norme ne donne aucune indication sur les éventuelles prescriptions de ces paragraphes qui pourraient ne pas être satisfaites si un niveau d'intégrité inférieur est visé. Pour revendiquer un SIL inférieur à 3, il est conseillé de respecter un maximum d'exigences du ***§ 6.7.9***.

Il faut rappeler que l'usage de la norme NF EN 60204-1 permet de répondre à de nombreuses préconisations de ce paragraphe de la norme.

Bilan sur le SIL final d'un sous-système

Il faut récapituler toutes les données propres au sous système tel que représenté dans le Tableau 6. Le SIL et la PFH_D des sous-systèmes sont les données finales qui seront reprises pour l'évaluation du SIL des SRCF dans lesquelles le sous-système intervient.

Lorsque que le résultat des analyses permet de revendiquer un SIL supérieur ou égal au SIL requis, du point de vue des contraintes architecturales, de l'intégrité de sécurité systématique et de la PFH_D, alors le SIL final du sous-système répond au SIL requis.

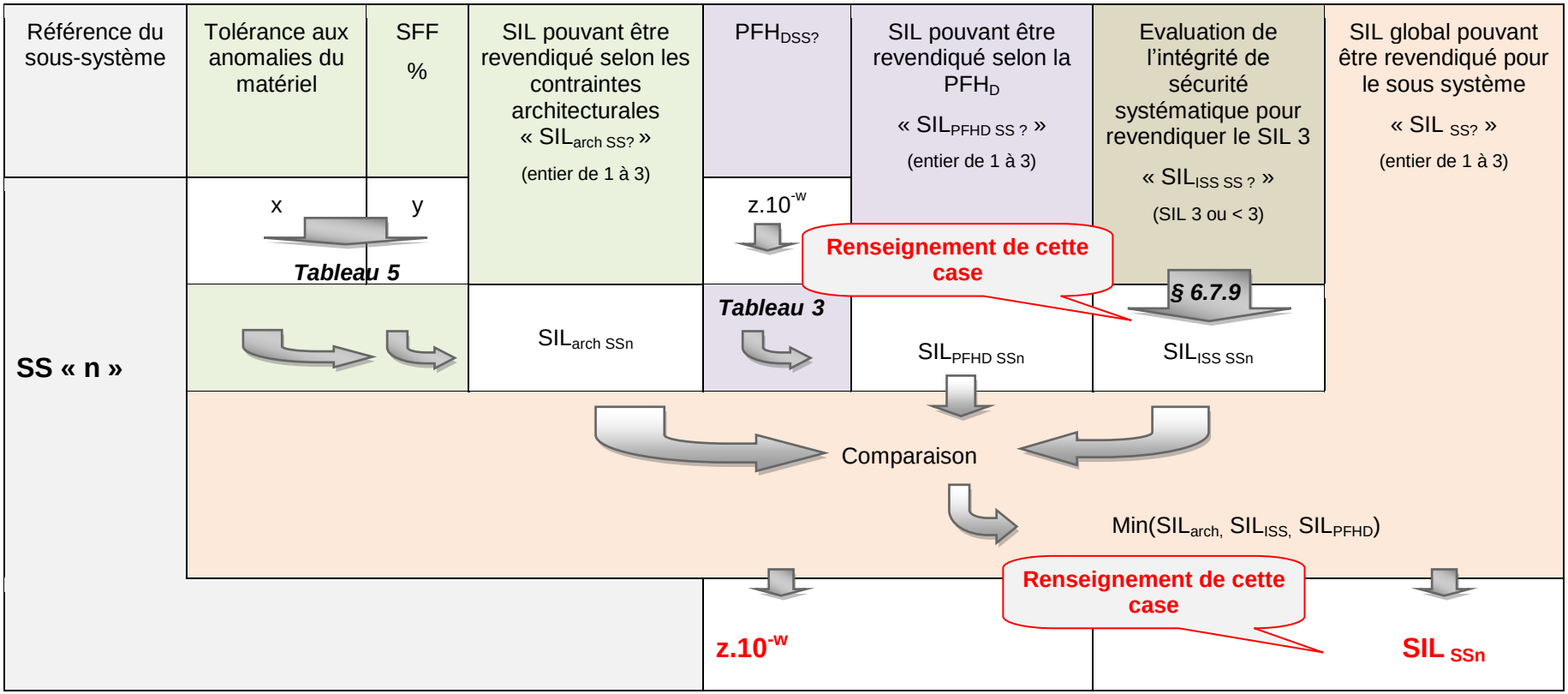


Tableau 6 : Récapitulatif du SIL pouvant être revendiqué pour un sous-système SS « n »

8.5 Préconisations concernant les fonctions de diagnostic

Lors de la conception d'un sous-système, les anomalies de ce dernier (et le cas échéant les conséquences des anomalies de ses éléments de sous-système) sont étudiées afin d'analyser leurs conséquences sur le comportement de la SRCF à laquelle le sous-système participe. Les anomalies susceptibles d'empêcher la SRCF d'assurer sa fonction sont défavorables au niveau d'intégrité de sécurité de la SRCF, tant du point de vue des exigences de contraintes architecturales (***§ 6.7.6***) que du point de vue de la PFH_D (***§ 6.7.8***).

Pour améliorer le SIL d'un sous-système (et particulièrement sa SFF et sa PFH_D), une des possibilités consiste à ajouter des fonctions de diagnostic (***§ 3.2.17***) afin de détecter les anomalies dangereuses pour la SRCF et de générer une réaction à ces anomalies (***§ 3.2.18***) pour faire réagir le SRECS en sécurité dans un temps qui doit être spécifié.

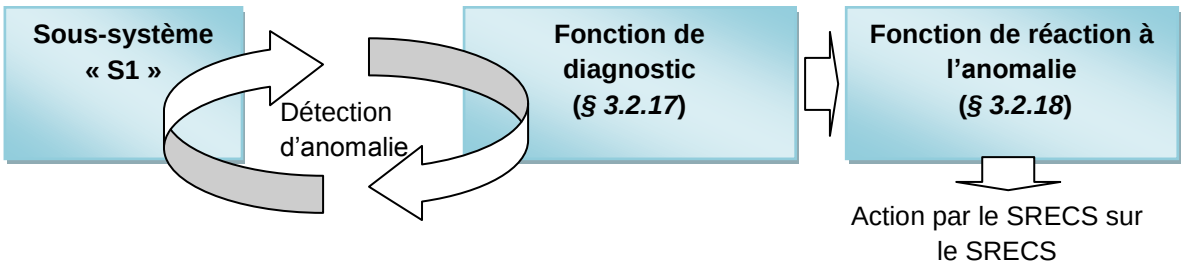


Figure 13 : Principe de mise en œuvre d'une fonction de diagnostic

La norme traite les fonctions de diagnostic, d'une part, en précisant des exigences comportementales du SRECS lors de la détection d'anomalies (***§ 6.3***), puis d'autre part, en décrivant des préconisations de réalisation de ces fonctions (***§ 6.8***).

8.5.1 Comportement d'un SRECS suite à la détection d'une anomalie

Deux cas peuvent se présenter suivant que la tolérance aux anomalies du matériel est :

- de « 0 » ; dans ce cas, le ***§ 6.3.2*** s'applique,
- ou supérieure à « 0 » ; dans ce cas, le ***§ 6.3.1*** s'applique ; si après l'apparition d'anomalies, la tolérance aux anomalies du matériel est réduite à 0, le ***§ 6.3.2*** s'applique.

Le ***§ 6.6.1.3*** impose que les fonctions de réaction aux anomalies spécifiées soient exécutées par le SRECS.

8.5.2 Préconisations de réalisation des fonctions de diagnostic

Le ***§ 6.8*** de la norme décrit les préconisations à respecter pour les fonctions de diagnostic. Elles sont considérées comme des fonctions à part entière et séparées des SRCF. Elles peuvent être réalisées par le même sous-système qui nécessite des fonctions de diagnostic ou d'autres sous-systèmes du SRECS, participant ou pas à la SRCF (***§ 6.8.2***).

Une fonction de diagnostic doit être documentée suivant le ***§ 6.8.5***, afin de bien déterminer le rôle de cette fonction vis-à-vis de l'anomalie à traiter. Il faut définir l'intervalle des tests de diagnostic (T2), évoqué dans le ***§ 6.7.8.1.4*** et le ***§ 6.7.8.1.5*** qui est également utile dans le calcul de la PFH_D pour l'architecture « D ».

Les fonctions de diagnostic sont soumises à des règles d'évitement des défaillances et anomalies systématiques (***§ 6.8.3***).

Le ***§ 6.8.4*** préconise que la probabilité de défaillance de la (des) fonction(s) de diagnostic du SRECS soit prise en compte lors de l'estimation de la PFH_D de la SRCF. Cette préconisation a pour but de sensibiliser le concepteur, afin qu'il mette en œuvre des moyens pour améliorer la fiabilité des

fonctions de diagnostic. C'est le sens des notes de cette préconisation et notamment de la note 3 qui demande clairement qu'une défaillance d'une (des) fonction(s) de diagnostic soit détectée et qu'une réaction appropriée soit déclenchée.

En complément du ***§ 6.8.4***, pour les sous-systèmes de tolérance aux anomalies du matériel égale à zéro, la norme (***§ 6.8.6)*** est plus exigeante en ce qui concerne la probabilité de défaillance dangereuse de la fonction de diagnostic.

8.5.3 Exemples de fonctions de diagnostic et de réaction à une anomalie

- Sous-système dont la tolérance aux anomalies est « 0 ». Une fonction de diagnostic est mise en œuvre pour une anomalie donnée. La détection de cette anomalie s'effectue lors de chaque sollicitation du sous-système (la fréquence de diagnostic est donc celle de sollicitation du sous-système), en contrôlant son état de sortie par rapport à celui attendu. Si le sous-système ne s'est pas comporté comme attendu lors du test, le SRECS réagit à cette anomalie en se mettant en sécurité avant que la situation dangereuse ne puisse se produire. Il s'agit par exemple de vérifier si l'état d'un contacteur électromécanique (via l'état de ses contacts) est en concordance avec l'état de son signal de commande (alimentation de la bobine).
- Sous système dont la tolérance aux anomalies est « 0 » et application de l'exception de ***§ 6.3.2*** de la norme. Une fonction de diagnostic est mise en œuvre pour une anomalie donnée. La détection de cette anomalie s'effectue par un test dynamique qui vient stimuler, à une fréquence 100 fois supérieure à celle de sollicitation de la SRCF, le sous-système pour vérifier s'il est apte à agir comme spécifié. Si le sous-système ne s'est pas comporté comme attendu lors du test, le SRECS réagit à cette anomalie en se mettant en sécurité.
- Un exemple de traitement d'un sous-système dont la tolérance aux anomalies est « 1 » est détaillé en annexe D de ce document.

9 Evaluation du SIL final des SRCF (§6.6.3)

Les préconisations du ***§ 6.6.3*** doivent être respectées.

Le SIL du SRECS doit être évalué pour chaque SRCF prise séparément (***§ 6.6.3.1***), en prenant en compte les trois critères nécessaires, la PFH_D du matériel, les contraintes architecturales et l'intégrité de sécurité systématique des sous-systèmes qui la composent.

Le SIL obtenu par une SRCF est inférieur ou égal à la valeur la plus faible des SIL de tous les sous-systèmes la constituant.

Les exigences correspondantes de la norme ne nécessitent pas d'informations complémentaires pour pouvoir être exploitées par un concepteur de SRECS.

Si la SRCF n'atteint pas le SIL requis, il faut recommencer le cycle de conception, par exemple, en revoyant l'architecture du SRECS, en diminuant le nombre de sous-systèmes, en améliorant la PFH_D des sous-systèmes (choix de composants avec une PFH_D plus faible, amélioration de l'architecture interne des sous-systèmes, amélioration de l'immunité aux défaillances de cause commune,…).

Dans le cas où un processus de communication de données numériques est utilisé pour relier des sous-systèmes (ex : RTdS), sa probabilité de défaillance dangereuse, appelée PTE dans la norme, doit être intégrée dans le calcul de la PFH_D de la SRCF.

Le Tableau 7 récapitule, pour une SRCF constituée de deux sous-systèmes sans processus de communication, les différents paramètres nécessaires ainsi que les opérations à effectuer pour l'évaluation du SIL.

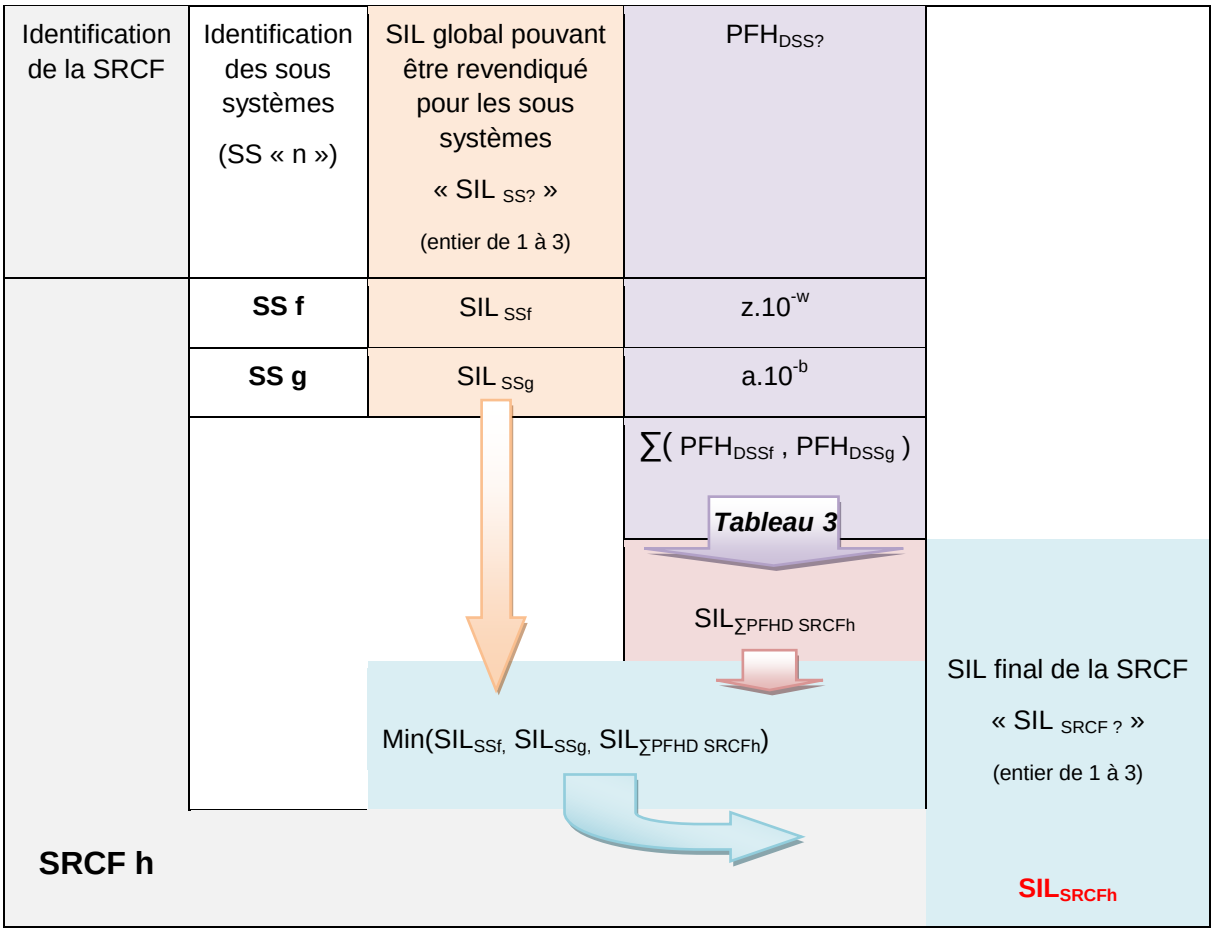


Tableau 7 : Exemple d'estimation du SIL d'une SRCF constituée de deux sous-systèmes

10 Logiciel relatif aux SRCF – Conception et développement (*§ 6.10 et 6.11*)

Si on utilise du logiciel dans une quelconque partie du SRECS réalisant une SRCF, une spécification des exigences de sécurité du logiciel doit être développée et documentée en suivant les préconisations des ***§ 6.10*** et ***6.11***.

Les phases de conception décrites ci-avant, permettant de concevoir ou de choisir du matériel dont l'intégrité de sécurité répond aux SRCF à traiter, ne doivent surtout pas faire mésestimer la phase de conception du logiciel. En effet, il est encore trop fréquent de penser que, dès lors qu'un matériel répond au SIL requis pour une SRCF, la réalisation des équations logiques peut alors s'effectuer sans règle particulière. C'est une erreur monumentale. Il faut garder à l'esprit qu'un circuit de commande réalisé par exemple avec un APIdS, apte à assurer des SRCF de SIL 3, peut se comporter de manière dangereuse si sa programmation n'a pas été effectuée dans les règles.

Les règles de la norme NF EN 62061 doivent donc être impérativement respectées. Elles couvrent l'ensemble des aspects de développement d'un logiciel dédié à des applications de sécurité et n'apportent pas vraiment d'éléments nouveaux. Elles ne posent donc pas de difficultés particulières.

L'INRS ayant déjà élaboré un guide pour le développement d'un logiciel applicatif de sécurité [8] basé sur les recommandations de la norme NF EN 62061, il n'est donc pas prévu de traiter de ce thème dans ce document, mais seulement de rappeler quelques principes élémentaires.

Spécification des exigences de sécurité du logiciel (*§ 6.10*)

Cette spécification va être basée sur les spécifications fonctionnelles des blocs fonctionnels ou des sous-systèmes des SRCF, complétées par les éventuelles fonctions de diagnostic. Le travail de spécification nécessaire pour le logiciel est déjà en grande partie réalisé. C'est ce qui ressort notamment des ***§ 6.10.2.2*** et ***6.10.2.6*** de la norme.

Conception et développement du logiciel (*§ 6.11*)

Le ***§ 6.11*** de la norme ne nécessite pas d'être à nouveau détaillé car il reprend toutes les exigences nécessaires, comme par exemple la gestion de la configuration du logiciel, celles relatives à l'architecture et le développement du code.

La Figure 14 représente un cycle en « V », qui est un modèle que recommande l'INRS aux concepteurs, pour leur permettre de gérer les phases de développement pour respecter les spécifications de la norme.

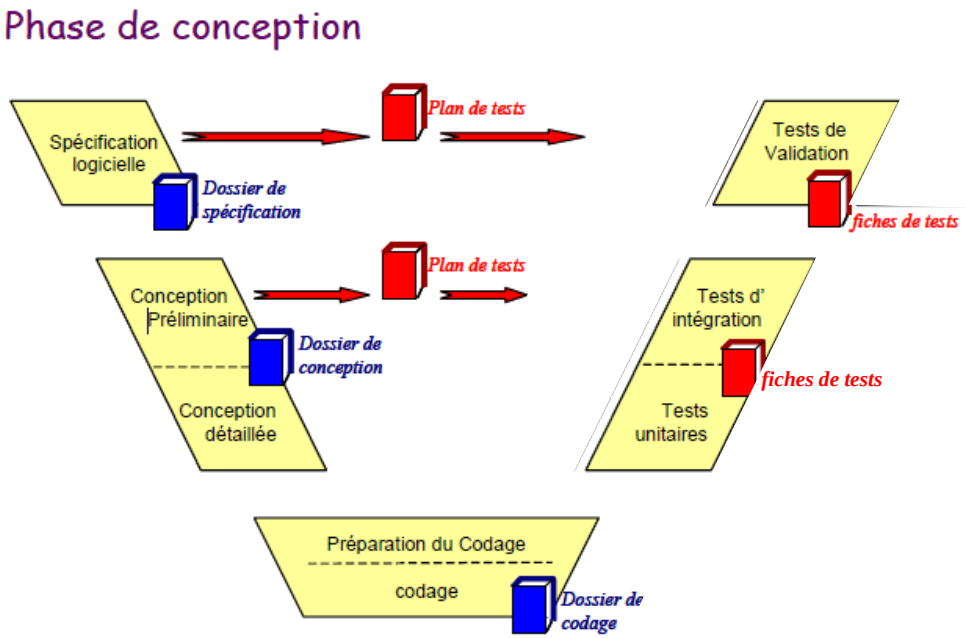


Figure 14 : Cycle en V de développement du logiciel applicatif du SRECS, montrant les différentes phases à suivre par le concepteur

Les phases décrites dans la branche de gauche de ce diagramme sont en général assez bien suivies par les concepteurs.

