POINT DE REPÈRE

CIRCUITS DE COMMANDE DES MACHINES

Un référentiel normatif pour leur conception

► *Jean-Pierre BUCHWEILLER, INRS, département Ingénierie des équipements de travail*

Le sujet des normes traitant la sécurité des systèmes de commande est régulièrement à l'ordre du jour dans les relations entre préventeurs et concepteurs ou utilisateurs de machines.
Les informations ne manquent pas concernant la publication de nouveaux référentiels normatifs, l'évolution de certains autres textes plus anciens... Mais lorsque le concepteur a enfin en main le référentiel adapté à sa problématique de conception, les difficultés réelles commencent car la lecture de ces référentiels, traitant d'un sujet complexe, n'est pas chose aisée.
Dans cet article, nous nous proposons de parcourir un des textes destinés à la conception des circuits de commande traitant des fonctions de sécurité : la norme NF EN62061 [1] [1] publiée en juillet 2005.
L'objectif est d'abord de présenter la philosophie de cette norme puis sa structure générale et, enfin, de détailler l'approche pratique proposée.
Il ne s'agit pas de paraphraser inutilement un texte, dont la lecture rigoureuse sera toujours indispensable avant d'entreprendre le développement d'un circuit de commande, mais de proposer un certain nombre de clés pour en faciliter la lecture et l'exploitation.

[1] *« Avant-propos national – Ce document constitue la version française complète de la norme européenne EN 62061:2005 en reprenant le texte de la publication CEI 62061:2005, y compris le corrigendum de juillet 2005 ».*

La norme NF EN 62061 a été rédigée dans le cadre des textes de normes mis en chantier pour venir en appui à la directive Machines 98/37/CE [2]. Sans entrer dans le détail de cette directive, il faut néanmoins rappeler qu'elle définit précisément son champ d'application – les machines et les composants de sécurité –, et qu'elle fixe, pour leur conception, un certain nombre d'objectifs sous la forme d'« exigences essentielles de sécurité »[2].

De la pratique de cette directive émergent deux idées fortes pour la conception des machines et des composants de sécurité :

- l'analyse du risque préalable à la conception,
- l'intégration de la sécurité à la conception.

Mais il faut reconnaître que la directive Machines est avant tout un texte réglementaire et qu'elle n'aborde pas le détail des solutions techniques permettant de satisfaire les prescriptions générales énoncées.

Pour répondre aux besoins méthodologiques et techniques liés au développement des circuits de commande traitant des fonctions de sécurité, des référentiels normatifs ont donc été rédigés, certains harmonisés [3] dans le cadre de la directive Machines - NF EN 62061 : 2005 [4] est de celles-là - et d'autres non.

On peut citer plusieurs autres référentiels comme EN 954-1 : 1996 [3], EN ISO 13849-1 [4], NF EN 61508 [5] traitant également du sujet abordé ici.

Les concepteurs peuvent parfois être amenés à s'interroger sur l'intérêt de chacune de ces normes et de celle qui nous occupe en particulier face à une même problématique. Tout au long de cet article, nous proposons donc de présenter NF EN 62061 en soulignant les spécificités pour en faire ressortir l'intérêt pour le concepteur.

DE LA MACHINE AU SRECS

La norme NF EN 62061 traite de sécurité des machines et en particulier des Systèmes de commande relatifs à la sécurité à technologies électriques, électroniques et électroniques programmables ou SRECS (Safety related electrical control system).

Pour préciser cette notion, nous proposons la représentation schématique de la *Figure 1*, construite à partir des définitions de la norme, montrant la place du SRECS dans la machine, ainsi que les deux types d'entités matérielles pouvant le composer.

Compte tenu de cette structure et des différentes entités matérielles concernées, l'objectif fixé pour la norme NF EN 62061 consiste à proposer une démarche pour choisir ou concevoir :

- le SRECS qui devra assumer les fonctions relatives à la sécurité d'une machine,
- les sous-systèmes qui se répartiront la fonction globale assignée au SRECS,
- les éléments de sous-systèmes qui se répartiront la sous-fonction assignée au sous-système.

Par ailleurs, la stratégie de conception retenue par la norme privilégie une approche d'intégration de dispositifs existants, conçus sur la base d'autres textes de normes.

UNE DÉMARCHE DE CONCEPTION SPÉCIFIQUE

La spécificité de la démarche de conception proposée par NF EN 62061 apparaît dès l'introduction du texte qui précise en particulier que « *La présente norme donne une méthodologie et les exigences pour... intégrer les sous-systèmes relatifs à la sécurité conçus selon l'ISO 13849 [...]* ». Ce parti pris est confirmé à plusieurs reprises par le texte qui précise sa relation avec les autres normes telles que EN 61204-1 [6], ISO 13849-1 et 2 et EN 61508.