Par contre, l'INRS a constaté que les phases de tests et surtout leur préparation étaient trop souvent négligées ou mal réalisées. Or, quelle que soit la méthode de développement suivie, ces opérations sont indispensables.

Il est impératif de prévoir, pour chacune des phases de conception, des « plans de tests » précisant notamment les moyens à mettre en œuvre, en se basant sur les spécifications. Il n'est pas concevable que les plans de tests soient conçus après le codage et/ou basés sur le code du logiciel. C'est malheureusement cette dernière situation qui est constatée assez fréquemment sur le terrain. Le résultat est alors catastrophique car les tests peuvent révéler que le code est correct, mais tout en lui laissant la possibilité de ne pas répondre aux spécifications.

Ensuite, lorsque les tests ont été réalisés, les résultats doivent être consignés dans des « fiches de tests ».

Personnel chargé de la réalisation du logiciel

Les APIdS du marché ont tous leurs spécificités, propres à chaque fabricant, que ce soit au niveau du langage et de leur outil de programmation, de leur structure interne ou du paramétrage de leurs cartes d'entrées/sorties. Il faut exiger que le personnel effectivement chargé de la réalisation du logiciel ait reçu une formation à la programmation de SRCF et sur le matériel retenu. Une formation effectuée sur un matériel dédié uniquement au traitement de fonctions « standard » ou à des applications du

domaine du « process » tel que la pétrochimie par exemple, n'est pas adaptée pour appréhender les spécificités des APIdS lors de la réalisation d'un SRECS suivant la norme NF EN 62061.

Vérification du logiciel (*§ 6.11.2.5*)

Il faut impérativement que cette phase soit prévue et réellement effectuée. Elle devrait inclure systématiquement une vérification par une équipe différente de celle qui a développé le logiciel, afin d'avoir un œil externe sur la programmation, moyen qui reste particulièrement efficace pour détecter et corriger des éventuelles erreurs. L'INRS recommande aux concepteurs de s'inspirer de son « guide pour la mise en œuvre d'une méthode de validation par tierce partie, des parties de circuit de commande de presses traitées par un système de commande programmable » [9].

Maintien de l'intégrité du logiciel

Des moyens tels qu'un mot de passe (***§ 6.2.11.2.1***) doivent être mis en œuvre pour que le logiciel ne puisse pas être modifié autrement que par du personnel qualifié. Les éventuelles modifications ne doivent surtout pas être effectuées en ligne sur une installation en service. Il est impératif qu'elles soient effectuées dans les mêmes conditions que celles imposées pour la conception du logiciel.

11 Intégration et tests du SRECS (*§ 6.12*)

Intégration du SRECS

La norme exprime clairement l'objectif à atteindre au niveau du SRECS. Les sous-systèmes et éléments de sous-systèmes doivent être interconnectés entre eux de façon à pouvoir répondre aux spécifications des SRCF correspondantes.

Pour l'exemple de la presse plieuse, l'intégration du SRECS a consisté à implanter ses éléments constitutifs dans les armoires électriques correspondantes, à interconnecter entre eux certains sous-systèmes du SRECS (les contacts des capteurs de position des protecteurs, le bornier de la barrière immatérielle, les contacts de la pédale de commande, l'APIdS,…).

Tests du SRECS

Il faut procéder à des tests fonctionnels afin de s'assurer que le SRECS remplit les fonctions prévues et n'en réalise pas qui ne soient pas prévues. Il faudra prévoir, le cas échéant, les tests d'intégration de la partie logicielle de certains sous-systèmes qui n'ont pas pu être réalisés en totalité car une interaction avec d'autres sous-systèmes était nécessaire.

La ***note du § 6.12*** rappelle que l'intégration d'un SRECS s'effectue généralement préalablement à l'installation, mais que dans certains cas, elle peut être effectuée après l'installation. En réalité, il faut souvent combiner ces deux façons de faire. Il est fréquemment possible d'effectuer une partie des tests sur le SRECS (ou une de ses parties) avant installation, et le reste seulement après installation, par exemple lorsque le SRECS a besoin d'échanger de nombreuses données avec ses périphériques traitant des fonctions « standard », ou lorsque certains sous-systèmes du SRECS ne peuvent être interconnectés qu'au moment de l'installation du SRECS.

La norme, ***§ 6.12.2,*** préconise que, lors de l'intégration du SRECS, des tests soient prévus pour chacune des mesures mises en œuvre pour maîtriser les exigences d'intégrité de sécurité systématiques du SRECS décrites dans le § 6 de ce document. Par exemple, pour les tests relatifs aux anomalies systématiques, il faudra procéder à des tests ou analyses de l'effet sur le comportement de SRCF des coupures d'alimentation du SRECS, des coupures de liaisons entre les sous-systèmes, des courts-circuits entre certains conducteurs.

12 Installation et validation du SRECS (*§6.13 et § 8*)

Ces deux phases doivent être réalisées conformément au plan de sécurité fonctionnelle (***§ 4.2*** de la norme).

12.1 Installation

Le SRECS doit être installé sur l'équipement auquel il est dédié de façon à ce qu'il soit apte à assurer l'usage prévu et qu'il soit prêt pour la validation. Cette installation doit s'effectuer en respectant toutes les consignes de la documentation d'installation du SRECS (suivant les préconisations du ***§ 7*** de la norme) ainsi que les schémas de raccordement. Les consignes telles que celles destinées à éviter les défaillances de cause commune (par exemple la séparation de certains câbles peut avoir été requise), qui ont été édictées et répertoriées lors de la conception du SRECS, doivent être respectées.

L'installation consiste principalement à :

- la mise en place et le raccordement du matériel relatif au SRECS sur l'équipement,
- l'interconnexion du SRECS aux périphériques avec lesquels il échange des informations.

Pour l'exemple de la presse plieuse, l'installation a consisté à constituer le circuit de commande complet de cette machine en connectant le SRECS aux parties de commande « standard » et aux distributeurs hydrauliques de commande du tablier.

Vérification de l'installation

Une fois le matériel mis en place sur l'équipement auquel il est destiné, il faut procéder à des contrôles afin de s'assurer qu'aucune erreur ne s'est produite lors de l'installation. Ces opérations doivent s'appuyer sur des plans de tests associés à des procédures correspondantes. Les exemples suivants illustrent quelques unes des vérifications de tests à effectuer, à adapter et à compléter suivant les cas.

Exemples de contrôles :

- Câblage électrique correct (pas de conducteurs non raccordés, effilochés, état des soudures, risques de contact entre deux conducteurs adjacents, serrage des vis des borniers, cheminement des câbles,…).
- Circuits de protection correctement calibrés par rapport aux valeurs prévues (par ex. valeur des fusibles).
- Masses et borne générale de mise à la terre correctement raccordées.
- Caractéristiques correctes des différentes sources d'alimentation (tension, par ex.).

Exemples d'autres contrôles à effectuer en prenant des dispositions pour que les actionneurs pouvant générer des mouvements potentiellement dangereux soient déconnectés et restent en situation sûre :

- sollicitation physique des entrées et vérification que l'information arrive bien au bon endroit sur le bornier de raccordement du SRECS – Par exemple, sollicitation d'un capteur de position d'un protecteur et vérification de l'information correspondante aux bornes prévues de raccordement au SRECS, ou le cas échéant, vérification au niveau du logiciel d'un APIdS de la variable correspondante.
- Sollicitation physique des différentes sorties et vérification que l'information arrive bien au bon endroit sur le bornier de raccordement des périphériques assujettis au SRECS. Par exemple, sollicitation par forçage d'une sortie et vérification de l'information correspondante aux bornes des distributeurs hydrauliques prévus pour l'arrêt d'un élément mobile dangereux.

Comme pour chaque étape du cycle de développement, les résultats doivent être enregistrés.

12.2 Validation (*§ 8*)

Elle a pour but de s'assurer que le SRECS, mis en service, réalise les exigences établies dans la spécification des exigences de sécurité. Les préconisations du ***§ 8*** de la norme décrivent précisément les opérations à effectuer.

13 Informations pour l'utilisation (*§ 7*), modification (*§ 9*) et documentation du SRECS (*§ 10*)

Les préconisations de la norme ne nécessitent pas de précisions complémentaires pour pouvoir être appliquées.

Bibliographie

[1] Norme NF EN 62061 – Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité. Paris, AFNOR, Juillet 2005, 106 p., et les corrigenda CEI 62061/AC1:2005 de Juillet 2005 (2 p.) et CEI 62061/AC2:2008 d'avril 2008 (13 p.).

[2] Norme NF EN ISO 13849-1 – Sécurité des machines. Parties des systèmes de commande relatives à la sécurité. Partie 1 : principes généraux de conception. Paris, AFNOR, Octobre 2008, 102 p.

[3] Directive 2006/42/CE du 17 mai 2006 relatives aux machines et modifiant la directive 95/16/CE (refonte). Journal Officiel des Communautés Européennes n° L157 du 09 juin 2006, 63 p.

[4] BUCHWEILLER J.P. - Circuits de commande des machines – Un référentiel normatif pour leur conception - Hygiène et sécurité du travail, Cahiers de notes documentaires, 2e trimestre 2008, PR 34-211, pp. 63-79.

[5] Directive 98/37/CE du 22 juin 1998 concernant le rapprochement des législations des Etats membres relatives aux machines. Journal Officiel des Communautés Européennes n° L207 du 23 juillet 1998, 46 p.

[6] Norme NF EN 12622 – Sécurité des machines-outils – Presses plieuses hydrauliques. Paris, AFNOR, Janvier 2010, 63 p.

[7] Norme NF EN 60204-1 - Sécurité des machines – Equipement électrique des machines – Partie 1 : Règles générales. Paris, AFNOR, Septembre 2006, 128 p.

[8] LAMY P., CHARPENTIER P. - Utilisation des automates programmables industriels dédiés à la sécurité – Guide pour le développement du logiciel applicatif. Hygiène et sécurité du travail, Cahiers de notes documentaires, 4e trimestre 2004, ND 2217-197-04, pp. 7-19.

[9] BAUDOIN J., BELLO J.P., BLAISE J.C. - Guide pour la mise en œuvre d'une méthode de validation, par tierce partie, des parties de circuits de commande de presses traitées par un système de commande programmable, INRS, NS 252, juin 2005, 34 p.

[10] Norme NF EN ISO 14121-1 – Sécurité des machines. Appréciation du risque. Partie 1 : principes. Paris, AFNOR, Novembre 2007, 40 p.

[11] Norme NF EN ISO 12100-1 – Sécurité des machines - Notions fondamentales, principes généraux de conception - Partie 1 : terminologie de base, méthodologie. Paris, AFNOR, Janvier 2004, 43 p.

[12] Norme NF EN ISO 12100-2 – Sécurité des machines - Notions fondamentales, principes généraux de conception - Partie 2 : principes techniques. Paris, AFNOR, Janvier 2004, 42 p.

[13] CEI 61508 parties 1 à 7 – Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité. Paris, AFNOR, Mars 2002, 439 p.

Exemple de conception d’un SRECS

Cet exemple illustre la conception du SRECS d’une presse plieuse.

Il part du niveau global de la machine, qualifie le SRECS et ses SRCF puis traite d’une SRCF particulière et d’un de ses sous-systèmes.

Seules des phases de conception significatives, faisant ressortir les détails et les commentaires jugés nécessaires pour assimiler les principes préconisés par la norme et en utilisant les outils décrits dans le guide, sont présentées.

SOMMAIRE de L'EXEMPLE

ANNEXE A - DESCRIPTION DE LA PRESSE PLIEUSE 50

A.1 GENERALITES 51
A.2 ELEMENTS PRIS EN COMPTE LORS DE L'APPRECIATION DES RISQUES DE LA PPH 52
A.3 DESCRIPTION DES MODES DE MARCHE DE LA PRESSE PLIEUSE HYDRAULIQUE 53
A3.1 Mode « réglage » 54
A3.2 Mode « Production » 54
A3.3 Protecteurs latéraux 55
A3.4 Protection de la face arrière 55
A3.5 Arrêts d'urgence 55

ANNEXE B - DETAIL DES FONCTIONS DE SECURITE ET DELIMITATION DU SRECS 57

B1. IDENTIFICATION DES FONCTIONS PRISES EN EXEMPLE POUR LA PRESSE PLIEUSE 57
B2. SEPARATION DES FONCTIONS DE SECURITE DES FONCTIONS DE COMMANDE 57
B3. IDENTIFICATION ET SPECIFICATION DES FONCTIONS DE SECURITE PRISES EN EXEMPLE POUR LA PRESSE PLIEUSE 58
B4. ARCHITECTURE DU CIRCUIT DE COMMANDE DU TABLIER DE LA PRESSE PLIEUSE 60
B5. IDENTIFICATION DE L'INTERFACE ENTRE LE SRECS ET LE CIRCUIT DE COMMANDE HYDRAULIQUE DU TABLIER DE LA PRESSE PLIEUSE 61

ANNEXE C - FORMALISATION DES SRCF 63

C1. IDENTIFICATION DES FONCTIONS DE COMMANDE RELATIVES A LA SECURITE (SRCF) 63
C2. SPECIFICATIONS DES EXIGENCES FONCTIONNELLES DES SRCF 63
C3. SPECIFICATIONS DES EXIGENCES D'INTEGRITE DE SECURITE DES SRCF 65
C4. CONCEPTION D'UNE SRCF 69
C4.1 Analyse/décomposition d'une SRCF en blocs fonctionnels 69
C4.2 Attribution de sous-systèmes aux blocs fonctionnels d'une SRCF 73

ANNEXE D - SPECIFICATION ET CHOIX / CONCEPTION D'UN SOUS-SYSTEME 76

D1. INFORMATIONS NECESSAIRES POUR LE CHOIX OU LA CONCEPTION D'UN SOUS-SYSTEME 76
D2. SPECIFICATIONS REQUISES POUR LE CHOIX/CONCEPTION D'UN SOUS-SYSTEME 76
D3. PHASES DE CHOIX/CONCEPTION DU SOUS-SYSTEME SS7 77
D4. PREMIERE PHASE : CHOIX D'UN COMPOSANT « TYPE » DU COMMERCE POUR REALISER L'INTEGRALITE DU SOUS SYSTEME SS7 (§ 6.7.3) 78
D4.1 Détermination du SIL pouvant être revendiqué par le sous-système 79
D4.1.1 Détermination du SIL vis-à-vis des contraintes architecturales du sous-système SS7 79
D4.1.2 Conclusions sur le SIL de SS7 81
D5. DEUXIEME PHASE : CONCEPTION D'UN SOUS-SYSTEME « PARTICULIER » 83
D5.1 Choix de l'architecture d'un sous-système 83
D5.2 Détermination du SIL pouvant être revendiqué par le sous-système SS7 85
D5.2.1 Détermination du SIL vis-à-vis des contraintes architecturales du sous-système SS7 85
D5.2.2 Détermination du SIL vis-à-vis de la PFHD du sous-système SS7 86
D5.2.3 Evaluation de l'intégrité de sécurité systématique du sous-système SS7 pour revendiquer le SIL 3 87
D5.3 Conclusions sur le SIL de SS7 88
D5.4 Tableau récapitulatif des caractéristiques du sous-système SS7 89
D5.5 Exemple d'estimation de la sensibilité aux défaillances de cause commune (CCF) du sous-système SS7 91

ANNEXE E - EVALUATION DU SIL FINAL DE LA SCRF C 94

ANNEXE F - EXTRAIT DES PLANS DE TESTS DE VALIDATION DU SRECS DE LA PRESSE PLIEUSE HYDRAULIQUE . 95

Annexe A - Description de la presse plieuse

Le cas traité dans le présent document pour illustrer la démarche de conception d'un SRECS est celui d'une presse plieuse hydraulique, utilisée pour le travail à froid des métaux et pour laquelle les opérations de production, dont l'approvisionnement de la tôle et son maintien pendant le pliage, sont effectuées manuellement.

Cette machine, représentative de l'industrie métallurgique, est soumise aux règles de conception de la directive « Machines » 2006/42/CE, anciennement dénommée 98/37/CE [5]. La norme de conception de type C, NF EN 12622 [6] traitant de la sécurité des presses plieuses hydrauliques donne présomption de conformité à cette directive.

Les exemples et les données fournis dans ce document, relatifs à la presse plieuse, le sont dans un but pédagogique. Certaines données de l'EN 12622 ont été déterminées à nouveau dans le but d'illustrer l'application de certains concepts de la norme NF EN 62061, par exemple pour la détermination des niveaux de performance des fonctions de sécurité.

Ces exemples et ces données n'ont pas vocation à :

- valider ou invalider les prescriptions réglementaires ou normatives citées précédemment,
- être appliqués, en l'état, pour la conception d'une presse plieuse.

Dans le cas présent, le circuit hydraulique de commande des mouvements principaux de cette machine est un composant du commerce, prenant en compte toutes les caractéristiques fonctionnelles et de sécurité nécessaires à cette machine et répondant en tous points aux exigences applicables de la directive et aux recommandations de la norme NF EN 12622. De fait, seule la conception complète de la partie électrique du circuit de commande doit être effectuée, ce qui justifie le choix du référentiel NF EN 62061.

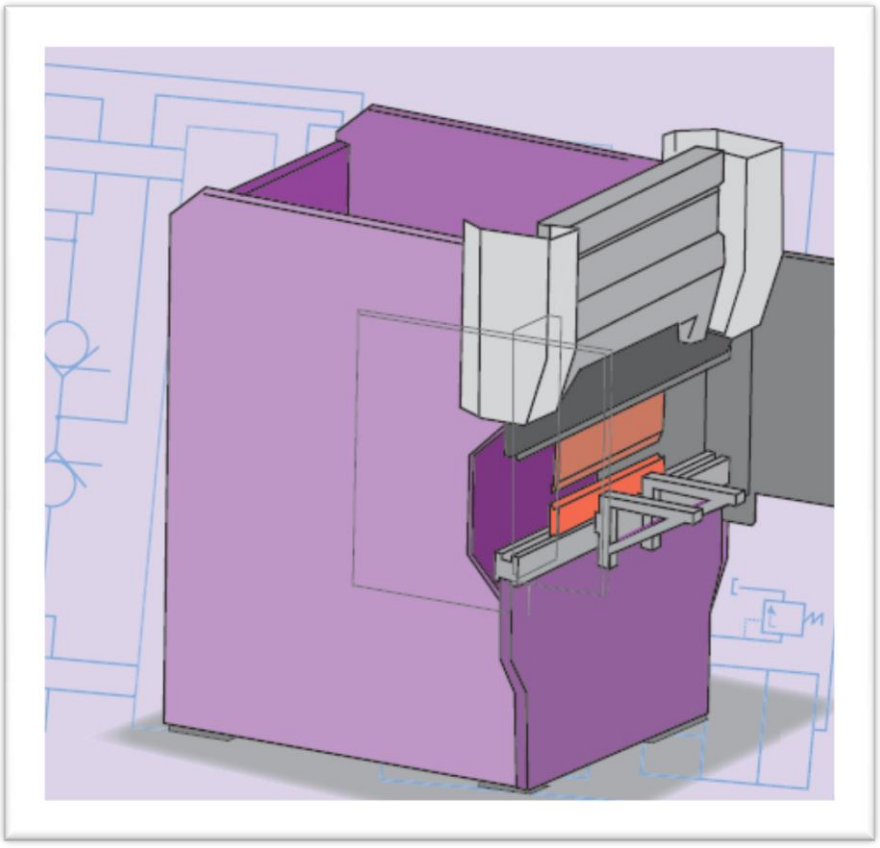


Figure 15 : Presse plieuse hydraulique

A.1 Généralités

La machine prise en exemple est une presse plieuse hydraulique destinée au pliage de tôles entre deux outils appelés poinçon pour l'outil supérieur et matrice pour l'inférieur. Cette presse plieuse est commandée et utilisée par un seul opérateur, situé sur la face avant, qui effectue des opérations de chargement et déchargement manuel de la tôle entre les outils. De plus, la pièce est généralement maintenue manuellement, par l'opérateur, notamment pendant la phase de fermeture des outils.