L'approche originale préconisée par NF EN 62061 correspond effectivement à un choix de conception de plus en plus souvent retenu par les constructeurs de machines ou de leurs circuits de commande. En effet, les fabricants de composants d'automatisme mettent couramment sur le marché des « sous-systèmes » élaborés, capables de traiter des fonctions plus ou moins complexes des machines : arrêt d'urgence, contrôle d'arrêts, communication entre entités, etc. La fonction et la performance de sécurité de ces sous-systèmes étant annoncées par leur fabricant (et souvent validées par des organismes indépendants des constructeurs), leur mise en œuvre apparaît plus facilement accessible aux constructeurs de machines.

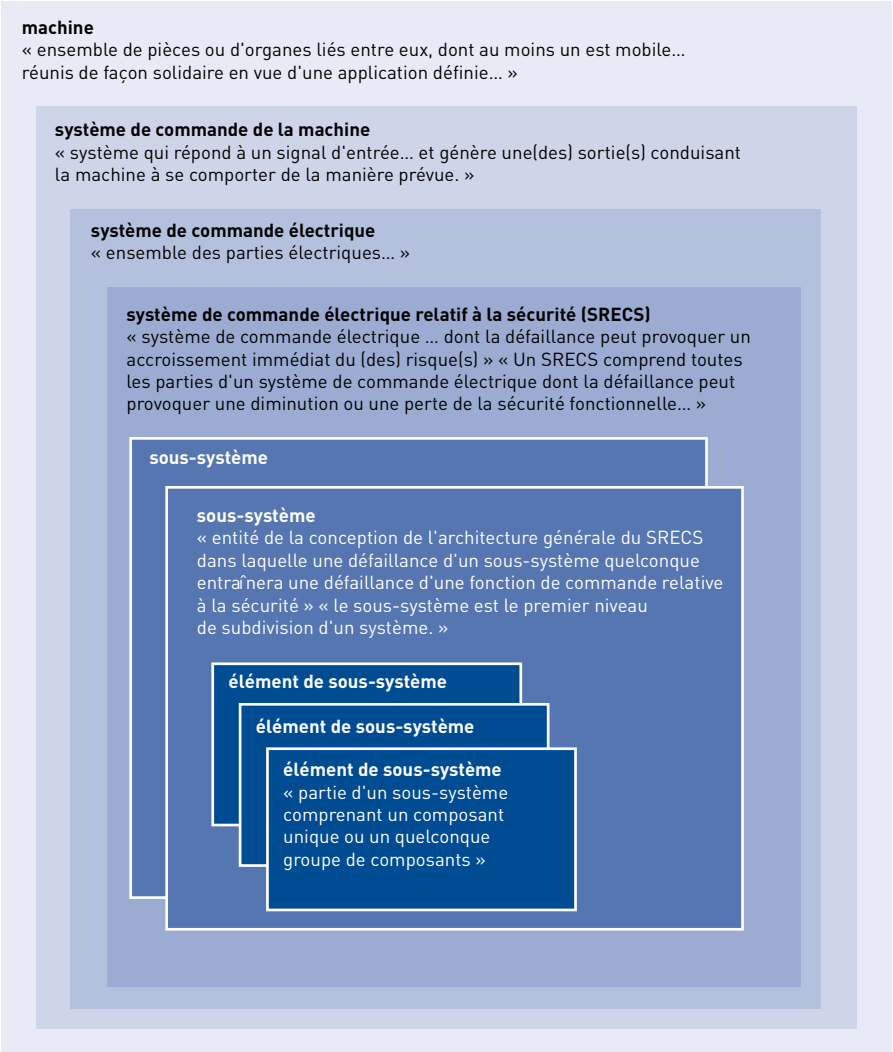
[2] *Annexe I de la Directive 98/37/CE.*

[3] *Une norme européenne harmonisée dont la référence est publiée au Journal Officiel de l'Union Européenne et qui couvre une ou plusieurs exigences essentielles de sécurité confère présomption de conformité aux exigences essentielles concernées par le produit qui est construit conformément à cette norme.*

[4] *Harmonisée le 31.12.2005.*

FIGURE 1

Imbrication des différentes entités matérielles définies par la norme NF EN 62061



La possibilité de réaliser des sous-systèmes à partir de composants logiques, dont la fonction n'est pas significative au regard du fonctionnement de la machine, n'est évidemment pas exclue par NF EN 62061 mais elle devra être réservée à des sous-systèmes simples, mettant en œuvre peu de composants de faible complexité. Dans le cas contraire, ces sous-systèmes devront être conçus en application des autres référentiels normatifs mieux adaptés à la complexité du cas à traiter et aux technologies envisagées [7].

EN RÉSUMÉ

Le normalisateur a spécifié et rédigé la norme NF EN 62061 pour traiter de la conception des Systèmes de commande électriques relatifs à la sécurité (SRECS) préférentiellement par intégration de sous-systèmes finis, disponibles sur le marché, dont la fonction et la performance de sécurité sont connues et qui sont conçus en application des référentiels normatifs adaptés (EN 954-1, ISO 13849-1 ou EN 61508).