Les éléments mobiles considérés sont :

- **un tablier supérieur mobile**, également appelé coulisseau sur lequel est fixé l'outil supérieur, le poinçon. Ce tablier se déplace suivant un axe vertical,
- **une butée motorisée**, située à l'arrière de l'axe de pliage (derrière les outils) destinée au positionnement de la tôle. La butée motorisée se déplace suivant un axe horizontal, perpendiculaire à l'axe de pliage.

Le tablier supérieur mobile est mû par deux vérins indépendants (Y1 à gauche et Y2 à droite) synchronisés par la commande numérique. L'énergie hydraulique nécessaire aux mouvements des vérins est obtenue par un groupe motopompe hydraulique propre à la presse plieuse. Les différents ordres issus du système de commande électrique agissent sur un ensemble de distributeurs hydrauliques, proportionnels ou non, destinés à commander les différents mouvements et à assurer des fonctions de sécurité (ex : les distributeurs prévus pour la redondance des éléments de retenue du tablier mobile).

La commande de fermeture des outils correspond au mouvement de descente du tablier mobile, la commande d'ouverture des outils correspond au mouvement de montée du tablier mobile.

Les mouvements de descente du tablier sont obtenus, selon les modes de fonctionnement et les phases de ces modes, soit en grande vitesse (GV), soit en petite vitesse (PV) ou vitesse de travail. Ces paramètres de vitesse sont gérés par la commande numérique et par des dispositions hydrauliques spécifiques.

Le Tableau 8 définit, pour les différents mouvements du tablier mobile (descente GV ou PV, montée ou arrêt) et pour les deux vérins Y1 et Y2 nécessaires à son mouvement, les distributeurs hydrauliques concernés et leur état d'actionnement. Parmi ces distributeurs proportionnels (PDG, PDD, PMG, PMD et EVP) ou tout ou rien (EV1, EV2, EV3, EV4 et EV5), certains sont destinés à assurer des fonctions de commande et/ou des fonctions de sécurité.

Distributeurs / **Mouvements**	Commande Descente EV Proport. Y1-Y2	Commande Montée EV Proport. Y1-Y2	Commande Descente PV	Commande Descente GV Y1-Y2	Commande Pression EV Proport.	Commande Descente Retenue Y1-Y2
	PDG-PDD	**PMG-PMD**	**EV1**	**EV2-EV3**	**EVP**	**EV4-EV5**
Descente (GV)	1	0	0	1	0	1
Descente (PV)	1	0	1	0	1	1
Montée	0	1	0	0	1	0
Arrêt	0	0	0	0	0	0

Tableau 8 : Diagramme d'actionnement des distributeurs hydrauliques de commande des mouvements du tablier mobile

La Figure 16 illustre les différentes phases du mouvement du tablier supérieur mobile ainsi que les appellations des différentes positions de ce tablier.

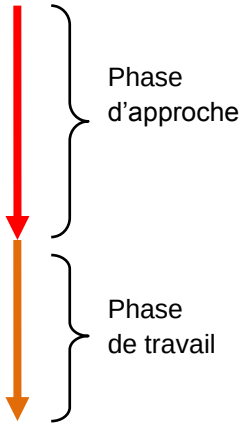
Positions du tablier supérieur mobile	Abréviations	Direction du mouvement du tablier mobile	
		Descente	Montée
Point Mort Haut	**PMH**		
Point de Commutation en Vitesse de Travail	**PCVT**		
Point Mort Bas	**PMB**		

Figure 16 : Illustration des mouvements et des positions du tablier supérieur mobile

La butée arrière motorisée est mue par un système à vis entraîné par un moteur électrique, piloté par un variateur qui est géré entièrement par la commande numérique.

Cette presse plieuse comporte deux modes de marche :

- un mode « réglage » prévu pour effectuer les réglages et changements d'outils de la presse plieuse,
- un mode « production » prévu pour une utilisation de la presse plieuse en production.

A.2 Eléments pris en compte lors de l'appréciation des risques de la PPH

L'appréciation des risques de la presse plieuse, qui n'est pas traitée dans ce document, a été effectuée suivant les normes NF EN ISO 14121-1 [10] et NF EN ISO 12100-1 [11] et 12100-2 [12]. Elle a montré que les éléments mobiles suivants présentent un risque pour l'opérateur :

- le tablier supérieur mobile lorsqu'il descend,
- la butée arrière motorisée lorsqu'elle se déplace vers l'avant de la machine.

L'estimation des risques pour chacun de ces mouvements dépend du mode de marche de la presse :

- **le tablier supérieur mobile lorsqu'il descend**
  - Phénomène dangereux mécanique : écrasement/sectionnement/coupure des membres supérieurs de l'opérateur, chocs à la tête
  - Gravité : Blessures irréversibles pouvant aller jusqu'à la mort
  - Fréquence d'accès :
    - 4 fois/équipe de 8 heures en réglage, chaque intervention d'une durée maximale de 15 mn,
    - 1 fois par minute en production, chaque intervention d'une durée maximale de 30 secondes.

- **la butée arrière motorisée lorsqu'elle se déplace vers l'avant de la machine**
    - Phénomène dangereux mécanique : écrasement/sectionnement des membres supérieurs de l'opérateur
    - Gravité : Blessures irréversibles pouvant aller jusqu'à la perte d'un doigt
    - Fréquence d'accès :
        - 4 fois/équipe de 8 heures en réglage (lors des opérations de montage d'outil sur le tablier),
        - théoriquement jamais en production.

Lors de l'appréciation des risques, des moyens de protection ont été définis conformément à ceux prévus par la norme NF EN 12622.

Dans le cas présent, les moyens de protection mis en œuvre et décrits dans la suite du document sont les suivants :

- Pour les risques liés aux mouvements de descente du tablier supérieur, depuis la face avant :
    - En mode réglage, la mesure de prévention retenue est une mesure de réduction des risques mettant en œuvre une commande à action maintenue du mouvement dangereux et une réduction de sa vitesse de déplacement. Le mouvement dangereux est maîtrisé avec possibilité d'arrêt en tout point de la course de descente. La réduction de la vitesse de descente favorise l'évitement du dommage.
    - En mode production, la mesure de prévention retenue est une mesure de suppression des risques par mise en place d'un dispositif de protection, une barrière immatérielle.
- Pour les risques liés aux mouvements de descente du tablier supérieur, depuis les faces latérales et arrière, la mesure de prévention retenue consiste à supprimer les risques par mise en place de protecteurs.
- Pour les risques liés aux mouvements d'avance de la butée arrière motorisée, depuis les faces latérales et arrière, la mesure de prévention retenue consiste à supprimer les risques par mise en place de protecteurs.
- Pour les risques liés aux mouvements d'avance de la butée arrière motorisée, depuis la face avant, la mesure de prévention retenue consiste à réduire les risques par démarcation d'une zone dans laquelle la vitesse de déplacement est réduite.
- Pour couvrir les éventuels risques résiduels, une mesure de prévention complémentaire est assurée par deux organes d'arrêt d'urgence disponibles au poste opérateur et sur le pupitre de commande général.

Les caractéristiques et le montage de ces moyens de protection répondent aux préconisations correspondantes de la norme NF EN 12622.

A.3 Description des modes de marche de la presse plieuse hydraulique

Les deux modes de marche de la presse plieuse sont sélectionnés au moyen d'un commutateur verrouillable à clé SE1.

Les organes de commande des mouvements du tablier mobile sont constitués d'une pédale de descente PED à trois positions (position 1 : arrêt pédale relâchée – position 2 : descente pédale actionnée – position 3 : arrêt pédale actionnée après un point dur, en cas de crispation de l'opérateur sur la pédale ou d'actionnement involontaire suite à un déséquilibre de l'opérateur) et d'une pédale de

montée PEM à deux positions (position 1 : arrêt pédale relâchée – position 2 : montée pédale actionnée).

Un bouton-poussoir de réarmement BPR permet de valider le mode de marche sélectionné et également de réinitialiser les conditions de fonctionnement après sollicitation d'un protecteur ou dispositif de protection de l'opérateur.

A3.1 Mode « réglage »

Mise en service

Le commutateur SE1 doit être positionné sur la position « 1 ». La mise en service du mode "réglage" se fait par une action sur le bouton-poussoir de réarmement (BPR).

Déroulement du mode

Une action maintenue sur la pédale PED (position 2) commande un mouvement de descente du tablier mobile. Au Point Mort Bas (PMB) programmé, la Commande Numérique (CN) commande l'arrêt du tablier.

La vitesse de déplacement du tablier, pendant la phase de descente, est limitée à la vitesse de travail (inférieure ou égale à 10 mm/s).

Un relâchement de la pédale PED ou son actionnement en 3e position commande l'arrêt et empêche le démarrage du mouvement de descente du tablier mobile, en tous points de sa course.

Une action maintenue sur la pédale PEM commande un mouvement de montée du tablier mobile. Au point mort haut (PMH) programmé, la CN commande l'arrêt du tablier.

Un relâchement de la pédale PEM commande l'arrêt du mouvement de montée du tablier mobile quelle que soit sa position.

Protection de l'opérateur en face avant

Le mouvement de descente du tablier mobile est arrêté ou empêché en cas :

- de relâchement de la pédale de descente PED en position 1, quelle que soit la position du tablier,
- d'actionnement de la pédale de descente PED en position 3, quelle que soit la position du tablier,
- de dépassement de la vitesse de 10 mm/s pendant ce mouvement.

Note : La barrière immatérielle (BI) de la face avant est hors service dans ce mode.

A3.2 Mode « Production »

Mise en service

Le commutateur SE1 doit être positionné sur la position « 2 ». La mise en service du mode "réglage" se fait par une action sur le bouton-poussoir de réarmement (BPR).

Déroulement du mode

La barrière immatérielle (BI) est active pendant tout le mouvement de descente du tablier (phase d'approche en grande vitesse et phase de travail en petite vitesse).

Une action maintenue sur la pédale PED (position 2) commande un mouvement de descente du tablier mobile, d'abord en grande vitesse dans sa phase d'approche puis en vitesse de travail

(inférieure ou égale à 10 mm/s) lorsqu'il atteint le point de commutation en vitesse de travail (PCVT) délivrée par la CN. Au point mort bas (PMB), la CN commande l'arrêt de descente du tablier et commande sa montée après un temps passé en pression, même si la pédale de descente est restée actionnée. Ce délai est réglé par l'opérateur à l'aide de la commande numérique.

Pour enclencher un nouveau cycle, l'opérateur doit, lorsque le tablier a atteint son point mort haut (PMH), relâcher la pédale de descente et l'actionner de nouveau.

Le relâchement de la pédale de descente ou son actionnement en 3e position commande l'arrêt et empêche le démarrage du mouvement de descente du tablier mobile, en tous points de sa course ; le tablier remonte immédiatement jusqu'au PMH si au moment de l'arrêt il n'a pas atteint le PCVT délivré par la CN.

L'occultation de la barrière immatérielle commande l'arrêt et empêche le démarrage du mouvement de descente du tablier mobile, en tous points de sa course; le tablier remonte immédiatement jusqu'au point mort haut si au moment de l'arrêt il n'a pas atteint le PCVT délivré par la CN.

Protection de l'opérateur en face avant

La protection de l'opérateur est assurée par une barrière immatérielle dont le champ de protection couvre tous les accès à la zone dangereuse depuis la face avant. Une occultation de son champ de protection commande l'arrêt et empêche le démarrage du mouvement de descente du tablier mobile, en tous points de sa course.

A3.3 Protecteurs latéraux

Ils sont constitués de protecteurs mobiles qui empêchent l'accès, depuis les côtés de la presse plieuse, au tablier mobile et à la butée arrière motorisée.

Lorsque les protecteurs latéraux sont ouverts, la commande de montée du tablier est possible en actionnant la pédale de montée.

Une fois les protecteurs latéraux fermés, pour rétablir les conditions initiales du circuit de commande, il est nécessaire d'appuyer sur le bouton-poussoir de réarmement (BPR).

L'ouverture du protecteur latéral droit ou gauche commande l'arrêt et empêche le démarrage des mouvements d'avance de la butée arrière motorisée et de descente du tablier mobile, en tous points de leur course.

A3.4 Protection de la face arrière

Elle est constituée d'un protecteur mobile et de protecteurs fixes qui empêchent l'accès, depuis l'arrière de la presse plieuse, au tablier mobile et à la butée arrière motorisée.

Lorsque le protecteur mobile arrière est ouvert, la commande de montée du tablier est possible en actionnant la pédale de montée.

Une fois le protecteur mobile arrière fermé, pour rétablir les conditions initiales du circuit de commande, il est nécessaire d'appuyer sur un bouton-poussoir de réarmement spécifique.

L'ouverture du protecteur mobile arrière commande l'arrêt et empêche le démarrage des mouvements d'avance de la butée arrière motorisée et de descente du tablier mobile, en tous points de leur course.

A3.5 Arrêts d'urgence

Deux boutons-poussoirs d'arrêt d'urgence sont situés à proximité du poste opérateur, l'un sur le pupitre de commande et l'autre sur le tablier de la presse plieuse.

Lorsqu'un BP d'arrêt d'urgence est actionné, la commande de montée du tablier est possible en actionnant la pédale de montée.

Une fois le BP d'arrêt d'urgence déverrouillé, pour rétablir les conditions initiales du circuit de commande, il est nécessaire d'appuyer sur le bouton-poussoir de réarmement (BPR).

L'actionnement d'au moins un BP d'arrêt d'urgence commande l'arrêt et empêche le démarrage des mouvements d'avance de la butée arrière motorisée et de descente du tablier mobile, en tous points de leur course.

Annexe B - Détail des fonctions de sécurité et délimitation du SRECS

B1. Identification des fonctions prises en exemple pour la presse plieuse

Les fonctions suivantes qui comprennent des fonctions de commande « standard » et des fonctions de sécurité sont déduites de la description des modes de marche et de protection de la presse plieuse hydraulique effectuée à l'annexe A de ce document.

Dans un souci de ne pas multiplier inutilement les exemples, les seules fonctions qui seront abordées dans la suite du document, sont les suivantes :

1. Arrêt et empêchement du démarrage du mouvement de descente du tablier mobile par relâchement de la pédale PED, en mode réglage et lorsque la vitesse est limitée à une valeur inférieure ou égale à 10 mm/s.
2. Arrêt et empêchement du démarrage du mouvement de descente du tablier mobile par actionnement de la pédale PED dans sa troisième position, en mode réglage et lorsque la vitesse est limitée à une valeur inférieure ou égale à 10 mm/s.
3. Arrêt et empêchement du démarrage du mouvement de descente du tablier mobile par occultation de la barrière immatérielle, en mode production.
4. Arrêt et empêchement du démarrage du mouvement de descente du tablier mobile par l'ouverture du protecteur latéral droit, dans tous les modes de fonctionnement.
5. Arrêt et empêchement du démarrage du mouvement d'avance de la butée arrière motorisée par l'ouverture du protecteur latéral droit, dans tous les modes de fonctionnement.
6. Commande du mouvement de montée du tablier mobile jusqu'au PMH, par actionnement de la pédale PEM, dans tous les modes de fonctionnement.
7. Commande du mouvement de descente du tablier mobile jusqu'au PMB, par actionnement de la pédale PED dans sa deuxième position, dans tous les modes de fonctionnement.

Les fonctions auxiliaires telles que réarmement, redémarrage, anti-répétition de cycle, etc. ne sont pas traitées dans les exemples présentés.

B2. Séparation des fonctions de sécurité des fonctions de commande

La Figure 17 illustre le principe de la priorité des fonctions de sécurité sur les fonctions de commande « standard » pour le mouvement de descente du tablier.

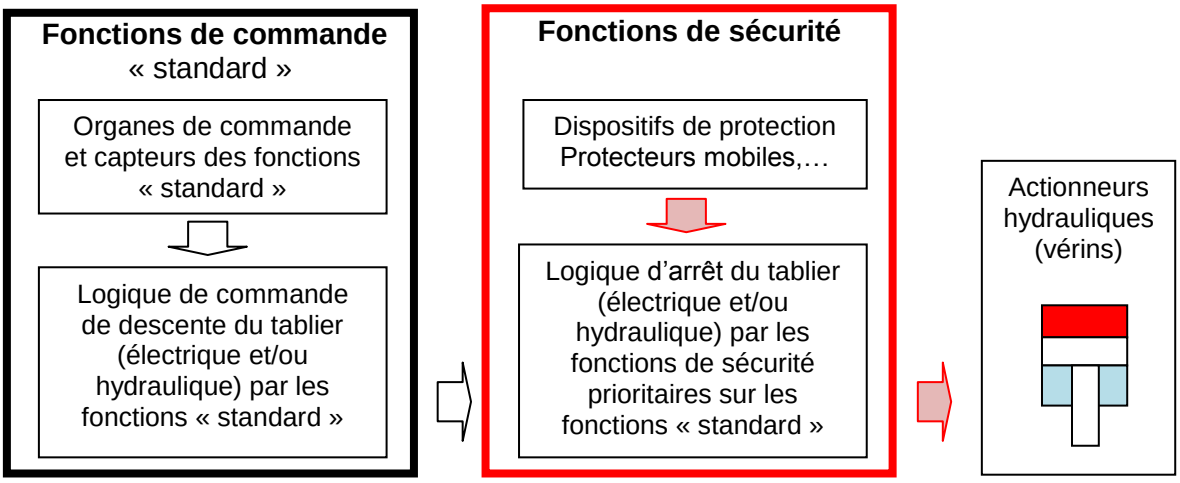


Figure 17 : Illustration de la priorité des fonctions de sécurité sur les fonctions de commande « standard »

B3. Identification et spécification des fonctions de sécurité prises en exemple pour la presse plieuse

L'identification des fonctions de sécurité proposée dans le Tableau 9 reprend la terminologie des fonctions identifiées précédemment (§ B1), mais permet par le découpage proposé d'isoler un certain nombre de critères qui seront utiles pour spécifier précisément, dans un premier temps, les fonctions de sécurité ainsi que leurs interactions, et dans un second temps, les SRCF.

Identification des fonctions de sécurité				
N° de la fonction de sécurité	**Action de sécurité**	**Elément mobile dangereux**	**Déclencheur de l'action de sécurité**	**Condition de validité de la fonction**
1	Arrêt et empêchement du démarrage du mouvement de descente	Tablier mobile	Relâchement de la pédale PED en position 1	Mode réglage et vitesse ≤ 10 mm/s
2	Arrêt et empêchement du démarrage du mouvement de descente	Tablier mobile	Actionnement de la pédale PED en position 3	Mode réglage et vitesse ≤ 10 mm/s
3	Arrêt et empêchement du démarrage du mouvement de descente	Tablier mobile	Occultation de la barrière immatérielle	Mode production
4	Arrêt et empêchement du démarrage du mouvement de descente	Tablier mobile	Ouverture du protecteur latéral droit	Dans tous les modes de fonctionnement
5	Arrêt et empêchement du démarrage du mouvement d'avance	Butée arrière	Ouverture du protecteur latéral droit	Dans tous les modes de fonctionnement

Tableau 9 : Identification des fonctions de sécurité

Le Tableau 10 présente un exemple de spécification de la fonction de sécurité n° 3 identifiée précédemment.

Spécification de la fonction de sécurité	
N°	**Nom de la fonction de sécurité**
3	***Arrêt du mouvement de descente du tablier par occultation de la barrière immatérielle, en mode production***
Conditions d'activation de la fonction	Cette fonction est active dans le mode « *Production* » ; elle est inactive lorsque le mode de marche « *Production* » n'est pas validé.
Interface de la fonction	Entrées : - Champ de protection de la barrière immatérielle Sortie : - Tablier mobile supérieur.
Description de la fonction	Lorsque cette fonction de sécurité est active : elle consiste à arrêter et empêcher le démarrage du mouvement de descente du tablier mobile en cas d'occultation du champ de protection de la barrière immatérielle et à autoriser ce même mouvement lorsque le champ de protection de la barrière immatérielle est libre.
Priorité par rapport à d'autres fonctions simultanées	Cette fonction de sécurité doit être prioritaire sur la fonction n° 7 de commande « standard » du mouvement de descente du tablier.
Autres fonctions de sécurité agissant sur le même élément mobile	Les fonctions de sécurité n°1, 2 et 4 agissent sur le même élément mobile que cette fonction de sécurité pour arrêter et empêcher le démarrage du même mouvement.
Temps de réaction maximal de la fonction	Compte tenu des distances de sécurité à respecter, le temps de réaction maximal du système de commande compris entre l'occultation du champ de protection de la barrière immatérielle et l'arrêt du mouvement de descente du tablier ne doit pas dépasser 160 ms.

Tableau 10 : Spécification de la fonction de sécurité n° 3

Quelques remarques concernant les différentes informations

- Condition d'activation de la fonction

  Cette information est importante pour les fonctions de sécurité qui ne sont pas actives en permanence (par exemple suivant le mode de fonctionnement de la machine), ce qui est le cas de cette fonction.

- Interface de la fonction de sécurité

  En entrée, on retrouve le ou les éléments déclencheurs de l'action de sécurité (ici, le champ de protection de la barrière immatérielle). En sortie, on retrouve le ou les éléments sur lesquels va agir la fonction de sécurité (ici, le tablier mobile).

- Description de la fonction de sécurité

  Elle doit faire clairement apparaître :

  - le déclencheur de l'action de sécurité (ici, la barrière immatérielle),
  - l'état du déclencheur qui active la fonction de sécurité (ici, occultation du champ de protection),
  - l'action de sécurité (ici un arrêt), en étant le plus précis possible,

- l'élément mobile dangereux sur lequel agit la fonction de sécurité (ici, le mouvement de descente du tablier mobile).

➢ Priorité par rapport à d'autres fonctions simultanées

Les fonctions simultanées sont des fonctions de sécurité ou des fonctions de commande « standard » qui agissent sur le même élément mobile que la fonction de sécurité traitée. Ces fonctions sont susceptibles de perturber la fonction traitée lorsqu'elles sont sollicitées simultanément. Par exemple, lorsque la fonction de sécurité n° 3 d'arrêt du tablier et la fonction « standard » n° 7 de commande de descente du tablier sont sollicitées simultanément, la fonction de sécurité n° 3 doit être prioritaire.

➢ Autres fonctions de sécurité agissant sur le même élément mobile

Lorsque plusieurs fonctions de sécurité agissent sur le même élément mobile (cas des fonctions de sécurité n° 1, 2, 3 et 4 dans notre exemple), il faudra au niveau du circuit de commande, réaliser une fonction logique pour que chacune de ces fonctions de sécurité puissent s'effectuer (ex : commander l'arrêt de l'élément mobile commun) sans perturber les autres, toutes aussi importantes. Il est donc conseillé de les recenser dès le stade des spécifications afin de tenir compte de cette fonction logique comme d'une spécification propre à chaque fonction de sécurité concernée.

➢ Temps de réaction maximal de la fonction de sécurité

Il faut renseigner ce paramètre avec le temps de réaction maximal admissible pour traiter la fonction de sécurité depuis le déclenchement de l'action de sécurité jusqu'à l'action de sécurité générée par la fonction.

Dans le cas de cette fonction, le temps de réaction court depuis l'occultation du champ de protection de la barrière immatérielle jusqu'à l'arrêt complet de l'élément mobile « dangereux » : le tablier mobile supérieur. Il inclut donc le temps de réaction du circuit de commande électrique et hydraulique et le temps de réaction de la partie mécanique.

B4. Architecture du circuit de commande du tablier de la presse plieuse

Dans cet exemple, le circuit hydraulique de la presse plieuse, comprenant les fonctions de commande et les fonctions de sécurité du mouvement de descente, n'est pas constitué de composants indépendants pour chacune des fonctions, mais d'un « bloc hydraulique » du commerce où les composants de commande du mouvement de descente du tablier et ceux propres à la fonction de maintien et d'arrêt en sécurité sont combinés. Il n'est donc pas possible de séparer, au niveau du circuit de commande hydraulique, les fonctions de commande de celles de sécurité ; cette imbrication impose de gérer en sécurité l'ensemble des commandes hydrauliques du mouvement de descente du tablier (descente et arrêt).

De ce fait, les fonctions de commande ont une interface commune avec les fonctions de sécurité au niveau du circuit de commande électrique. Il revient donc au SRECS de gérer la priorité entre ces fonctions, ce qui ajoute une difficulté supplémentaire au développement du SRECS.

La Figure 18 illustre l'architecture matérielle de la presse plieuse prise en exemple.

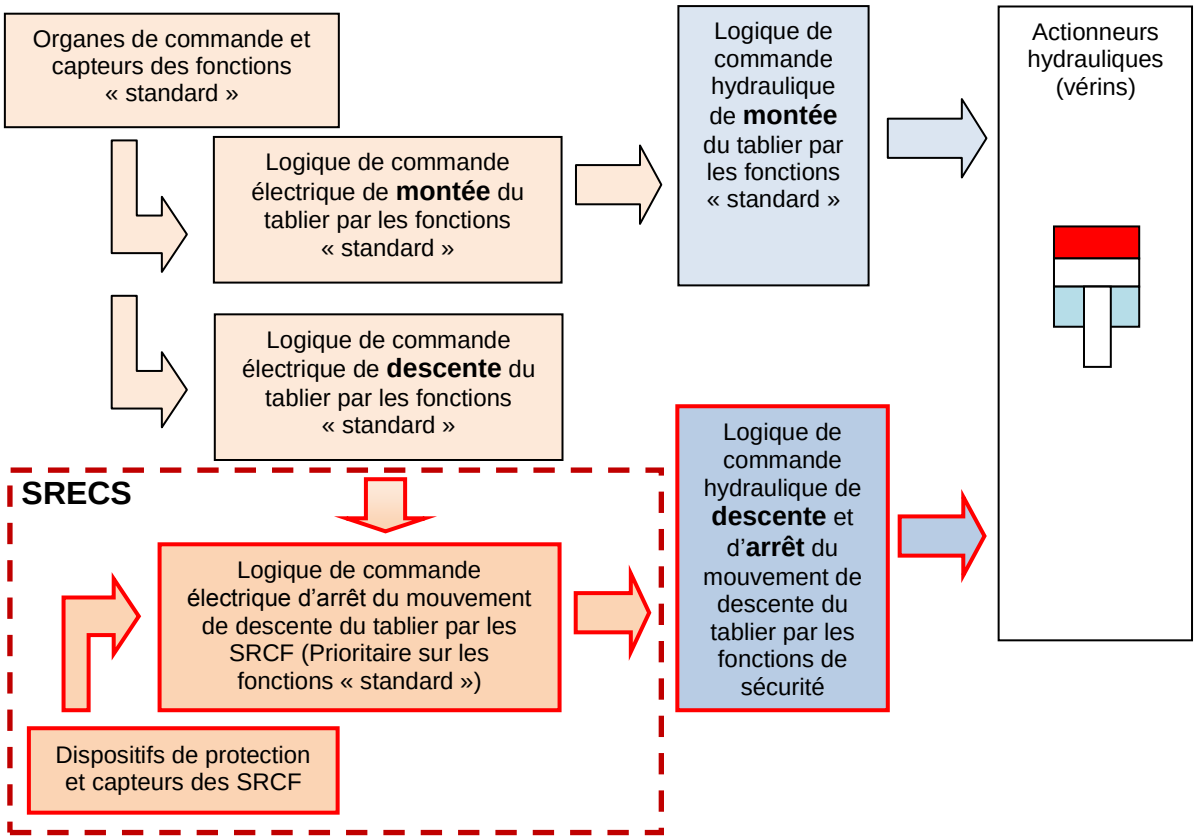


Figure 18 : Exemple d'architecture du circuit de commande complet du tablier de la PPH

Cet exemple fait apparaître :

- les parties de commande électrique et hydraulique dédiées spécifiquement et uniquement au traitement des fonctions de commande « standard », qui gèrent le mouvement « non dangereux » de montée du tablier,
- la partie de commande hydraulique relative à la sécurité dédiée spécifiquement au mouvement « dangereux » de descente du tablier,
- le SRECS qui traite les parties électrique/électronique des fonctions de sécurité d'arrêt du mouvement de descente du tablier ainsi que leur priorité par rapport aux fonctions de commande « standard » de ce mouvement.

Les parties contribuant aux fonctions de sécurité sont entourée de rouge. Elles font intervenir le SRECS ainsi que le système de commande hydraulique.

B5. Identification de l'interface entre le SRECS et le circuit de commande hydraulique du tablier de la presse plieuse

Les composants hydrauliques, mis en œuvre pour assurer les fonctions de sécurité liées au tablier mobile, sont issus du Tableau 8, présenté dans l'annexe A de ce document. Les composants pilotés par le SRECS sont uniquement ceux qui agissent sur le mouvement de descente du tablier mobile afin d'assurer son empêchement ou sa mise à l'arrêt. Dans le cas présent, ce mouvement est obtenu par deux vérins indépendants Y1 et Y2 dont la fonction de sécurité d'arrêt est obtenue par deux composants hydrauliques distincts pour chacun des vérins.

Vérins	**Y1**		**Y2**	
Distributeurs / **Mouvements**	Commande Descente Proportionnelle **PDG**	Commande Descente Retenue **EV4**	Commande Descente Proportionnelle **PDD**	Commande Descente Retenue **EV5**
Descente (GV)	1	1	1	1
Descente (PV)	1	1	1	1
Montée	0	0	0	0
Arrêt	0	0	0	0

Tableau 11 : Diagramme d'actionnement des distributeurs hydrauliques pilotés par le SRECS

L'interface entre le SRECS et le circuit de commande hydraulique de la presse plieuse se situe au niveau de l'alimentation électrique des distributeurs hydrauliques PDG, EV4 et PDD, EV5.

Annexe C - Formalisation des SRCF

C1. Identification des Fonctions de Commande Relatives à la Sécurité (SRCF)

Certaines priorités entre fonctions mises en évidence lors de la spécification des fonctions de sécurité ne seront pas reprises par les SRCF compte tenu de l'architecture adoptée pour le circuit de commande et des limites définies pour le SRECS. C'est le cas dans l'exemple d'architecture, proposée pour le circuit de commande de la presse plieuse, illustré en Figure 18, où la priorité, entre les fonctions de commande « standard » du mouvement de descente du tablier et les fonctions de sécurité d'arrêt de ce même mouvement, est prise en charge par la partie hydraulique du circuit de commande et donc en dehors du SRECS.

Dans le cas présent, les fonctions de sécurité (n° 1 à 5) identifiées lors de la phase préparatoire font toutes intervenir, pour tout ou partie, le circuit de commande électrique et donc le SRECS. Chacune de ces fonctions de sécurité énumérées Tableau 9 devra donc être déclinée en une SRCF telle que représenté dans le Tableau 12 ci-après.

N° Fonction de sécurité	N° SRCF	Nom de la SRCF
1	A	Arrêt descente tablier par relâchement pédale PED
2	B	Arrêt descente tablier par actionnement pédale PED position 3
3	C	Arrêt descente tablier par barrière immatérielle
4	D	Arrêt descente tablier par protecteur latéral
5	E	Arrêt moteur avance butée par protecteur latéral

Tableau 12 : Liste des SRCF prises en compte dans ce document

C2. Spécifications des exigences fonctionnelles des SRCF

Le Tableau 13 présente, en exemple, les spécifications de la SRCF n° C. Ces spécifications sont déduites des spécifications de la fonction de sécurité n° 3 dont le détail est fourni Tableau 10 de ce document.

Spécification des exigences fonctionnelles de la SRCF	
N°	**Nom de la SRCF**
C	**Arrêt descente tablier par barrière immatérielle**
Conditions d'activation de la SRCF	Cette SRCF est active lorsque le mode de marche « *Production* » est validé ; elle est inactive lorsque le mode de marche « *Production* » n'est pas validé. Il n'est pas validé si un autre mode de marche est validé ou si plusieurs modes de marche sont sélectionnés simultanément ou si aucun mode de marche n'est sélectionné.
Interface de la SRCF	Entrée : - champ de protection de la barrière immatérielle. Sortie : - l'alimentation électrique des distributeurs hydrauliques commandant la descente du tablier PDG, PDD, EV4 et EV5 (voir Tableau 11).
Description de la SRCF	Lorsqu'elle est active, cette SRCF consiste à couper l'alimentation électrique des distributeurs hydrauliques de commande du mouvement de descente du tablier lorsque le champ de protection de la barrière immatérielle est occulté et à autoriser l'alimentation électrique de ces distributeurs lorsque le champ de protection de la barrière immatérielle est libre.
Priorité par rapport à d'autres fonctions simultanées	Cette SRCF doit être prioritaire sur la fonction de commande « standard » d'alimentation électrique des distributeurs hydrauliques de commande du mouvement de descente du tablier.
Autres SRCF agissant sur la même interface de sortie	Les SRCF A, B et D agissent sur la même interface de sortie que cette SRCF pour arrêter ou autoriser l'alimentation électrique des distributeurs hydrauliques de commande du même mouvement.
Temps de réaction maximal de la SRCF	Le temps de réaction maximal du SRECS compris entre l'occultation du champ de protection de la barrière immatérielle et la coupure de l'alimentation électrique des distributeurs hydrauliques de commande du mouvement de descente du tablier ne doit pas dépasser 80 ms.
Fréquence de fonctionnement de la SRCF	1 fois/minute (cas d'une presse plieuse qui travaille 8 heures par jour, pendant 220 jours par an - La fréquence moyenne de travail est de 60 coups par heure).
Réaction aux fautes/Conditions de redémarrage	La réaction en cas de défaut doit conduire à couper l'alimentation électrique des distributeurs hydrauliques de commande du mouvement de descente du tablier et maintenir cette coupure tant que l'ensemble des défauts n'est pas éliminé.
Conditions d'ambiance	Respect des préconisations de la norme NF EN 12622 – Degré de protection minimal IP 54.
Taux de cycles de manœuvres, catégorie d'utilisation pour les dispositifs électromécaniques	Non renseigné pour cet exemple car le type de matériel (dispositifs électromécaniques) n'est pas encore défini à cette étape de spécification.

Tableau 13 : Spécifications des exigences fonctionnelles de la SRCF n° C

Quelques remarques concernant les différentes informations

- Interface de la SRCF

  Dans l'exemple de la presse plieuse, le choix de l'entraînement du tablier par des vérins hydrauliques est imposé dès le début et le circuit hydraulique est composé d'un bloc du commerce, les distributeurs d'arrêt du mouvement du tablier sont clairement identifiés. La spécification de l'interface de sortie entre le SRECS et le reste du circuit de commande peut donc faire référence à l'alimentation électrique de ces composants hydrauliques.

- Description de la SRCF

  Elle doit faire clairement apparaître :

  - le déclencheur de la fonction ou l'interface avec le déclencheur si celui-ci ne fait pas partie du SRECS (dans l'exemple présent, la barrière immatérielle qui est le déclencheur de la fonction fait partie du SRECS),
  - l'état du déclencheur qui active la SRCF (ouvert-fermé, libre-occulté) : dans notre exemple, c'est le champ de protection occulté qui active la SRCF),
  - le résultat attendu (ici une coupure d'alimentation), en étant le plus précis possible,
  - l'organe ou l'interface, lorsque le SRECS ne réalise pas l'intégralité de la fonction de sécurité, sur lequel agit la SRCF : dans notre exemple, la fonction de sécurité agit sur le tablier mobile, alors que la SRCF se borne à agir sur l'interface entre le SRECS et le circuit hydraulique de commande du mouvement de descente du tablier.

- Priorité par rapport à d'autres fonctions simultanées

  Dans l'exemple présent, l'architecture présentée dans la Figure 18 pour la réalisation du système de commande nous montre que la priorité des fonctions de sécurité par rapport aux ordres de commande « standard » du mouvement dangereux devra être gérée par le SRECS et donc prise en compte par cette SRCF.

- Autres SRCF agissant sur la même interface de sortie

  Dans l'exemple présent, l'identification des fonctions de sécurité effectuée dans le Tableau 9 nous montrent que d'autres SRCF vont agir sur la même interface de sortie.

- Temps de réaction maximal de la SRCF

  Dans notre cas, le temps de réponse maximal de la fonction de sécurité n° 3 est de 160 ms. Le temps de réaction de la partie hydraulique du traitement de cette fonction étant de 80 ms, le temps de réaction maximal de la SRCF C est donc de 80 ms.

C3. Spécifications des exigences d'intégrité de sécurité des SRCF

L'exemple suivant traite de la détermination du SIL requis pour la SRCF n° C « Arrêt descente tablier par barrière immatérielle ». Les critères à prendre en compte sont décrits ci-après.

- Gravité du dommage – Se, de 1 à 4

  La gravité a été évaluée en tenant compte des phénomènes dangereux identifiés et des parties du corps pouvant être affectées.

- Probabilité d'apparition d'un dommage

  Les préconisations du ***§ A.2.4 de l'annexe A*** de la norme NF EN 62061 doivent être respectées. Pour le cas de la SRCF n° C « *Arrêt descente tablier par barrière immatérielle*», une description des risques propres au mode de marche « production » dans lequel la SRCF est active a été effectuée, en rappelant le phénomène dangereux, la zone dangereuse correspondante et les personnes exposées.

Ensuite, l'analyse des tâches a été effectuée, en prenant en compte les cas les plus défavorables. Les phases de travail et les situations génératrices de risques correspondantes ont été définies dans les phases où la SRCF est active.

- Fréquence et durée d'exposition - Fr, de 2 à 5

  Elles dépendent directement de l'usage prévu de la presse plieuse. La fréquence est estimée en prenant en compte le nombre de plis effectués. La durée correspond au temps pendant lequel les mains de l'opérateur maintiennent la tôle « *sous la protection de la SRCF* » soit dans notre cas, depuis l'introduction de la tôle entre les outils jusqu'à son retrait de la zone de pliage et sur toute la course de descente du tablier.

- Probabilité d'apparition d'un évènement dangereux – Pr, de 1 à 5

  Au sens de la norme NF EN ISO 14121-1, un évènement dangereux est un évènement susceptible de causer un dommage, à court ou à long terme. L'occurrence d'un évènement dangereux peut être d'origine technique ou humaine. Pour la presse plieuse le phénomène dangereux identifié est le mouvement de descente du tablier mobile (fermeture des outils). L'événement est dangereux lorsque les mains de l'opérateur sont soumises au phénomène dangereux identifié. Dans notre cas lorsque les mains de l'opérateur se trouvent dans la zone de fermeture des outils.

  Pour pouvoir apprécier cette probabilité, sur la base des éléments du ***§ A.2.4.2 de l'annexe A*** et en se basant notamment sur des historiques d'accidents, l'INRS a procédé de la manière suivante :

  - création d'une liste des éléments qui diminuent la probabilité d'apparition d'un évènement dangereux,
  - création d'une liste de ceux qui l'augmentent,
  - jugement global, sur la base de ces éléments, de la probabilité pour attribution d'un score de 1 à 5.