Cette norme permettra également de traiter la conception de sous-systèmes réalisés à base de quelques composants logiques simples.

LA DEMARCHE PROPOSÉE

La norme NF EN 62061, articulée autour des trois entités matérielles précédemment évoquées, définit trois principales activités pour le développement du SRECS.

La *Figure 2* montre l'organisation de ces activités qui permettront le passage de l'expression d'un besoin – un circuit de commande de machine ayant à traiter des fonctions de sécurité – à un SRECS conçu pour répondre à ce besoin.

LE PLAN DE SÉCURITÉ FONCTIONNELLE

La norme NF EN 62061 prévoit d'abord la définition et la mise en place d'un cadre permettant le déroulement du développement du SRECS dans les meilleures conditions.

Ce rôle est dévolu au plan de **sécurité fonctionnelle** devant permettre de détailler et tracer les différentes activités techniques et de gestion, nécessaires à la réalisation de la sécurité fonctionnelle prescrite pour le SRECS.

La norme détaille le plan de sécurité fonctionnelle qui doit :

- identifier les activités du développement,
- décrire la politique et la stratégie pour satisfaire aux exigences de sécurité fonctionnelle,
- décrire la stratégie pour réaliser la sécurité fonctionnelle du logiciel,
- identifier les personnes et les ressources responsables de chacune des activités du développement,
- identifier ou établir les procédures et les ressources d'enregistrement et d'entretien des informations appropriées à la sécurité,
- décrire la stratégie de gestion de configuration,
- établir le plan de vérification, et de validation...

NF EN 62061 :
Un plan de sécurité fonctionnelle doit être dressé et documenté pour chaque projet de conception de SRECS et doit être mis à jour autant que nécessaire. Le plan doit inclure les procédures de contrôle des activités spécifiées...

Le plan de sécurité fonctionnelle est un document, voire un recueil de documents, qui permettra au concepteur du SRECS :

- de s'assurer qu'aucun des aspects du développement n'aura été négligé,
- de mettre en place le suivi et la traçabilité du déroulement du projet de SRECS,

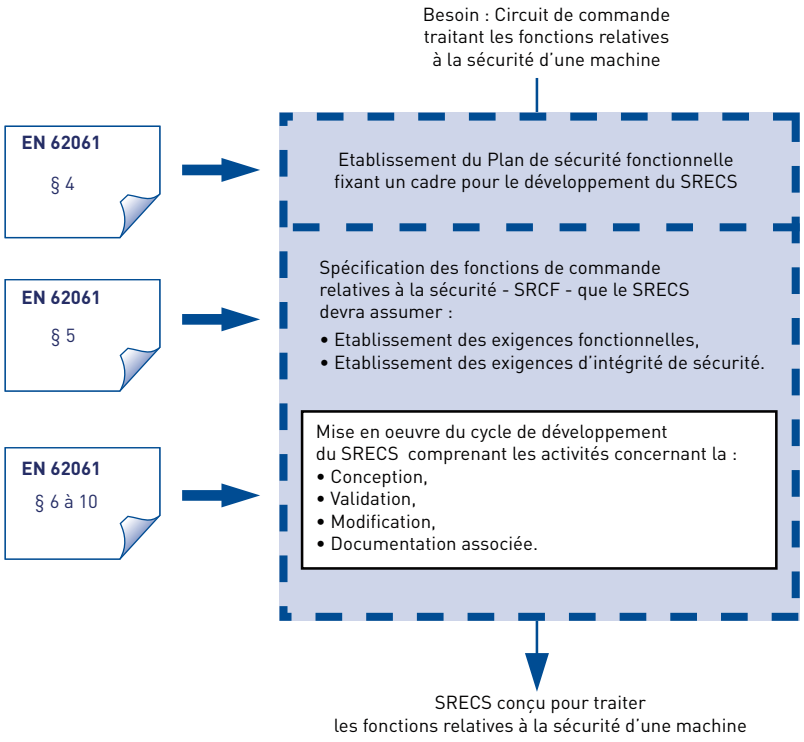
• de faciliter les phases de vérification et de validation du SRECS en incitant à l'écriture préalable des objectifs à atteindre.

Le plan de sécurité fonctionnelle devra être mis à jour et enrichi autant que nécessaire tout au long du déroulement du projet.

La définition et la mise en place d'un plan de sécurité fonctionnelle – cadre formel pour le développement du SRECS – nécessitent une mise en œuvre d'énergie non négligeable, mais les concepteurs doivent être convaincus que la réussite de leur projet de développement sera souvent à ce prix. L'expérience montre en effet que bien des projets n'échouent pas uniquement sur des écueils techniques...