- Probabilité d'évitement ou de limitation du dommage – AV, 1, 3 et 5

  Pour pouvoir apprécier cette probabilité, sur la base des éléments du ***§ A.2.4.3 de l'annexe A***, l'INRS a procédé de la manière suivante :

  - création d'une liste des éléments qui diminuent la probabilité d'évitement ou de limitation du dommage,
  - création d'une liste de ceux qui l'augmentent,
  - jugement global, sur la base de ces éléments, de la probabilité pour attribution d'un score de 1, 3 ou 5.

Rappel : La SRCF n° C est active dans le mode production, elle met en œuvre un dispositif de protection (barrière immatérielle) destiné à couvrir les risques liés à un phénomène dangereux (fermeture des outils de la presse plieuse) consécutif au mouvement de descente du tablier mobile supérieur de cette machine.

Le Tableau 14 récapitule les éléments pris en compte.

Estimation du risque et attribution du SIL requis pour la SRCF n° C	
Critères d'appréciation	**Eléments d'appréciation et résultats de l'analyse**
Phénomène dangereux	Mouvement de fermeture des outils de la presse plieuse (descente du tablier mobile supérieur).
Risques *(avec détail des phénomènes dangereux, des zones dangereuses correspondantes et des personnes exposées).*	**Risque 1 – Ecrasement/sectionnement** - entre les outils lors de leur fermeture - Opérateur ou tierce personne (blessure aux membres supérieurs, possible à la tête mais pas de cas répertorié). **Risque 2 - Choc** - par le tablier mobile ou les outils lors de leur fermeture - Opérateur ou tierce personne (blessure aux membres supérieurs ou à la tête). **Risque 3 - Coupure/Cisaillement** – entre la tôle et le tablier pendant la phase de pliage - Opérateur (blessure aux doigts).
Phases de travail/situations génératrices de risques Il faut considérer la phase ou la situation de travail pour laquelle le dispositif de protection (donc la SRCF), destiné à couvrir les risques qui lui sont associés, est actif.	- Maintien manuel de la tôle sur la matrice avant et durant le pliage, les mains sont à proximité de l'outil - risques 1 et 2. - Maintien manuel en plaquant la tôle en butée avant et durant le pliage (risque d'échappement de la tôle/à la butée) - risques 1 et 2. - Accompagnement/maintien manuel de la tôle lors du pliage - risque 3. - Rapprochement de la tête de l'opérateur pour visualisation d'un traçage sur la tôle et alignement avec l'axe de pliage - risques 1 et 2.
Sévérité des dommages (Se)	L'estimation du paramètre se fait dans le pire cas **Se = 4**
Fréquence et durée de l'exposition (pour une durée > 10 mn). *Pour simplifier la compréhension, la notion de fréquence est remplacée par le nombre d'accès par période de temps*	Prise en compte de la fréquence de travail prévue lors de l'élaboration du cahier des charges de la presse plieuse et reprise dans l'estimation des risques (cf. Annexe A2) **Résultat de l'analyse : Fr = 5**

Estimation du risque et attribution du SIL requis pour la SRCF n° C	
Critères d'appréciation	**Eléments d'appréciation et résultats de l'analyse**
Probabilité d'apparition des événements dangereux	*Eléments qui diminuent la probabilité d'apparition de l'événement dangereux* ✓ *Pour le travail, les mains de l'opérateur ne sont pas placées dans la zone dangereuse, mais en dehors, pour maintenir la tôle.* ✓ *Lors du maintien de la tôle, cette dernière est en butées. Les mains sont hors de la zone dangereuse.* ✓ *La pédale de commande est capotée pour éviter les risques de démarrage intempestifs.* ✓ *Les mains de l'opérateur sont éloignées de la zone dangereuse si la taille des pièces est importante.* *Eléments qui augmentent la probabilité d'apparition de l'événement dangereux* ✓ *Tablier descendant (gravité).* ✓ *Cadences fortes (stress,…).* ✓ *Mains de l'opérateur pouvant être très proches de la zone dangereuse si la taille des pièces est faible.* **Résultat de l'analyse : Pr = 4**
Probabilité d'évitement ou de limitation du dommage	*Eléments qui diminuent la probabilité d'évitement ou de limitation du dommage* (AV↑) ✓ *Mouvements dangereux à vitesse rapide* *Eléments qui augmentent la probabilité d'évitement ou de limitation du dommage* (AV↓) ✓ *Possibilité spatiale de s'écarter du phénomène dangereux, car espace suffisant.* ✓ *Reconnaissance du phénomène dangereux, par visualisation du mouvement du tablier.* *Maîtrise du mouvement par action volontaire et maintenue sur un organe de commande.* **Résultat de l'analyse : Av = 3**
Classe de probabilité d'un dommage CL = Fr + Pr + Av	**CL = 5 + 4 + 3 = 12**
Attribution d'un SIL ***Tableau A.6*** de la norme NF EN 62061	**SIL = 3**

Tableau 14 : Estimation du SIL requis pour la SRCF n° C

Le SIL requis pour les autres fonctions est fourni à titre indicatif dans le Tableau 15, sans les détails de l'analyse, simplement pour permettre la poursuite de la description de la démarche de conception.

N°	Nom de la SRCF	SIL Requis
A	Arrêt descente tablier par relâchement pédale PED	2
B	Arrêt descente tablier par actionnement pédale PED position 3	3
C	Arrêt descente tablier par barrière immatérielle	3
D	Arrêt descente tablier par protecteur latéral	2
E	Arrêt moteur avance butée par protecteur latéral	1

Tableau 15 : Récapitulatif du SIL requis de chacune des SRCF de la presse plieuse

C4. Conception d'une SRCF

La complexité du SRECS de la presse plieuse vient du fait qu'elle comprend :

- des conditions d'activation des SRCF telles que la sélection des modes de marche, pour gérer des SRCF ayant à agir sur un actionneur commun,
- des SRCF, de SIL requis différents ou pas, prenant en compte une même information d'entrée (par ex : les SRCF n° D et E),
- des SRCF, de SIL requis différents ou pas, agissant en sortie sur le même actionneur ou la même interface (par ex : les SRCF n° A, B, C et D),
- des priorités entre les SRCF et des fonctions de commande « standard ».

Ce document détaille, dans les paragraphes suivants, les analyses nécessaires pour traiter ces cas représentatifs de nombreuses applications de l'industrie.

Pour décrire les principes généraux à mettre en œuvre, ce document s'appuie sur l'exemple de la SRCF n° C.

C4.1 Analyse/décomposition d'une SRCF en blocs fonctionnels

Le traitement de la SRCF n° C permet d'aborder les aspects suivants :

- une condition d'activation propre à cette SRCF (le mode de marche « production »),
- elle agit sur la même interface de sortie que d'autres SRCF, de SIL requis différents,
- une priorité entre cette SRCF et une fonction de commande « standard » agissant sur la même interface de sortie.

Cet exemple s'appuie sur les spécifications des exigences fonctionnelles décrites dans le Tableau 13 et sur le SIL requis « SIL 3 » déterminé Tableau 14 de ce document.

Détermination des éléments nécessaires pour la décomposition en blocs fonctionnels

Les éléments pris en compte pour cette SRCF déterminés sur la base de ses spécifications (Tableau 13) et les références des blocs fonctionnels qui ont été créés sont décrits ci-après :

- les informations dont l'acquisition est nécessaire
    - champ de protection de la barrière immatérielle [bloc fonctionnel BF5]
    - les conditions d'activation de la SRCF, ici les informations issues de la sélection des modes de marche [bloc fonctionnel BF8]
    - nature et état des autres SRCF n° A, B et D agissant sur la même interface
    - nature et état de l'ordre de commande « standard » agissant sur la même interface ou sur le même actionneur.
- les actions de sortie à obtenir
    - couper ou autoriser l'alimentation électrique des distributeurs hydrauliques de commande du mouvement de descente du tablier [bloc fonctionnel BF16].
- la logique à réaliser pour assurer la fonction de sécurité
    - lorsque le mode « production » est validé, la logique de cette SRCF consiste à couper l'alimentation électrique des distributeurs hydrauliques de commande du mouvement de descente du tablier lorsque le champ de protection de la barrière immatérielle est occulté et à autoriser l'alimentation électrique de ces distributeurs lorsque le champ de protection de la barrière immatérielle est libre [bloc fonctionnel BF11].
- prendre en compte l'état des autres SRCF n° A, B et D agissant sur la même interface
    - définition de l'état attendu de cette SRCF lorsque le mode « production » n'est pas validé afin de permettre le fonctionnement des autres modes de marche [bloc fonctionnel BF11] :
        - lorsqu'un autre mode (réglage) est validé, la logique de cette SRCF consiste à autoriser l'alimentation électrique des distributeurs hydrauliques de commande du mouvement de descente du tablier,
        - lorsqu'aucun mode de marche n'est validé (si plusieurs modes de marche sont sélectionnés simultanément ou si aucun mode de marche n'est sélectionné), la logique de cette SRCF consiste à couper l'alimentation électrique de ces distributeurs.
    - logique à réaliser, sur la base de l'état des SRCF n° A, B, C et D afin qu'elles puissent toutes agir sur la même interface sans se perturber [bloc fonctionnel BF14].
- gérer la priorité de la SRCF sur l'ordre de commande « standard » du mouvement de descente du tablier [bloc fonctionnel BF15].

Découpage en blocs fonctionnels

La structure retenue pour le découpage en blocs fonctionnel de cette SRCF, qui est un exemple parmi toutes les variantes possibles, fait apparaître entre autres :

- La création de blocs fonctionnels spécifiques pour gérer les interactions avec les autres SRCF (BF 14) et la priorité vis-à-vis de la fonction de commande standard (BF 15). Cette façon de procéder permet « d'attacher » ces spécificités, qui ne font pas partie intégrante de la fonction de sécurité définie à la base, à la SRCF concernée. Elle permet également, de s'assurer que ces spécificités seront effectivement prises en compte par un sous-système.
- Le regroupement, au sein d'un même bloc fonctionnel (BF 14), des actions communes des différentes SRCF (sorties des BF de traitement des SRCF n° A, B, C et D) agissant sur la même interface. Ce regroupement génère une information unique représentative de l'état de toutes ces SRCF. Dans cette structure, les blocs fonctionnels BF 15 et BF 16 deviennent communs à toutes ces SRCF et seront donc utilisés pour leur décomposition en blocs fonctionnels.

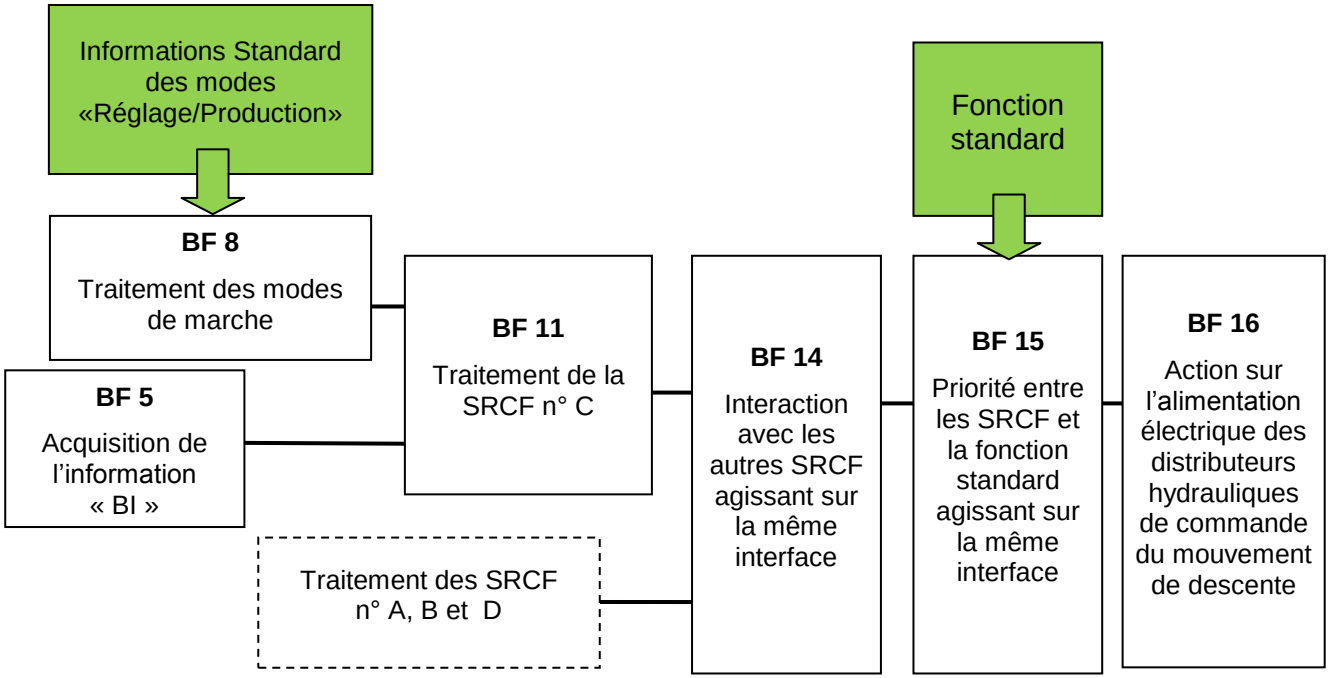


Figure 19 : Découpage en blocs fonctionnels de la SRCF n° C

Spécifications des blocs fonctionnels

Bloc fonctionnel BF5 – Acquisition de l'information « BI »

- Entrée : Contrôle du champ de protection de la barrière immatérielle
- Sortie : Etat du champ de protection – « libre » ou « occulté »
- Logique : Le champ de protection est « libre » lorsque la barrière immatérielle ne détecte aucune présence, le champ de protection est « occulté » lorsque la barrière immatérielle détecte au moins un membre supérieur.

Bloc fonctionnel BF8 – Traitement des modes de marche

- Entrée : Informations du mode de marche sélectionné (réglage, production)
- Sortie : Mode (réglage ou production ou « aucun mode actif »)
- Logique : L'information du mode de marche en entrée est validée en sortie si un seul mode de marche est sélectionné. L'information « aucun mode actif » est transmise en sortie si aucun mode n'est sélectionné ou si plusieurs modes sont sélectionnés simultanément.

Bloc fonctionnel BF11 – Traitement de la SRCF n° C

- Entrées : Etat du champ de protection de la barrière immatérielle (BF5)
  Mode (réglage ou production ou « aucun mode actif ») (BF8)
- Sortie : Etat de la SRCF n° C – « arrêt » ou « autorisation » du mouvement de descente du tablier
- Logique : La sortie donne un ordre « arrêt » si :
  - L'information du mode est « aucun mode actif »,
  - Ou l'information du mode est « production » et le champ de la barrière immatérielle est « occulté »

  La sortie donne un ordre « autorisation » si :
  - L'information du mode est « production » et le champ de la barrière immatérielle est « libre »
  - Ou l'information du mode est « réglage ».

Bloc fonctionnel BF14 – Interaction avec les autres SRCF agissant sur le mouvement du tablier via la même interface

- Entrées : Etat de la SRCF n° A « arrêt » ou « autorisation » du mouvement de descente du tablier (BF9)
  Etat de la SRCF n° B « arrêt » ou « autorisation » du mouvement de descente du tablier (BF10)
  Etat de la SRCF n° C « arrêt » ou « autorisation » du mouvement de descente du tablier (BF11)
  Etat de la SRCF n° D « arrêt » ou « autorisation » du mouvement de descente du tablier (BF12)
- Sortie : Etat de l'autorisation du mouvement de descente du tablier – « ARRET » ou « AUTORISATION »
- Logique : la sortie donne un ordre « ARRET » si l'une au moins des entrées fournit un ordre « arrêt »
  La sortie donne un ordre « AUTORISATION » si toutes les entrées fournissent un ordre « autorisation ».

Bloc fonctionnel BF15 – Priorité entre les SRCF et la fonction de commande « standard » agissant sur le mouvement du tablier via la même interface

- Entrées : Informations de commande « standard » du mouvement du tablier « arrêt descente » ou « marche descente »

  Etat de l'autorisation du mouvement de descente du tablier – « ARRET » ou « AUTORISATION » (BF14)
- Sortie : Arrêt prioritaire du mouvement de descente du tablier – « ARRET » ou « transmission des informations de commande standard »
- Logique : Si l'autorisation du mouvement de descente du tablier fournit un ordre « ARRET », la sortie donne un ordre « ARRET ».

  Si l'autorisation du mouvement de descente du tablier fournit un ordre « AUTORISATION », la sortie prend l'état de l'information de commande « standard » du mouvement du tablier (arrêt descente ou marche descente).

Bloc fonctionnel BF16 – Action sur l'alimentation électrique des distributeurs hydrauliques de commande du mouvement de descente

- Entrée : Arrêt prioritaire du mouvement de descente du tablier « ARRET » ou « transmission des informations de commande standard » (BF15)
- Sortie : Action sur l'alimentation électrique des distributeurs hydrauliques commandant la descente du tablier PDG, EV4, PDD et EV5
- Logique : Mise en forme du signal pour exploitation par les distributeurs hydrauliques. Lorsque l'état de l'arrêt prioritaire du mouvement de descente du tablier est « ARRET », l'alimentation électrique des distributeurs hydrauliques commandant la descente du tablier est coupée. Lorsque cet état est « transmission des informations de commande standard », l'alimentation est dépendante de la commande standard.

C4.2 Attribution de sous-systèmes aux blocs fonctionnels d'une SRCF

Attribution d'un sous-système à chaque bloc fonctionnel

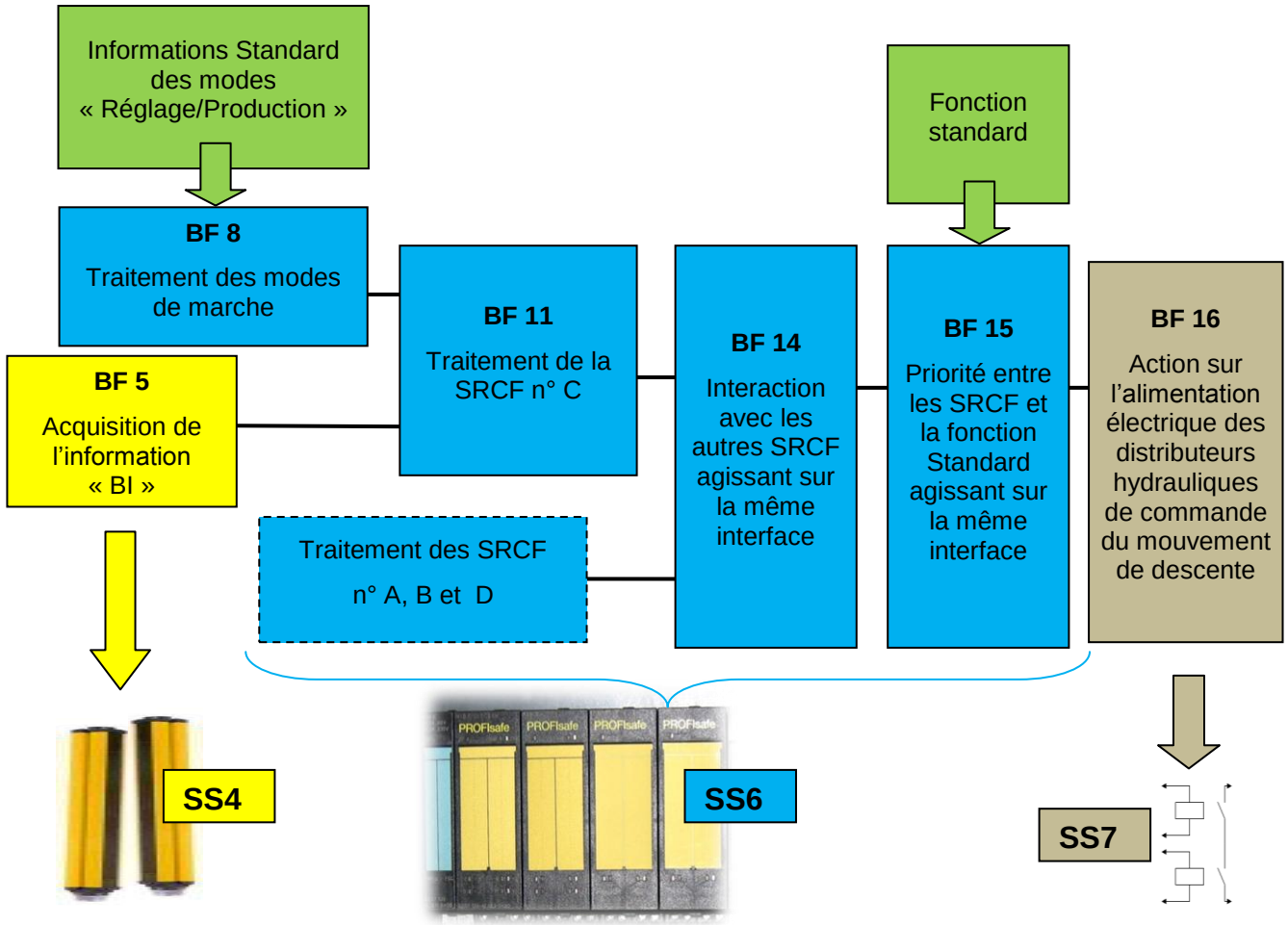


Figure 20 : Attribution des sous-systèmes pour la SRCF n° C

Sous-systèmes envisagés

Sous-système SS4 : le bloc fonctionnel BF5, représenté en jaune, sera attribué au sous-système SS4, constitué d'une barrière immatérielle. Le SIL requis pour cette SRCF est SIL3.