FIGURE 2

Organisation des principales activités de conception du SRECS, d'après NF EN 62061



LA SPÉCIFICATION DES FONCTIONS DU SRECS (SRCF)

Pour bien comprendre son positionnement dans l'ensemble des normes concernant la réduction des risques liés aux machines, l'introduction du texte précise que la norme NF EN 62061 *«est prévue pour être utilisée dans le cadre de la réduction systématique du risque décrite dans l'ISO 12100-1 [8] et conjointement avec l'appréciation du risque selon les principes décrits dans l'ISO 14121 [9] [...] ».*

Les actions menées dans ce cadre, préalablement au développement du SRECS, devront conduire à ce que tous les besoins en fonctions de sécurité soient déterminés.

NF EN 62061 traite de la conception du SRECS, partie du système de commande électrique de la machine dont la défaillance peut provoquer un accroissement des risques. Afin d'atteindre l'objectif de réduction des risques de la machine, les fonctions que le SRECS aura à assumer devront l'être avec un certain niveau de sécurité, c'est-à-dire avec une certaine garantie que le SRECS soit capable d'exécuter de manière nominale les fonctions de commande relatives à la sécurité.

Pour ce faire, avant d'entamer la réalisation du SRECS, chacune des fonctions de commande relatives à la sécurité – SRCF, Safety related control function – doit être complètement spécifiée.

La Figure 3 illustre l'enchaînement des tâches préconisées par la norme pour établir ces spécifications.

LA SPÉCIFICATION DES EXIGENCES FONCTIONNELLES DES SRCF

Les exigences fonctionnelles de chacune des fonctions de commande relatives à la sécurité (SRCF) doivent décrire complètement :

- le fonctionnement attendu,
- ses conditions d'activation ou d'inactivation,
- sa fréquence de fonctionnement,
- son temps de réponse,
- son interfaçage avec le reste de la machine,
- l'environnement de fonctionnement,
- la (des) fonction(s) de réaction à l'anomalie du SRECS...

Sur le plan méthodologique, la norme ne détaille pas cette phase de spécification fonctionnelle. Les concepteurs devront donc se tourner vers des outils ou méthodes de leur choix, les mieux adaptés pour assurer la complétude et la validité des spécifications.

Il est essentiel de noter ici l'importance qu'attache le normalisateur à l'aptitude à la fonction du futur SRECS. En effet, des prescriptions minimales d'immunité CEM [5] sont déjà définies par la norme au niveau fonctionnel pour les SRCF si elles doivent s'exercer dans un environnement industriel.

LA SPÉCIFICATION DES EXIGENCES D'INTEGRITÉ DE SÉCURITÉ DES SRCF

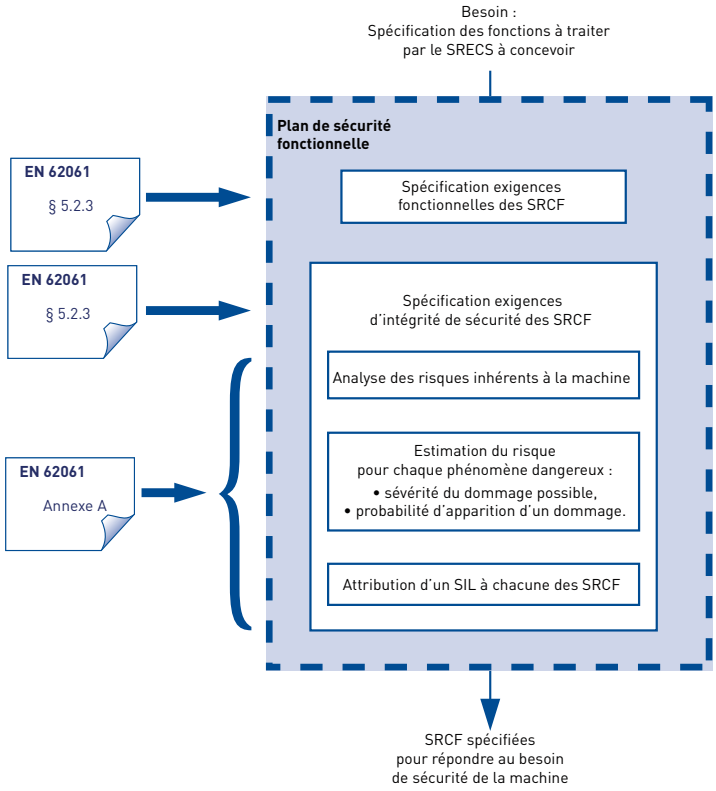
La norme NF EN 62061 est plus prolixe concernant ce volet de la spécification des SRCF. Elle propose les outils nécessaires à l'établissement de ces spécifications, en particulier des définitions et une méthodologie.

L'objectif à atteindre au terme de cette phase de spécification est de définir, pour chacune des SCRF, des exigences d'**intégrité de sécurité** exprimées en termes de **SIL** (Safety integrity level ou niveau d'intégrité de sécurité).

[5] *La norme NF EN 62061 reprend comme valeurs de base d'immunité, les exigences définies par la norme NF EN 61000-6-2 et prescrit des exigences complémentaires dans son annexe 4*

FIGURE 3

Organisation des principales activités de spécification des fonctions de commande relatives à la sécurité - SRCF, d'après NF EN 62061



NF EN 62061 :

Intégrité de sécurité : probabilité pour qu'un SRECS ou ses sous-systèmes exécutent de manière satisfaisante les fonctions de commande relatives à la sécurité requises dans toutes les conditions spécifiées.
SIL : niveau discret permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions de commande relatives à la sécurité à allouer aux SRECS, le niveau 3 d'intégrité de sécurité possédant le plus haut degré d'intégrité et le niveau 1 possédant le plus bas.

Un préambule concernant l'intégrité de sécurité

Lorsqu'elle traite de l'intégrité de sécurité des SRCF, la norme fait correspondre à chacun des niveaux de SIL, une valeur prévisionnelle (valeur cible) admissible de probabilité de défaillance dangereuse par heure – PFH_D. Le *Tableau I*, extrait du texte de norme, établit cette correspondance.

Le tableau de correspondance montre que plus le risque couvert par la SRCF en question sera important, moins sa perte pourra être tolérée ; la probabilité de défaillance dangereuse du système pouvant entraîner la perte de cette SRCF sera d'autant plus faible.

L'assignation de ce niveau de SIL à atteindre pour la fonction de sécurité est une étape essentielle du développement du SRECS, car cette revendication aura des conséquences fortes sur les performances et la réalisation de toutes les entités qui interviendront dans le traitement de ladite SRCF.

Ainsi, au terme du développement du SRECS et pour que celui-ci soit acceptable pour le traitement de la SRCF, le concepteur devra s'assurer que :

- le SIL de chaque sous-système (vis-à-vis des contraintes architecturales et de l'intégrité de sécurité systématique) impliqué dans une SRCF donnée soit au minimum égal au SIL prescrit pour la SRCF,
- la somme des probabilités de défaillance dangereuse de tous les sous-systèmes impliqués dans une SRCF donnée soit inférieure à la valeur cible de probabilité de défaillance dangereuse, déduite du niveau de SIL affecté à la SRCF.

TABLEAU I

Correspondance entre SIL et valeur de probabilité de défaillance dangereuse par heure à réaliser par le SRECS – d'après le tableau 3 de la norme NF EN 62061

Niveau d'intégrité de sécurité	Probabilité de défaillance dangereuse par heure (PFHD)
3	$\geq 10^{-8}$ à $<10^{-7}$
2	$\geq 10^{-7}$ à $<10^{-6}$
1	$\geq 10^{-6}$ à $<10^{-5}$

Il est important d'insister sur le fait que le SIL *n'est pas égal* à une probabilité de défaillance dangereuse de la fonction de sécurité, mais qu'à chacune des valeurs de SIL *correspond* une valeur cible de probabilité de défaillance dangereuse. En effet, réduire un SIL à la seule probabilité de défaillance dangereuse – comme c'est trop souvent le cas – peut avoir pour conséquences de négliger d'autres aspects primordiaux du développement du SRECS et de nuire au final à sa performance de sécurité réelle.

Une méthodologie pour l'attribution d'un SIL à chacune des SRCF est décrite à l'annexe A de la norme NF EN 62061. Le statut informatif de cette annexe n'enlève rien à son intérêt pour les concepteurs de circuits de commande relatifs à la sécurité. La méthode préconisée consiste d'abord à déterminer les valeurs de quatre paramètres relatifs au risque à couvrir, puis à en déduire le SIL cible pour la SRCF correspondante. Nous allons passer en revue ces différents paramètres et préciser ce qu'ils recouvrent.

L'identification des phénomènes dangereux de la machine

Le préalable à l'estimation du risque est l'identification de l'ensemble des phénomènes dangereux liés à l'utilisation de la machine ou de l'installation concernée. Comme cette activité n'entre pas dans le champ d'application de la norme NF EN 62061, les concepteurs devront se tourner vers des outils ou des méthodes adaptés pour s'assurer de la complétude et de la validité de cette partie de l'analyse des risques. En pratique, l'identification des phénomènes dangereux est issue de l'expérience et du savoir-faire des experts du domaine et nécessite une bonne connaissance de la machine et de son environnement.

Pour mener à bien cette tâche, les concepteurs pourront s'appuyer sur l'annexe A du projet de norme pr NF EN ISO 14121-1 déjà cité et sur des supports généraux [10, 11] qui pourront être adaptés à la situation à traiter.