Sous-système SS6 : les blocs fonctionnels BF8, BF11, BF14 et BF 15, représentés en bleu, seront attribués à un même sous-système SS6, capable de traiter des fonctions logiques différentes, équipé d'entrées/sorties compatibles avec les sous-systèmes externes correspondants. Il s'agira dans cet exemple d'un APIdS (Automate Programmable Industriel dédié à la Sécurité). Le SIL requis pour cette SRCF est SIL3.

Sous-système SS7 : le bloc fonctionnel BF16, représenté en kaki, sera attribué au sous-système SS7. Il est constitué d'une interface comprenant un(des) relais électromécanique(s) permettant d'alimenter électriquement les distributeurs hydrauliques PDG, EV4, PDD et EV5 commandant la descente du tablier. Le SIL requis pour cette SRCF est SIL3.

N°	SIL requis	Nom de la SRCF	Blocs fonctionnels	Sous-systèmes impliqués
C	3	Arrêt descente tablier par barrière immatérielle	BF5	SS4
			BF8, BF11, BF14, BF15	SS6
			BF16	SS7

Tableau 16 : Récapitulatif des BF et SS de la SRCF n° C

Annexe D - Spécification et choix / conception d'un sous-système

D1. Informations nécessaires pour le choix ou la conception d'un sous-système

Le SIL requis d'un sous-système doit être supérieur ou égal au plus élevé des SIL requis revendiqué par les SRCF qui utilisent ce sous-système.

Le Tableau 17 fournit un exemple de tableau récapitulatif du SIL requis pour l'ensemble des SRCF traitées, du SIL requis pour les sous-systèmes traitant de ces SRCF ainsi que du(des) bloc(s) fonctionnel(s) affecté(s) à chacun de ces sous-systèmes.

	SIL requis pour la SRCF n° A	SIL requis pour la SRCF n° B	SIL requis pour la SRCF n° C	SIL requis pour la SRCF n° D	SIL requis pour la SRCF n° E	SIL requis du SS	BF pris en compte par le SS
SS1	SIL2	SIL3				**SIL3**	**BF1**
SS2	SIL2					**SIL2**	**BF2**
SS3		SIL3				**SIL3**	**BF3**
SS4			SIL3			**SIL3**	**BF5**
SS5				SIL2	SIL1	**SIL2**	**BF6**
SS6	SIL2	SIL3	SIL3	SIL2	SIL1	**SIL3**	**BF8, BF9, BF10, BF11, BF12, BF14, BF15**
SS7	SIL2	SIL3	SIL3	SIL2		**SIL3**	**BF16**
SS8					SIL1	**SIL1**	**BF17**

Tableau 17 : Récapitulatif du SIL requis pour les sous-systèmes constitutifs des SRCF n° A à E

D'après le Tableau 17, le sous-système SS7, qui traite des SRCF n° A à D avec des SIL revendiqués pour ces fonctions allant de SIL2 à 3, aura un SIL requis de SIL3. Il doit réaliser la fonction du bloc fonctionnel BF 16

D2. Spécifications requises pour le choix/conception d'un sous-système

L'exemple traité concerne le sous-système SS7.

Les informations requises pour le choix du sous-système, listées dans les lignes 1 à 8 du Tableau 2 de ce document, sont précisées dans le Tableau 18.

Spécifications du sous-système SS7	
Type d'information	**Informations requises**
SIL requis	SIL3 minimal
Fonction	Ce sous-système réalise la fonction de BF 16. Lorsque l'entrée est alimentée en tension, les distributeurs hydrauliques PDG, EV4, PDD et EV5 sont alimentés électriquement (descente du tablier commandée). Lorsque l'entrée n'est pas alimentée en tension, les distributeurs hydrauliques PDG, EV4, PDD et EV5 ne sont plus alimentés électriquement (descente du tablier non commandée).
Entrée	Une entrée bipolaire destinée à être commandée en tension, raccordée à une seule sortie bipolaire de l'APIdS gérant la sortie de BF 16. Caractéristiques compatibles avec celles de la sortie correspondante du sous-système SS6 (caractéristiques de courant, tension,…).
Sortie	Quatre sorties bipolaires électromécaniques de type « Tout ou rien » (fonctionnant comme un contact électrique de type « F »), une pour chacun des distributeurs hydrauliques commandant la descente du tablier PDG, EV4, PDD et EV5. Caractéristiques compatibles avec celles des distributeurs (pouvoir de coupure).
Temps de réponse	La somme des temps de réponse des différents sous-systèmes composant la SRCF n° C, y compris le SS7, doit être inférieure ou égal à 80ms. En première approche, le temps de réponse retenu pour le sous-système SS7 est de 8 ms. Cette première approche est obtenue suite à une première estimation des temps de réponse des différents sous-systèmes qui composent le SRECS.
Conditions environnementales	Le relais étant positionné dans l'armoire électrique, son degré de protection est IP 20. Les câbles de raccordement entre le relais et les bobines des distributeurs doivent résister à un environnement industriel.
Fréquence de fonctionnement	1/mn.
PFH_D	Limitée à celle du SIL requis : $< 10^{-7}$.

Tableau 18 : Informations requises pour le choix du sous système SS7

D3. Phases de choix/conception du sous-système SS7

Cet exemple décrit les phases préconisées par la norme pour le choix/conception d'un sous-système de SIL 3 requis. La première phase s'oriente vers le choix d'un composant « type ». Comme cette solution ne convient pas, la deuxième phase consiste à concevoir un sous-système « particulier » en faisant évoluer l'architecture, en procédant à deux itérations, jusqu'à atteindre le SIL requis.

Un concepteur « expérimenté » passera certainement très vite au choix d'un composant « type » répondant intégralement aux spécifications du sous-système ou à la phase de conception décrite en 2ème itération de cet exemple (§ D5) pour mettre immédiatement en œuvre une architecture redondante avec diagnostic. Pour un concepteur qui n'a jamais utilisé la norme NF EN 62061, la

description des différentes phases de conception permettra de bien assimiler les principes de cette norme.

D4. Première phase : choix d'un composant « type » du commerce pour réaliser l'intégralité du sous système SS7 (§ 6.7.3)

Il s'agit, dans un premier temps, de choisir un matériel répondant aux caractéristiques fonctionnelles et de vérifier ensuite s'il est apte à répondre au SIL 3 requis.

Le choix se porte sur un relais électromécanique dont les caractéristiques rappelées dans le Tableau 19 répondent aux spécifications requises pour le sous-système.

Spécifications du matériel choisi pour le sous-système SS7	
Type d'information	**Informations**
SIL	à déterminer – voir ci-dessous.
Fonction	Ce sous-système réalise la fonction de BF 16. Lorsque l'entrée est alimentée en tension, les distributeurs hydrauliques PDG, EV4, PDD et EV5 sont alimentés électriquement (descente du tablier commandée). Lorsque l'entrée n'est pas alimentée en tension, les distributeurs hydrauliques PDG, EV4, PDD et EV5 ne sont plus alimentés électriquement (descente du tablier non commandée).
Entrée	Une bobine destinée à être commandée en tension, raccordée à une seule sortie bipolaire de l'APIdS gérant la sortie de BF 16. Caractéristiques compatibles avec celles de la sortie correspondante du sous-système SS6 (caractéristiques de courant, tension,…).
Sortie	Quatre contacts électromécaniques de type « F », un pour chacun des distributeurs hydrauliques commandant la descente du tablier PDG, EV4, PDD et EV5. Une des bornes de chacune de ces sorties doit être reliée directement à une borne du distributeur correspondant. Caractéristiques compatibles avec celles des distributeurs (pouvoir de coupure).
Temps de réponse	7 ms
Conditions environnementales	IP 20. Les câbles de raccordement entre le relais et les bobines des distributeurs sont prévus pour résister à un environnement industriel.
Fréquence de fonctionnement	Ce relais est compatible avec la fréquence de 1/mn requise.
PFH_D	Valeur à calculer.

Tableau 19 : Caractéristiques du matériel choisi pour le sous-système SS7

Le raccordement envisagé pour le sous-système SS7 est présenté Figure 21

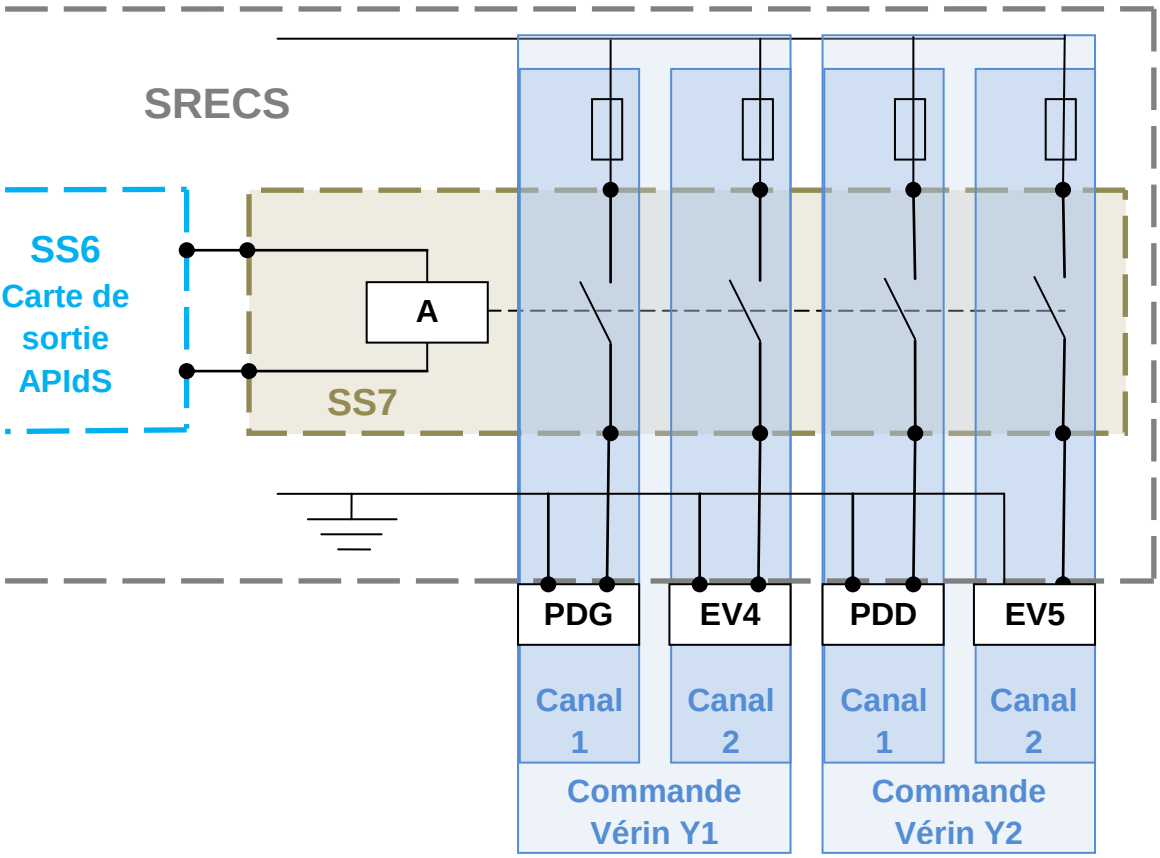


Figure 21 : Raccordement envisagé pour le sous-système SS7

Le SIL et la PFH_D du sous-système doivent être déterminés. Les caractéristiques du relais électromécanique envisagé fournies par le fabricant et nécessaires sont présentées dans le Tableau 20.

Caractéristiques	Unité	Valeur
B10	manœuvre	1.10^6
Relais à contacts liés suivant EN 50205		oui
Proportion de défaillances menant l'ensemble du relais à un état identique à sa position « repos » - état 0	%	50
proportion de défaillances menant l'ensemble du relais à un état identique à sa position « travail » - état 1	%	50
Durée de vie	année	20

Tableau 20 : Caractéristiques du relais électromécanique envisagé

D4.1 Détermination du SIL pouvant être revendiqué par le sous-système

D4.1.1 Détermination du SIL vis-à-vis des contraintes architecturales du sous-système SS7

Estimation de la tolérance aux anomalies du matériel

Dans le cas présent, le sous-système SS7 est composé d'un seul élément de sous-système qui est le relais électromécanique. Potentiellement, sa défaillance peut affecter les SRCF auxquelles il participe et de manière dangereuse. Par exemple, si ce relais est bloqué à l'état passant de ses contacts de sortie, le mouvement de descente en cas de sollicitation de la barrière immatérielle ne pourra plus être arrêté.

Une seule défaillance est susceptible de provoquer la perte de la SRCF, donc la tolérance aux anomalies du sous-système est de « 0 ».

Estimation de la proportion de défaillance en sécurité

Pour estimer ce paramètre, il faut procéder à une analyse des modes de défaillance du sous-système, en vue de déterminer la proportion de défaillances en sécurité (SFF) et celle des défaillances provoquant la perte de la SRCF. Pour le cas du relais électromécanique choisi, les modes de défaillance et leurs conséquences sont récapitulées dans le Tableau 21.

Modes de défaillance	Conséquence pour la SRCF	Pourcentage de défaillance dangereuse $\%d_D$	Pourcentage de défaillance en sécurité $\%d_S$
Relais global à l'état 1	Potentiellement dangereux	50	
Relais global à l'état 0	Sécurité		50

Tableau 21 : Modes de défaillance du relais électromécanique choisi

Notes :

- Dans cet exemple, les défaillances des contacts prises indépendamment n'ont pas été étudiées, car le relais étant à contacts liés, ce type de défaut n'est pas pris en compte. Seules les défaillances du relais global sont donc étudiées.
- Si les modes de défaillance ne sont pas fournis par le fabricant, ***l'annexe D*** de la norme NF EN 62061 fournit des exemples de modes de défaillance de composants couramment utilisés.

La proportion de défaillances en sécurité (*SFF*) est calculée en utilisant l'équation détaillée au § 8.4.1 de ce document

$$\textbf{SFF}\ (\text{exprimé en \%}) = [\ \sum \%d_S + \sum \%d_{DD}\ ] / [\ \sum \%d_S + \sum \%d_D\ ]$$

où

$\%d_S$ = 50

$\%d_D$ = 50

$\%d_{DD}$ = 0 car il n'y a pas de fonction de diagnostic.

Dans le cas du relais unique, sans fonction de diagnostic pour détecter d'éventuelles défaillances dangereuses, la SFF est :

$$\textbf{SFF} = \textbf{(50 + 0) / (50 + 50) = 50 \%}$$

D'après le ***tableau 5*** de la norme NF EN 62061, pour une proportion de défaillance en sécurité **SFF = 50%** et pour une tolérance aux anomalies de **« 0** », le SIL maximal pouvant être revendiqué est « **Non autorisé** ».

D4.1.2 Conclusions sur le SIL de SS7

Le sous-système « SS7 » ne peut donc pas être utilisé en l'état pour réaliser une SRCF de SIL 3 requis. Il faut donc faire évoluer l'architecture du sous-système.

Précisions sur l'usage d'un sous-système composé d'un seul élément de sous-système, de tolérance aux anomalies de « 0 », pour une SRCF de SIL 3.

Pour atteindre un SIL 3 en ayant recours à une architecture de tolérance aux anomalies de 0, le ***§ 6.7.6.3*** et le ***tableau 5*** de la norme exigent une proportion de défaillances en sécurité SFF, supérieure ou égale à 99 %. Atteindre ce taux avec l'usage d'un seul élément de sous-système est quasiment impossible. L'utilisation de l'architecture « C » avec ajout d'une fonction de diagnostic pour augmenter la proportion de défaillance en sécurité, si elle reste théoriquement possible, est trop contraignante pour pouvoir être mise en œuvre. En effet, les exigences du ***§ 6.8.6*** de la norme imposent entre autres que la réaction à l'anomalie spécifiée pour le diagnostic soit exécutée avant que le phénomène dangereux ne puisse se produire, préconisation difficile à mettre en œuvre dans le cas présent.

La norme NF EN 62061 est très exigeante pour les sous-systèmes de SIL3 requis et de tolérance aux anomalies de « 0 », ceci afin de s'assurer que les contraintes architecturales mises en œuvre soient appropriées (note du ***§ 6.7.6.3***).

Dans notre cas, on s'oriente vers la conception d'un sous-système « particulier » constitué de deux éléments de sous-systèmes.

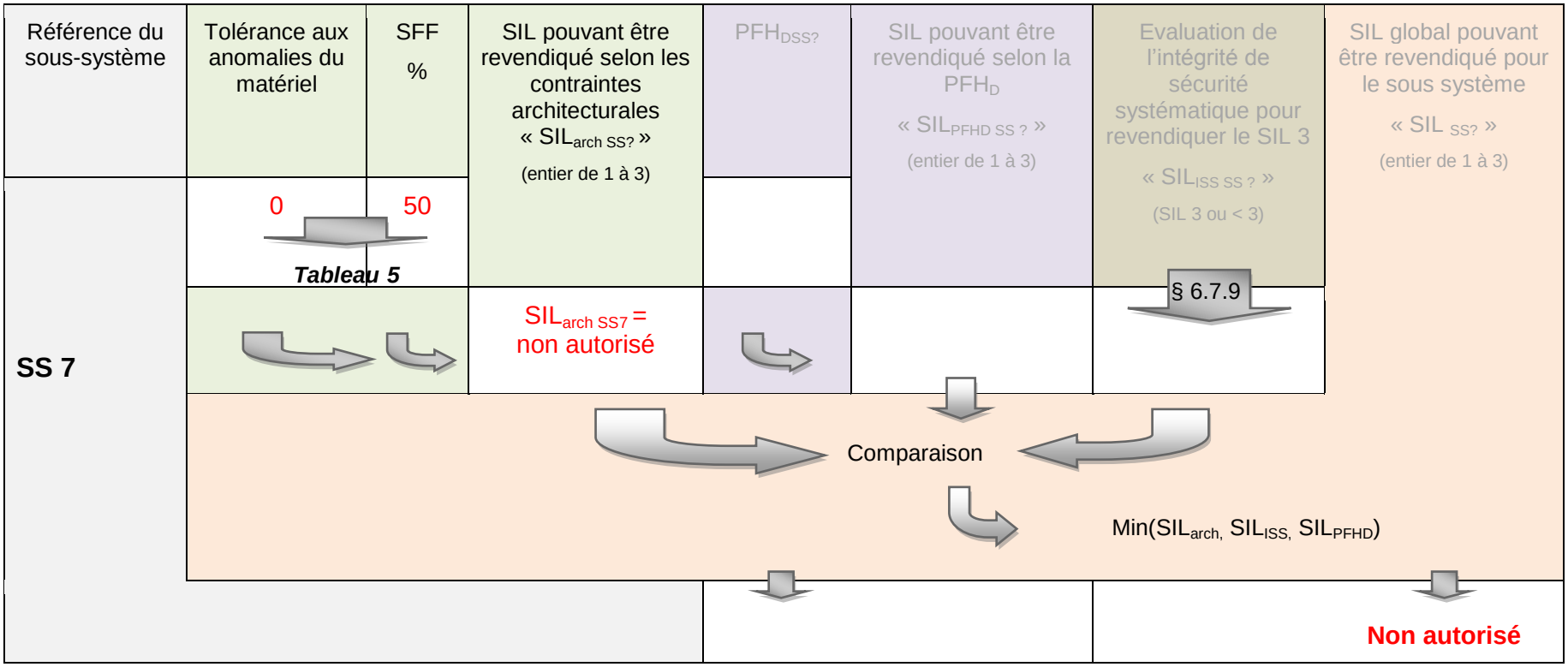


Tableau 22 : Récapitulatif du SIL pouvant être revendiqué pour le sous-système SS7, renseigné selon les contraintes architecturales

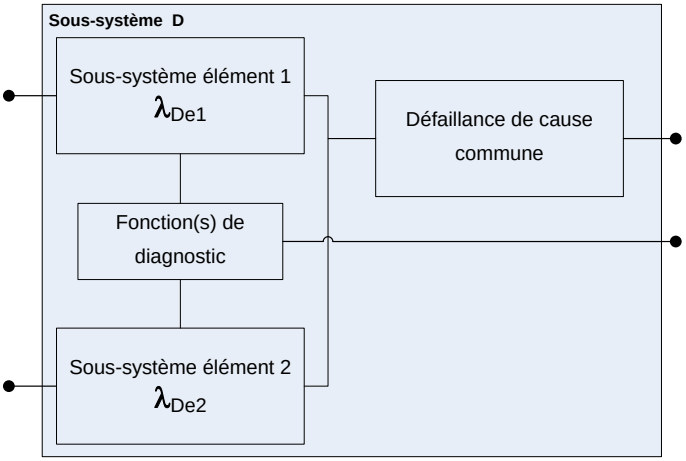
D5. Deuxième phase : conception d'un sous-système « particulier »

Cette phase a été traitée en deux itérations :

- 1ère itération : Mise en œuvre d'une architecture de type »B ». Le résultat obtenu n'atteignait pas le SIL requis. Pour ne pas alourdir l'exemple, cette itération n'est pas présentée dans ce document.
- 2ème itération : mise en œuvre d'une architecture de type « D », Comme décrit ci-après.

D5.1 Choix de l'architecture d'un sous-système

Le choix se porte sur une architecture de type « D ».



Production d'une architecture du sous-système

La Figure 22 représente le processus complet correspondant, qui est détaillé dans la suite de cette annexe.

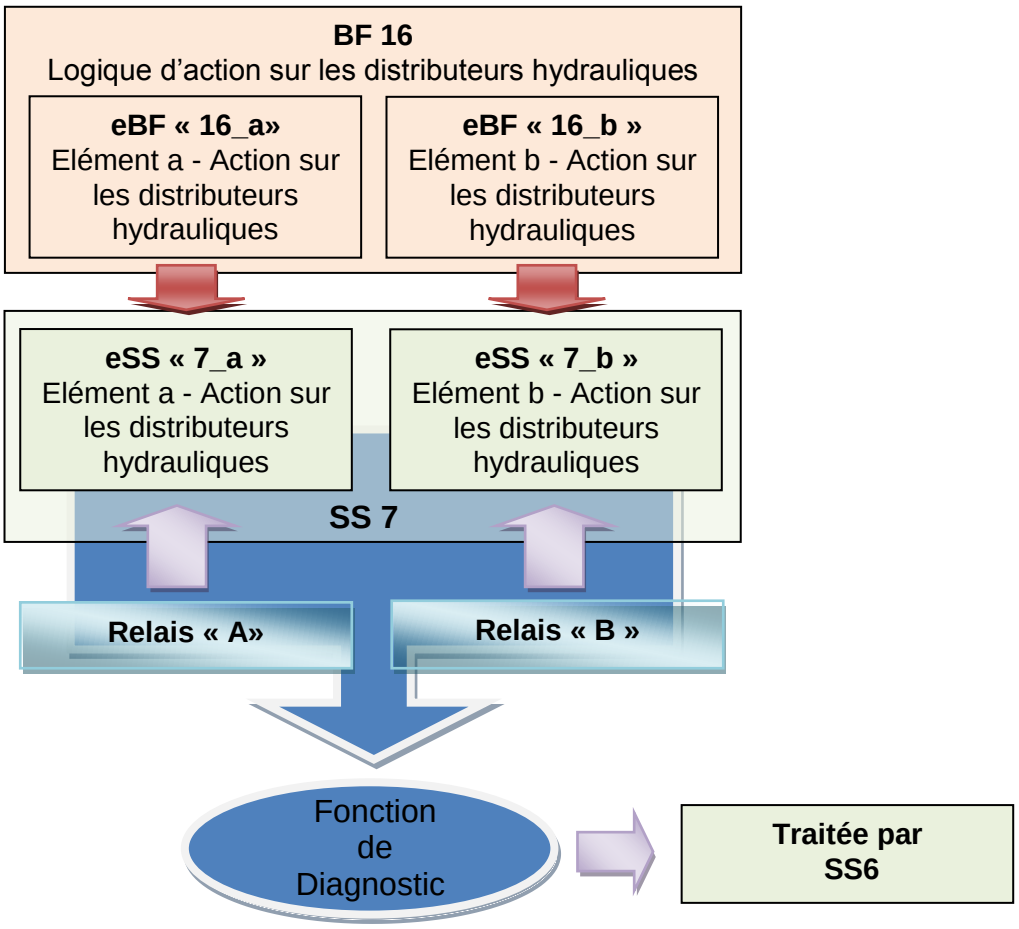


Figure 22 : Architecture de type « D » du sous-système SS7

Spécification des éléments de blocs fonctionnels

Les spécifications des éléments de blocs fonctionnels sont identiques à celles de la première itération.

Choix et mise en œuvre des éléments de Sous-Systèmes (eSS)

Le sous-système de base est identique à celui de la première itération, mais auquel une fonction de diagnostic est ajoutée.

Contribution de la fonction de diagnostic au sous-système

La spécification des SRCF concernées précise que « la réaction en cas de défaut doit conduire à couper l'alimentation électrique des distributeurs hydrauliques de commande du mouvement de descente du tablier et maintenir cette coupure tant que l'ensemble des défauts n'est pas éliminé ».

La fonction de diagnostic est prévue pour détecter les défaillances potentiellement dangereuses identifiées des éléments de sous-système puis enclencher la réaction à ces anomalies.

Pour le sous-système SS7, les défaillances dangereuses identifiées se traduisent par un blocage des relais à l'état 1. Pour détecter ces anomalies, des contacts « O » des deux relais seront utilisés et leur état comparé par rapport à l'état de la bobine des relais. Cette fonction est confiée au sous-système SS6.

Cette fonction de diagnostic est considérée, au sens de la norme, comme une fonction séparée. Le § 8.5.2 de ce document fournit des précisions sur les préconisations correspondantes. La fonction de diagnostic du SS7 n'est pas décrite dans ce document, mais uniquement illustrée sur la Figure 23.

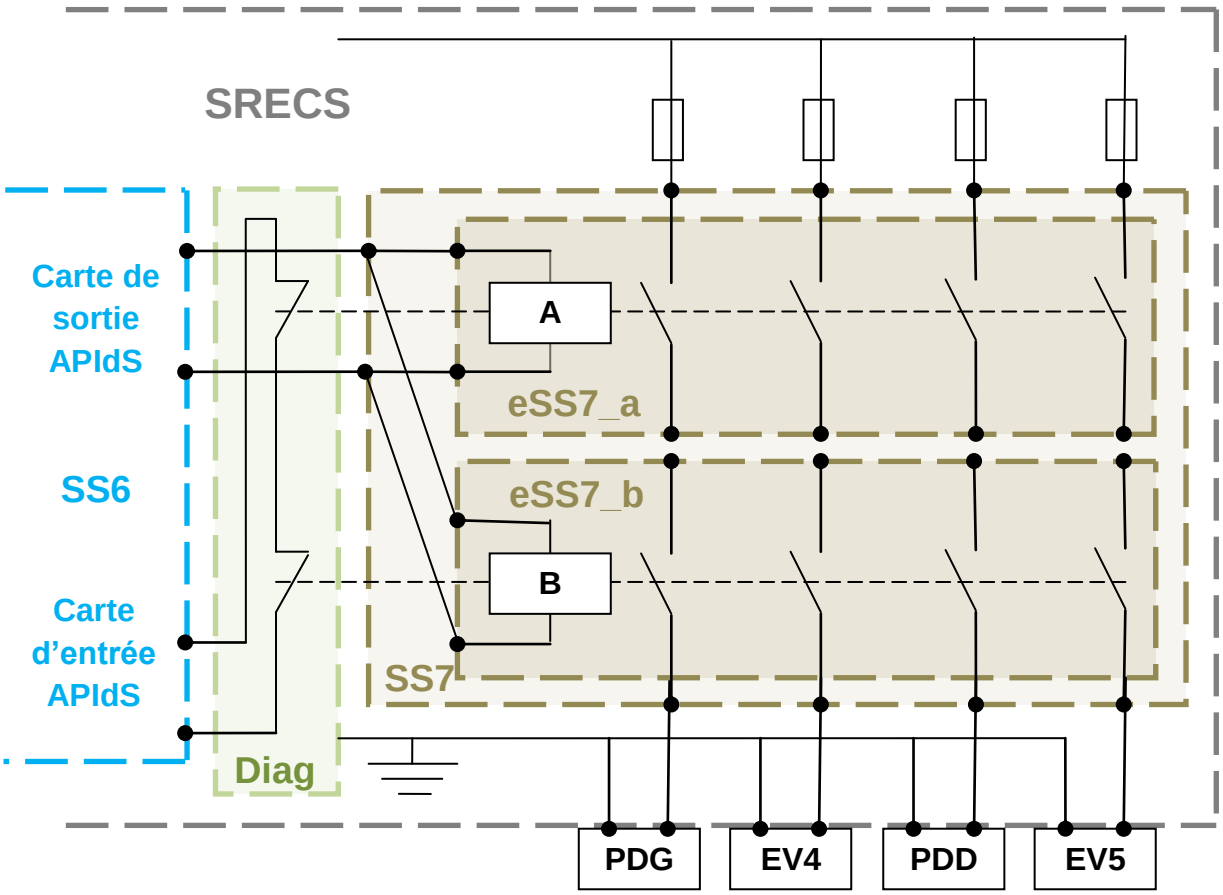


Figure 23 : Raccordement du sous-système SS7 et de la fonction de diagnostic

D5.2 Détermination du SIL pouvant être revendiqué par le sous-système SS7

D5.2.1 Détermination du SIL vis-à-vis des contraintes architecturales du sous-système SS7

Estimation de la tolérance aux anomalies du matériel

Comme pour la première itération, le sous-système SS7 est composé de deux éléments de sous-système qui sont deux relais électromécaniques. Potentiellement, la défaillance des deux relais est nécessaire pour que la SRCF, à laquelle ils participent, se comporte de manière dangereuse.

Deux défaillances sont susceptibles de provoquer la perte de la SRCF, donc la tolérance aux anomalies du matériel est de « 1 ».

Estimation de la proportion de défaillance en sécurité

La fonction de diagnostic permet de détecter la totalité des défaillances dangereuses sur un relais à contacts liés, le pourcentage de défaillance dangereuse $\%d_D$ étant de 50 %, le pourcentage de défaillance dangereuse détectée $\%d_{DD}$ du relais est donc de 50 %. En se basant sur la formule décrite dans la 2ème itération, la SFF devient :

$$\textbf{SFF} \text{ (exprimé en \%)} = [\sum\%d_S + \sum\%d_{DD}] / [\sum\%d_S + \sum\%d_D]$$

$$\textbf{SFF} = \textbf{(50 + 50 + 50 + 50) / (50 + 50 + 50 + 50) = 100 \%}$$

D'après le ***tableau 5*** de la norme, pour une proportion de défaillance en sécurité de SFF = 100 % et pour une tolérance aux anomalies de « 1 », le SIL maximal pouvant être revendiqué est SIL 3.

Le sous-système SS7 peut donc, du point de vue des contraintes architecturales, être utilisé en l'état pour une SRCF de SIL 3 requis.

D5.2.2 Détermination du SIL vis-à-vis de la PFHD du sous-système SS7

La formule préconisée pour calculer la probabilité de défaillance dangereuse aléatoire d'un sous-système lorsque deux éléments de sous-systèmes identiques sont utilisés, dans le cas d'une architecture de type « D » est la suivante :

$$PFH_{Dss7} = \lambda_{Dss7\ x}\ 1h$$

$$\lambda_{Dss7} = (1-\beta)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1-DC)] \times T_1\} + \beta \times \lambda_{De}$$

Liste des données nécessaires et détermination des différents paramètres

Paramètre calculé à partir des données du fabricant de relais

B10 : Donnée de fiabilité fournie par le fabricant du relais
Pour chacun des relais utilisés :

$$B10d = B10/\%d_{De} = 1.10^6/0.5 = 2.10^6$$

Donnée des spécifications des exigences fonctionnelles de la ou des SRCF concernée(s)

C : Nombre d'opérations par heure du sous-système. Il dépend de la fréquence de sollicitation de la ou des SRCF traitées par le sous-système. Pour « SS7 » :

C = 60 opérations/heures

Paramètres calculés ou déterminés par le concepteur du sous-système

λ_{De} : Taux de défaillance de l'élément de sous-système. Pour les composants électromécaniques, il est calculé avec la formule $\lambda_{De} = 0{,}1 \times C/B10d$. Pour chacun des relais utilisés :

$$\lambda_{De} = 0{,}1 \times C/B10d = 3.10^{-6}$$

DC : Couverture de diagnostic. Elle peut être calculée en utilisant l'équation suivante : $DC = \Sigma\ \lambda_{DD} / \lambda_{Dtotal}$ où λ_{DD} est le taux de défaillance dangereuse détectée pour le matériel et λ_{Dtotal} est le taux de toutes les défaillances dangereuses pour le matériel. Comme le diagnostic mis en œuvre détecte toutes les défaillances de chaque relais :

DC=1

T_2 : Intervalle de diagnostic. Dans le cas du sous-système « SS7 », le diagnostic est effectué à chaque commutation d'un relais, donc du sous-système. Pour « SS7 » :

$$T_2 = 1/60 = 1{,}7\ 10^{-2}$$

T_1 : Intervalle de test périodique ou la durée de vie selon la valeur la plus faible :

Durée de vie du contacteur : 175 200 h (20 ans à 8 760 h/an).

Intervalle de test périodique : 17 520 h (un test tous les 2 ans est jugé utile par le concepteur du sous-système)

T_1 = 17 520 h

β **:** Sensibilité aux défaillances de cause commune. Elle est déterminée par le concepteur du sous-système, par exemple en suivant la méthodologie de ***l'annexe F (informative)*** de la norme. Le détail est repris § D5.5 de ce document, le score obtenu détermine une valeur de :

β= 0,02

Calcul de la probabilité de défaillance dangereuse aléatoire de « SS7 »

$$\lambda_{Dss7} = (1- \beta)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1-DC)] \times T_1\} + \beta \times \lambda_{De}$$

$$\lambda_{Dss7} = 6. 10^{-8}$$

$$PFH_{Dss7} = \lambda_{Dss7} \times 1h = 6. 10^{-8}$$

D'après le ***tableau 3 - § 5.2.4.2*** de la norme, pour une PFH_D du sous-système, comprise entre 10^{-7} et 10^{-8}, le SIL maximal pouvant être revendiqué est SIL 3.

Le sous système SS7 peut donc, du point de vue de la PFH_D, être utilisé en l'état pour une SRCF de SIL 3 requis.

D5.2.3 Evaluation de l'intégrité de sécurité systématique du sous-système SS7 pour revendiquer le SIL 3

Les mesures mises en œuvre dans cet exemple pour répondre aux préconisations des ***§ 6.7.9.1 et 6.7.9.2*** de la norme ne sont pas décrites.

Le respect de la totalité des exigences des ***§ 6.7.9.1 et 6.7.9.2*** entraîne la possibilité pour le sous-système de revendiquer, vis-à-vis de la prise en compte des défaillances systématiques, un SIL 3.

D5.3 Conclusions sur le SIL de SS7

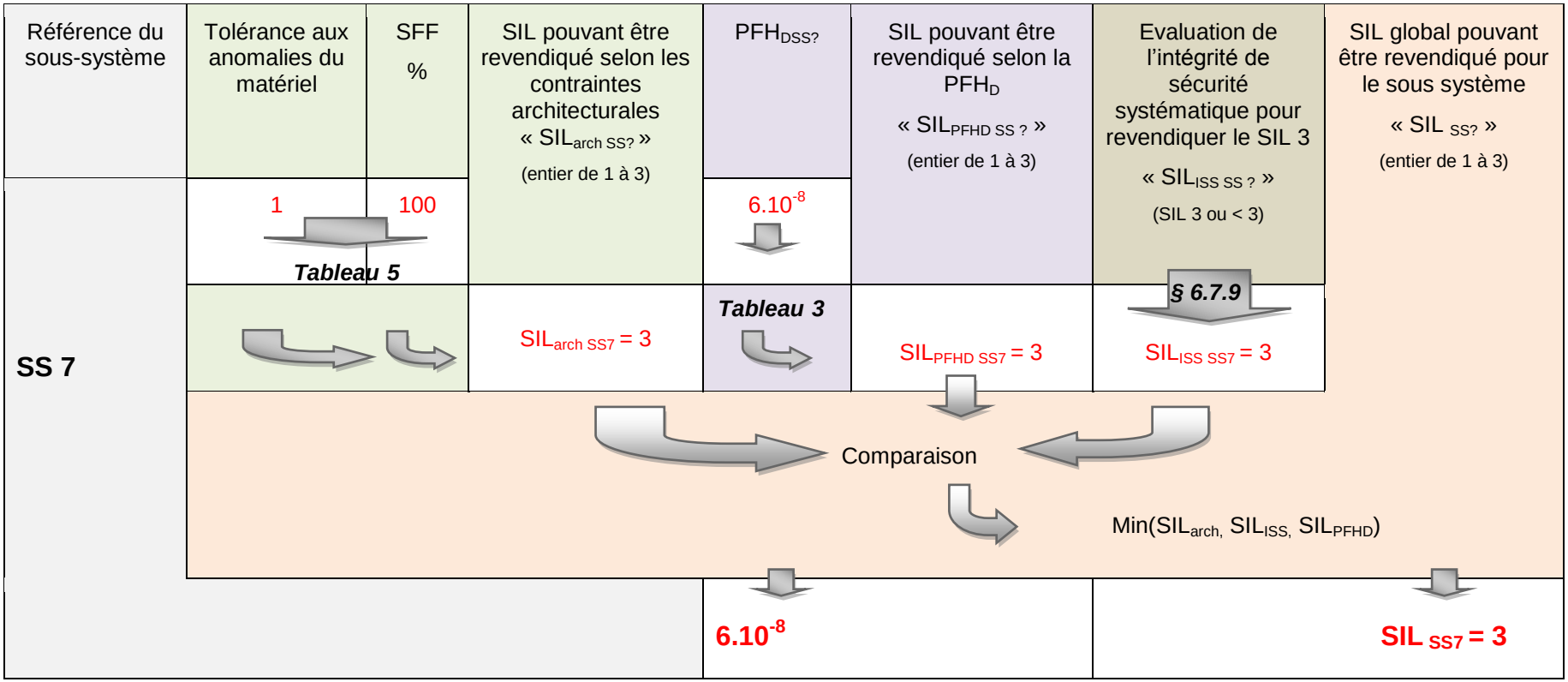


Tableau 23 : Récapitulatif du SIL pouvant être revendiqué pour un sous-système SS 7

Compte tenu que le sous-système SS7 peut revendiquer un SIL 3 selon ses contraintes architecturales, sa PFHD et son intégrité de sécurité systématique, ce sous-système SS7 est de SIL 3.