La norme NF EN 62061 traite uniquement des risques pouvant être réduits par l'intervention d'une fonction de sécurité réalisée par le SRECS. Il faudra donc extraire de l'inventaire des phénomènes dangereux liés à la machine ceux qui pourront être réduits par l'intervention du SRECS, comme par exemple le contrôle de la fermeture d'un protecteur asservi.

Ce travail d'analyse nécessite que le concepteur prenne en compte la machine équipée de l'ensemble de ses dispositifs et mesures de protection. Le choix des dispositifs et des mesures de protection aura dû être fait préalablement, dans le cadre général de la réduction systématique du risque décrit dans l'ISO 12100-1, la norme NF EN 62061 n'abordant pas ce sujet.

L'étape suivante d'estimation du risque sera conduite pour chacun des risques devant être réduit par l'intervention d'une fonction de sécurité supportée par le SRECS à concevoir.

L'estimation du risque pour chaque phénomène dangereux

Le risque lié à chacun des phénomènes dangereux identifiés doit être évalué à partir de deux paramètres, la sévérité du dommage possible (Se) et de la probabilité d'apparition du dommage en question (Cl). La norme propose en annexe informative une méthode pour l'évaluation de ces paramètres *(cf. Encadré 1)*. De ces résultats pourra être déduite la spécification de sécurité de chaque fonction de sécurité qui interviendra sur le phénomène dangereux en question.

Attribution d'un SIL à une SRCF

A partir des valeurs estimées pour Se et Cl, la norme propose de déterminer le SIL requis pour la SRCF à partir du *Tableau II* extrait de la norme.

En résumé

Les prescriptions de la norme concernant la spécification des SRCF sont relativement claires et lisibles. Elles

Encadré 1

Paramètres à estimer en préalable à l'attribution d'un SIL à une SRCF

la sévérité du dommage possible - Se

Ce paramètre représente la gravité du dommage, s'il se produit.
Il doit être déterminé pour chacun des risques.

	Conséquences	Sévérité (Se)
Irréversible	mort, perte d'un œil ou d'un bras	4
	membre(s) brisé(s), perte d'un(de) doigt(s)	3
Réversible	nécessitant l'attention d'un praticien médical	2
	nécessitant des premiers soins	1

la probabilité d'apparition d'un dommage – Cl

Ce paramètre peut être déduit de l'estimation de trois paramètres permettant d'apprécier la probabilité d'apparition d'un dommage : **Cl = Fr + Pr + Av**

Fr - Fréquence et durée de l'exposition

L'estimation de ce paramètre doit prendre en compte en particulier :
- le besoin d'accéder à la zone dangereuse en fonction des modes d'utilisation,
- la nature de l'accès (réglage, approvisionnement de la machine, etc.).

La défaillance éventuelle de la fonction n'est pas prise en compte à ce stade.

Fréquence d'exposition	Durée > 10 min	Durée <= 10 min
≥ 1 par heure	5	5
< 1 par heure à ≥ 1 par jour	5	4
< 1 par jour à ≥ 1 toutes les 2 semaines	4	3
< 1 toutes les 2 semaines à ≥ 1 par an	3	2
< 1 par an	2	2

Pr - Probabilité d'apparition d'un événement dangereux

L'estimation de ce paramètre prend en compte en particulier :
- le comportement prévisible des parties de la machine liées au phénomène dangereux,
- les caractéristiques spécifiées ou prévisibles du comportement de l'homme dans son interaction avec les parties de la machine liées au phénomène dangereux.

Probabilité d'apparition	Probabilité (Pr)
Très forte	5
Probable	4
Possible	3
Rare	2
Négligeable	1

Av - Probabilité d'évitement ou de limitation d'un dommage

L'estimation de ce paramètre se réfère à des données très subjectives et doit prendre en compte en particulier :
- la soudaineté et la vitesse de l'apparition de l'événement dangereux,
- la possibilité de s'écarter du phénomène dangereux.

Probabilité d'évitement ou de limitation d'un dommage (AV)	
Impossible	5
Rare	3
Problable	1

permettent de définir les informations à utiliser pour l'établissement de ces spécifications et celles qui devront figurer dans le document de spécification.

La méthode proposée par l'annexe A de la norme pour l'attribution du SIL requis pour une SRCF donnée est simple et bien décrite. La norme insiste sur la nécessité de conduire cette activité de manière collégiale et consensuelle, en prenant en compte les points de vue des différents intervenants sur la machine (du concepteur à l'utilisateur final). En effet, seule une telle démarche pourra permettre une estimation réaliste de certains des paramètres évoqués ci-dessus et donc, à terme, de déterminer le SIL le plus juste, adapté à chacune des fonctions de sécurité.

De plus, le SIL retenu pour une SRCF ayant des incidences fortes sur le développement du SRECS, pour que le «prix à payer» pour le SRECS soit accepté par tous, il est essentiel que les spécifications établies aient été au préalable acceptées par tous.

DE LA SRCF AU SRECS...

Une fois le cadre procédural mis en place et les SRCF complètement spécifiées, la phase de conception du SRECS peut débuter.

L'objectif fixé par la norme NF EN 62061 à la démarche qu'elle préconise est de permettre la conception d'un SRECS qui satisfasse à toutes les prescriptions édictées pour chacune des SRCF.

Pour ce faire, les spécifications fonctionnelles et d'intégrité de sécurité édictées pour chacune des SRCF devront être déclinées sous la forme d'exigences pour le SRECS, afin d'être prises en compte dans sa réalisation.

Pour satisfaire les exigences d'intégrité de sécurité exprimées pour les SRCF, le SIL requis pour le SRECS devra être, s'il réalise plusieurs fonctions de sécurité, au minimum égal au plus grand SIL prescrit pour les SRCF dans les conditions d'utilisation spécifiées de la machine.

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 :
  - pour l'évitement des défaillances systématiques du matériel,
  - pour la maîtrise des anomalies systématiques,
  - 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.

TABLEAU II

Exemple d'attribution du niveau de SIL - d'après la Figure A.3 de la norme NF EN 62061

Sévérité (Se)	Classe (Cl)				
	4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Zone noire = mesures de sécurité prescrites
Zone grise (OM) = autres mesures

L'essentiel du texte de la norme concerne la conception et le développement du SRECS, mais s'il existe sur le marché un SRECS répondant parfaitement au besoin exprimé, ou encore pour les concepteurs que la tâche de développement rebuterait, la norme propose la possibilité de choisir un SRECS existant. Dans une telle alternative, il restera au concepteur du circuit de commande de s'assurer que le dispositif retenu remplisse effectivement les prescriptions établies pour les SRCF. Pour cette vérification, il devra s'appuyer sur une partie des prescriptions de la norme pour la conception du SRECS [6] et sur les données fournies par le constructeur du SRECS pressenti.

En plus d'un certain nombre d'exigences générales concernant le SRECS, la norme insiste pour que les exigences comportementales lors de la détection d'anomalie ainsi que les exigences pour l'intégrité de sécurité systématique soient prises en compte même pour le choix du SRECS. Lors d'un tel choix de conception, les aspects logiciels, intégration, etc. resteront à traiter par le constructeur du circuit de commande de la machine.

EXIGENCES COMPORTEMENTALES LORS DE LA DÉTECTION D'UNE ANOMALIE DANS LE SRECS

La norme NF EN 62061 prévoit de spécifier, en plus des SRCF, certaines fonctions qui devront être implémentées dans le SRECS pour garantir son intégrité de sécurité.

Une des difficultés à la lecture de la norme est que ces fonctions y sont abordées bien avant que leur nécessité apparaisse. Nous nous limiterons donc à une présentation générale de leur rôle en précisant que, le cas échéant, leur spécification se fera lors de la conception des sous-systèmes, pour en améliorer la performance de sécurité.

Contrairement aux SRCF, les fonctions de réaction aux anomalies et de diagnostic n'ont pas d'incidence directe et immédiate sur le fonctionnement en sécurité de la machine. Elles sont destinées à surveiller le bon fonctionnement du matériel constituant le SRECS afin de garantir la performance de sécurité qui lui a été assignée. Elles seront définies et implémentées au cours du processus de développement du SRECS.

Fonctions de réaction aux anomalies

Le concepteur du SRECS doit spécifier les fonctions de réaction aux anomalies. Elles devront être implémentées dans tous les sous-systèmes ayant une tolérance aux anomalies du matériel supérieure à zéro *(cf. Encadré 2)* pour garantir la détection des anomalies dangereuses. La spécification éventuelle de ces fonctions nécessitant parfois une connaissance du détail des sous-systèmes, ne pourra bien entendu être finalisée qu'après leur conception.

6 *§ 6.5 de NF EN 62061*

Fonctions de diagnostic

Comme pour la fonction de réaction aux anomalies, la nécessité des fonctions de diagnostic apparaîtra seulement lors de la conception du détail des sous-systèmes. Sans trop anticiper sur ce sujet, nous pouvons cependant préciser qu'en fonction du modèle d'architecture retenu pour les sous-systèmes constituant le SRECS, il peut être nécessaire de prévoir des fonctions de diagnostic pour atteindre l'objectif d'intégrité de sécurité pour le SRECS. Dans un tel cas, les fonctions nécessaires devront être complètement spécifiées et implémentées dans le SRECS.

PRESCRIPTIONS POUR L'INTÉGRITÉ DE SÉCURITÉ SYSTÉMATIQUE

Pour satisfaire les prescriptions pour l'intégrité de sécurité systématique, la norme énonce des mesures techniques, organisationnelles, procédurales, etc. qui devront être appliquées pour l'exécution de chacune des tâches de la conception du SRECS, pour les aspects matériel et logiciel. Les prescriptions de la norme sont identiques quel que soit le niveau de SIL requis pour le SRECS.