D5.4 Tableau récapitulatif des caractéristiques du sous-système SS7

Sous-système : SS7	
Type d'information	Caractéristiques du sous-système
SIL	SIL 3
Fonction(s)	Lorsque l'entrée est alimentée en tension, les distributeurs hydrauliques PDG, EV4, PDD et EV5 sont alimentés électriquement (descente du tablier commandée). Lorsque l'entrée n'est pas alimentée en tension, les distributeurs hydrauliques PDG, EV4, PDD et EV5 ne sont plus alimentés électriquement (descente du tablier non commandée).
Entrée(s)	Une bobine destinée à être commandée en tension, raccordée à une seule sortie bipolaire de l'APIdS gérant la sortie de BF 16. Caractéristiques compatibles avec celles de la sortie correspondante du sous-système SS6 (caractéristiques de courant, tension, …)
Sortie(s)	Quatre contacts électromécaniques de type « F », un pour chacun des distributeurs hydrauliques commandant la descente du tablier PDG, EV4, PDD et EV5. Une des bornes de chacune de ces sorties doit être reliée directement à une borne du distributeur correspondant. Caractéristiques compatibles avec celles des distributeurs (pouvoir de coupure).
Temps de réponse	7 ms
Conditions environnementales (ex. température, humidité, vibrations,…)	IP 20. Les câbles de raccordement entre le relais et les bobines des distributeurs sont prévus pour résister à un environnement industriel.
Fréquence de fonctionnement du sous-système	Compatible avec la fréquence de 1/mn requise.
PFH_D	6.10^{-8}

Sous-système : SS7	
Type d'information	Caractéristiques du sous-système
Environnement et conditions de fonctionnement qu'il convient d'observer (***§ 6.7.2.2- c***) (afin de maintenir la validité des taux de défaillance estimés dus aux défaillances aléatoires de matériel)	Les câbles d'alimentation de chaque distributeur hydraulique qui cheminent hors de l'armoire électrique doivent être réservés à cette fonction et être séparés des autres câbles du SRECS. Les câbles d'alimentation en énergie électrique doivent être séparés des câbles de signaux ainsi que leurs borniers. Effectuer une mise à la terre d'une borne de l'alimentation des distributeurs et respecter les mesures préconisées par la norme NF EN 60204-1 pour la protection de l'équipement électrique.
Durée de vie du sous-système qu'il convient de ne pas dépasser (***§ 6.7.2.2- c***) (afin de maintenir la validité des taux de défaillance estimés dus à des défaillances aléatoires du matériel)	175 200 h (20 ans à 8 760 h/an).
Tests et/ou exigences de maintenance à respecter (***§ 6.7.2.2- d***)	17 520 h (un test tous les 2 ans est jugé utile par le concepteur du sous-système)
Diagnostic(s) qu'il est prévu de confier à un autre sous-système (***§ 6.7.2.2- e***)	La fonction de diagnostic prévue pour le sous système SS7 doit être réalisée conformément à ses spécifications par le sous-système SS6.
Limitations afin d'éviter les défaillances systématiques (***§ 6.7.2.2- h***)	Respecter les mesures préconisées par la norme NF EN 60204-1 pour la protection de l'équipement électrique (protection contre les surintensités,…). Le sous-système doit être installé à l'intérieur d'une armoire électrique. Les câbles d'alimentation de chaque distributeur hydraulique, qui cheminent hors de l'armoire électrique, doivent être protégés des risques de dégradation mécanique.
Les informations nécessaires à l'identification de la configuration du matériel et du logiciel (***§ 6.7.2.2- j***)	Sans objet
Probabilité d'erreur de transmission dangereuse dans le cas de processus de communication de données numériques (***§ 6.7.2.2- k***)	Sans objet

Tableau 24 : Récapitulatif des caractéristiques du sous-système SS7

D5.5 Exemple d'estimation de la sensibilité aux défaillances de cause commune (CCF) du sous-système SS7

La sensibilité aux CCF est évaluée par le concepteur du sous-système en suivant la méthodologie de ***l'annexe F (informative)*** de la norme.

Sous-système SS7			
Mesures mises en œuvre	**Réf**	**Score retenu**	**Commentaires**
Séparation/ségrégation			
Tous les câbles de signaux d'un SRECS pour les canaux particuliers cheminent-ils séparément des autres canaux vers tous les points de raccordement ou sont-ils suffisamment blindés ? **Score : 5**	1a	5	Les câbles d'alimentation de chaque distributeur hydraulique qui cheminent hors de l'armoire électrique sont réservés à cette fonction et sont donc séparés des autres câbles du SRECS
Lorsqu'on utilise l'encodage/décodage des informations, est-ce suffisant pour la détection des erreurs de transmission d'un signal ? **Score : 10**	1b	0	Pas d'encodage/décodage pour la transmission des informations du SS6 vers SS7 et de SS7 aux bornes de raccordement du SRECS
***NOTE** : Une alternative (par exemple les références 1a et 1b) est donnée dans le ce Tableau s'il est prévu qu'une revendication peut être établie afin de contribuer à l'évitement des CCF provenant uniquement de l'élément le plus approprié*		Les scores 1a et 1b ne peuvent pas être cumulés	
Les câbles d'alimentation en énergie électrique et les câbles de signaux d'un SRECS sont-ils séparés sur tous les points de raccordement ou sont-ils suffisamment blindés ? **Score : 5**	2	5	Les câbles d'alimentation en énergie électrique sont séparés des câbles de signaux ainsi que leurs borniers
Si les éléments d'un sous-système peuvent contribuer à une CCF, sont-ils fournis comme des dispositifs séparés dans leurs propres enveloppes? **Score : 5**	3	5	Les relais possèdent chacun leur propre boîtier et leur propre bornier et sont dans la même armoire électrique, mais sans risque de CCF
Diversité/redondance			
Le sous-système emploie-t-il des technologies électriques différentes, par exemple une technologie électronique ou électronique programmable et une autre avec un relais électromécanique ? **Score : 8**	4	0	NON

Sous-système SS7			
Mesures mises en œuvre	**Réf**	**Score retenu**	**Commentaires**
Le sous-système emploie-t-il des éléments utilisant des principes physiques différents (par exemple, des capteurs sur une porte de protection utilisant des techniques de détection mécaniques et magnétiques) ? **Score : 10**	5	0	NON
Le sous-système emploie-t-il des éléments avec des différences temporelles dans les modes de fonctionnement fonctionnels et/ou les modes de défaillance? **Score : 10**	6	0	NON
Les éléments du sous-système ont-ils un intervalle de test de diagnostic ≤ 1 mn ? **Score : 10**	7	10	OUI
Complexité/conception/utilisation			
L'interconnexion entre des canaux du sous-système est-elle empêchée excepté pour ceux utilisés pour les besoins des tests de diagnostic ? **Score : 2**	8	2	OUI. Les deux canaux du sous-système destinés à alimenter les distributeurs PDG et EV4 ou PDD et EV5 sont séparés physiquement. Un court-circuit entre les canaux n'affecte pas la sécurité du sous-système
Appréciation/analyse			
Les résultats des analyses des modes de défaillance et de leurs effets ont-ils été examinés afin d'établir des sources de défaillance de cause commune et éliminer dès la conception les sources prédéterminées de défaillance de cause commune ? **Score : 9**	9	9	OUI. Des mesures pour éviter les fautes systématiques (mise à la terre d'une borne de l'alimentation, et respect des mesures préconisées par la norme NF EN 60204-1 pour la protection de l'équipement électrique) ont été mises en œuvre
Les défaillances relevées sur le terrain ont-elles été analysées de manière exhaustive avec retour d'expérience vers la conception ? **Score : 9**	10	9	OUI. L'usage d'interfaces à deux relais avec fonction de diagnostic représente l'état de l'art
Compétence/formation			

Sous-système SS7			
Mesures mises en œuvre	**Réf**	**Score retenu**	**Commentaires**
Les concepteurs de sous-systèmes comprennent-ils les causes et les conséquences des défaillances de cause commune ? **Score : 4**	11	4	OUI. Les concepteurs ont reçu une formation adéquate
Maîtrise de l'environnement			
Les éléments de sous-système sont-ils en mesure de fonctionner toujours dans la plage de température, d'humidité, de corrosion, de poussière, de vibrations, etc. pour laquelle ils ont été testés, sans utiliser la maîtrise extérieure de l'environnement ? **Score : 9**	12	9	OUI. Matériel industriel adapté, sélectionné en fonction de l'usage attendu et placé dans une armoire électrique
Le sous-système possède-t-il une immunité contre les influences néfastes des interférences électromagnétiques jusqu'à et y compris les limites spécifiées en ***Annexe E*** ? **Score : 9**	13	9	OUI. Usage exclusif de composants électromécaniques
SCORE FINAL		**67**	β **= 0.02**

Tableau 25 : Estimation de la sensibilité aux CCF du sous-système SS7

Annexe E - Evaluation du SIL final de la SCRF C

Le Tableau 26 récapitule, pour la SRCF C constituée de trois sous-systèmes sans processus de communication, les différents paramètres nécessaires ainsi que les opérations à effectuer pour l'évaluation du SIL.

Identification de la SRCF	Identification des sous systèmes (SS « n »)	SIL global pouvant être revendiqué pour les sous systèmes SIL_{SS} «n» (entier de 1 à 3)	PFH_{DSS} «n»	
SRCF C	**SS 4**	SIL_{SS4} = **3**	**$1{,}5.10^{-8}$**	
	SS 6	SIL_{SS6} = **3**	**$5{,}1.10^{-9}$**	
	SS 7	SIL_{SS7} = **3**	**6.10^{-8}**	
			$\sum(PFH_{DSS4}, PFH_{DSS6}, PFH_{DSS7})$ = **$8{,}01\ 10^{-8}$**	
			Tableau 3 $SIL_{\sum PFHD\ SRCF\ C}$ = **3**	
		$Min(SIL_{SS4}, SIL_{SS6}, SIL_{SS7}, SIL_{\sum PFHD\ SRCF\ C})$		SIL final de la SRCF « $SIL_{SRCF\ C}$ » (entier de 1 à 3) **SIL_{SRCFC} = 3**

Tableau 26 : Exemple d'estimation du SIL de la SRCF C constituée de trois sous-systèmes

Annexe F - Extrait des plans de tests de validation du SRECS de la presse plieuse hydraulique

Cette annexe est destinée à illustrer les tests qui ont été effectués sur la presse plieuse prise en exemple et ne constitue qu'un extrait de ces tests.

Ces derniers permettent de répondre partiellement aux exigences du ***§ 6.12.1*** de la norme pour les tests d'intégration qui n'ont pas pu être effectués avant installation et aux exigences du ***§ 8.2.3*** pour les tests de validation des SRCF.

Ils succèdent aux autres vérifications effectuées sur la machine telle que la vérification du câblage et d'autres tests préliminaires ayant pu être effectués sans mouvement des éléments mobiles, en séparant le circuit de commande et/ou le SRECS de la partie puissance.

Conditions particulières des tests

Il s'agit de décrire les conditions nécessaires pour que :

- le test se déroule correctement du point de vue de l'enchaînement des séquences,
- la machine soit prédisposée pour que les risques vis-à-vis du personnel devant effectuer les tests soient réduits au maximum, au cas où une fonction de sécurité ne se comporterait pas comme attendu. Quelques exemples de ce style de mesures sont décrits ci-après :
    - la position des butées doit être éloignée des outils et située au centre de la presse (programmation d'une pièce de grande profondeur et de faible largeur),
    - pas de mouvement des butées (hormis la phase d'initialisation),
    - lorsque des obstructions des faisceaux optiques des dispositifs de protection seront nécessaires, elles ne seront jamais effectuées avec une partie du corps de l'opérateur, mais toujours avec un obstacle calibré en procédant comme décrit ci-après :
        - soit en positionnant un obstacle calibré sur la matrice d'essais (occultation pendant la phase d'approche),
        - soit en glissant un obstacle calibré en cours de cycle (occultation en phase de travail) en utilisant le support de tôle et une tôle positionnée sur une matrice supplémentaire.

Dénomination de la fiche de tests	**Mode Production (Descente tablier)** **Tests Fonctions « standard »**		**PTV …..** **Rév. ……**
Document de référence	Notice d'instructions doc. n° … version …..	Pages	……..
Description du test	Ce test consiste à vérifier le déroulement des cycles (sans sollicitation des protecteurs et dispositifs de protection) du mode Production		
Conditions initiales	Le mode réglage est validé (SE1 en position 1), le tablier est au PMH, les protecteurs latéraux et arrière sont fermés, les BP d'arrêt d'urgence sont déverrouillés, le champ de protection de la barrière immatérielle est libre, les organes de commande sont au repos, la Commande Numérique (CN) est opérationnelle. **Programme pièce n° …..**		

Dénomination de la fiche de tests	**Mode Production (Descente tablier)** **Tests Fonctions « standard »**	**PTV …..** **Rév. ……**
Remarques préalables		
Ce test ne concerne que le mouvement de descente du tablier		

Dénomination de la fiche de tests	**Mode Production (Descente tablier)** **Tests Fonctions « standard »**			**PTV …..** **Rév. ……**
Action	**Situation attendue**	**C**	**NC**	**Observations**
Test validation du mode de fonctionnement				
Positionner le commutateur SE1 sur la position 2	Pas de mouvement du tablier			
Impulsion sur BPR (durée x)	Pas de mouvement du tablier			
Impulsion sur le BP « START » de la CN	Voyant CN « I » allumé			
Test non-répétition (cycle complet)				
Action maintenue sur la pédale PED	Le tablier descend en grande vitesse			
	A partir du PCVT le tablier descend en petite vitesse			
	Au point mort bas, le tablier s'arrête			
	Après un temps passé en pression, le tablier monte			
	Au point mort haut, le tablier s'arrête			
Relâchement de la pédale de descente	Pas de mouvement du tablier			
Test relâchement pédale en phase d'approche				
Action maintenue sur la pédale de descente jusqu'à mi-course (au-dessus du PCVT)	Le tablier descend en grande vitesse			
Relâchement de la pédale de descente	Le tablier s'arrête puis remonte immédiatement et s'arrête au Point Mort Haut			
Test relâchement pédale en phase de travail				
Action maintenue sur la pédale de descente jusqu'à une position située en-dessous du PCVT	Le tablier descend en grande vitesse			
	A partir du PCVT le tablier descend en petite vitesse			

Dénomination de la fiche de tests	**Mode Production (Descente tablier) Tests Fonctions « standard »**			**PTV ….. Rév. ……**
Action	**Situation attendue**	**C**	**NC**	**Observations**
Relâchement de la pédale de descente	Le tablier s'arrête immédiatement			
Impulsion sur la pédale de montée	Le tablier monte et s'arrête au Point Mort Haut			
Test remontée automatique				
Action maintenue sur la pédale de descente pendant toute la phase de descente et jusqu'à mi-course de la phase de remontée	Le tablier descend en grande vitesse			
	A partir du PCVT le tablier descend en petite vitesse			
	Au point mort bas, le tablier s'arrête			
	Après un temps passé en pression, le tablier monte			
Relâchement de la pédale de descente	Le tablier continue la phase de remontée			
	Au point mort haut, le tablier s'arrête			
Test troisième position pédale en phase d'approche				
Action maintenue sur la pédale de descente et forçage maintenu de la troisième position de la pédale à mi-course (au-dessus du PCVT)	Le tablier descend en grande vitesse, s'arrête au forçage de la troisième position de la pédale puis remonte immédiatement et s'arrête au Point Mort Haut			
Relâchement complet de la pédale de descente	Pas de mouvement du tablier			
Test troisième position pédale en phase de travail				
Action maintenue sur la pédale de descente et forçage maintenu de la troisième position de la pédale en-dessous du PCVT	Le tablier descend en grande vitesse			
	A partir du PCVT le tablier descend en petite vitesse puis s'arrête au forçage de la troisième position de la pédale			
Relâchement complet de la pédale de descente	Pas de mouvement du tablier			
Impulsion sur la pédale de montée	Le tablier monte et s'arrête au Point Mort Haut			
Commentaires				

Dénomination de la fiche de tests	**Mode Production (Descente tablier) Tests Fonctions « standard »**			**PTV ….. Rév. ……**
Action	**Situation attendue**	**C**	**NC**	**Observations**

Dénomination de la fiche de tests	**Mode Production (Descente tablier) Tests SRCF « C »**		**PTV ….. Rév. ……**
Document de référence	Notice d'instructions doc. n° …., version …….	Pages	……..
Description du test	Ce test consiste à vérifier le déroulement des cycles (avec sollicitation des protecteurs et dispositifs de protection)		
Conditions initiales	Le mode Production est validé (SE1 position 2), le tablier est au PMH, les protecteurs latéraux et arrière sont fermés, les BP d'arrêt d'urgence sont déverrouillés, le champ de protection de la barrière immatérielle est libre, les organes de commande sont au repos, la CN est opérationnelle. **Programme pièce n° …**		
Remarques préalables			
Ce test ne concerne que le mouvement de descente du tablier.			

Dénomination de la fiche de tests	**Mode Production (Descente tablier) – Tests SRCF « C »**			**PTV ….. Rév. ……**
Action	**Situation attendue**	**C**	**NC**	**Observations**
Test barrière immatérielle en phase d'approche				
Action maintenue sur la pédale de descente et occultation maintenue de la barrière immatérielle à mi-course (au dessus du PCVT)	Le tablier descend en grande vitesse, s'arrête au franchissement de la barrière puis remonte immédiatement et s'arrête au Point Mort Haut			
Désoccultation de la barrière immatérielle	Pas de mouvement du tablier			
Relâchement de la pédale de descente	Pas de mouvement du tablier			
Test barrière immatérielle en phase de travail				
Action maintenue sur la pédale de descente et occultation maintenue de la barrière immatérielle en dessous du PCVT	Le tablier descend en grande vitesse			
	A partir du PCVT le tablier descend en petite vitesse puis s'arrête au franchissement de la barrière			

Dénomination de la fiche de tests	**Mode Production (Descente tablier) – Tests SRCF « C »**			**PTV ….. Rév. ……**
Action	**Situation attendue**	**C**	**NC**	**Observations**
Relâchement de la pédale de descente	Pas de mouvement du tablier			
Action maintenue sur la pédale de descente	Pas de mouvement du tablier			
Relâchement de la pédale de descente	Pas de mouvement du tablier			
Impulsion sur la pédale de montée	Le tablier monte et s'arrête au Point Mort Haut			
Test barrière immatérielle en phase de remontée automatique				
Action maintenue sur la pédale de descente et occultation maintenue de la barrière immatérielle à mi-course de la phase de remontée	Le tablier descend en grande vitesse			
	A partir du PCVT le tablier descend en petite vitesse			
	Au point mort bas, le tablier s'arrête			
	Après un temps passé en pression, le tablier monte			
	Au point mort haut, le tablier s'arrête			
Désoccultation de la barrière immatérielle	Pas de mouvement du tablier			
Relâchement de la pédale de descente	Pas de mouvement du tablier			
Test barrière immatérielle au départ du cycle				
Occultation de la barrière immatérielle	Pas de mouvement du tablier			
Action maintenue sur la pédale de descente	Pas de mouvement du tablier			
Commentaires				