De la prise en compte effective de ces prescriptions dépendra la capacité du SRECS à satisfaire ou non les spécifications des SRCF en termes d'intégrité de sécurité. Ces prescriptions couvrent en particulier :

- l'évitement des défaillances systématiques du matériel,
- la maîtrise des anomalies systématiques,
- le volet immunité de la compatibilité électromagnétique (CEM).

Pour prendre en compte les prescriptions fonctionnelles déjà évoquées, et en particulier les prescriptions d'immunité face aux perturbations électromagnétiques, la norme NF EN 62061 décrit les critères d'aptitude définissant le comportement acceptable du SRECS en présence des perturbations décrites dans la norme NF EN 61000-6-2 [12] et l'annexe 4 de NF EN 62061.

Ces critères d'aptitude sont les suivants :

- des conditions non sûres ou des phénomènes dangereux ne doivent pas être introduits et
- aucune perte de SRCF ne doit se produire ou
- la SRCF peut être perturbée temporairement, voire de façon permanente, sous réserve que la machine soit dans un état sûr avant qu'un phénomène dangereux ne puisse se produire.
- Lorsqu'une perturbation peut entraîner la destruction de composants, on doit garantir que la sécurité n'est pas affectée.

L'immunité du SRECS face aux perturbations électromagnétiques sera vérifiée lorsque celui-ci sera réalisé par des analyses ou des tests adaptés.

NF EN 62061 :
Intégrité de sécurité systématique : probabilité pour qu'un SRECS ou ses partie de l'intégrité de sécurité d'un SRECS ou de ses sous-systèmes qui se rapporte à sa résistance aux défaillances systématiques dans un mode dangereux
Défaillance systématique : défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés.

RÉALISATION DU SRECS

La *Figure 4* montre l'enchaînement des différentes tâches préconisées par la norme NF EN 62061 pour réaliser le SRECS, c'est-à-dire passer de la spécification des SRCF à un dispositif matériel qui les prendra en charge.

La première tâche à effectuer lors de cette démarche de conception du SRECS est la conception de son architecture

Conception de l'architecture du srecs

Cette étape de la réalisation du SRECS est celle qui permettra le passage des SRCF spécifiées (point de vue fonctionnel) aux entités matérielles qui constitueront le SRECS (point de vue matériel).

La *Figure 5* illustre cette phase de conception de l'architecture.

La norme NF EN 62061 détaille ainsi les étapes de la conception :

- décomposition de chaque SRCF en blocs fonctionnels (sous-fonctions),
- détail des prescriptions d'intégrité de sécurité pour chaque bloc fonctionnel,
- attribution de chaque bloc fonctionnel à un seul sous-système matériel,
- vérification de l'affectation effective de chacun des blocs fonctionnels à un sous-système matériel,
- vérification des prescriptions de chacun des sous-systèmes.

En pratique, la décomposition de chacune des SCRF en sous-fonctions ne peut pas se faire sans une connaissance approfondie de l'ensemble de la démarche de conception proposée par la norme. En effet, le texte est souvent approximatif quand il s'agit de l'ordre de déroulement des différentes tâches à exécuter, de la profondeur des décompositions fonctionnelles, etc. De plus, la décomposition des SRCF ne pourra se faire sans quelques règles pratiques, ne figurant pas toujours de manière explicite dans le texte de la norme :

- la décomposition fonctionnelle pouvant théoriquement se faire jusqu'au niveau des composants logiques élémentaires, il est important d'en limiter la profondeur et le niveau de détail.

Cette décomposition doit se limiter strictement à 3 niveaux du fait de la structure même de la norme quant aux entités matérielles qu'elle envisage (*cf. Figure 1)* :

- le SRECS prenant en charge la fonction (SRCF),
- le sous-système prenant en charge la sous-fonction ou bloc fonctionnel,
- l'élément de sous-système prenant en charge l'élément de sous-fonction ou élément bloc fonctionnel [7] ;

- la prescription de SIL pour la SRCF doit se répercuter telle qu'elle sur chacune des sous-fonctions résultantes de la décomposition (pour une SRCF de SILn, la spécification de chacune des sous-fonctions devra au minimum être du SILn) ;
- chaque bloc fonctionnel doit être attribué à un sous-système unique ;
- un sous-système peut prendre en charge plusieurs blocs fonctionnels ;
- la décomposition fonctionnelle ne peut se faire de manière efficace sans une connaissance approfondie des solutions techniques envisageables, c'est-à-dire disponibles sur le marché (sous-système, élément de sous-système). Une autre approche consiste à procéder par itérations successives, en confrontant le résultat de la première décomposition fonctionnelle aux catalogues de composants des différents fabricants et, le cas échéant, à modifier le premier découpage pour permettre préférentiellement l'utilisation d'éléments du marché.

FIGURE 4

Organisation des principales activités de conception du SRECS, d'après NF EN 62061

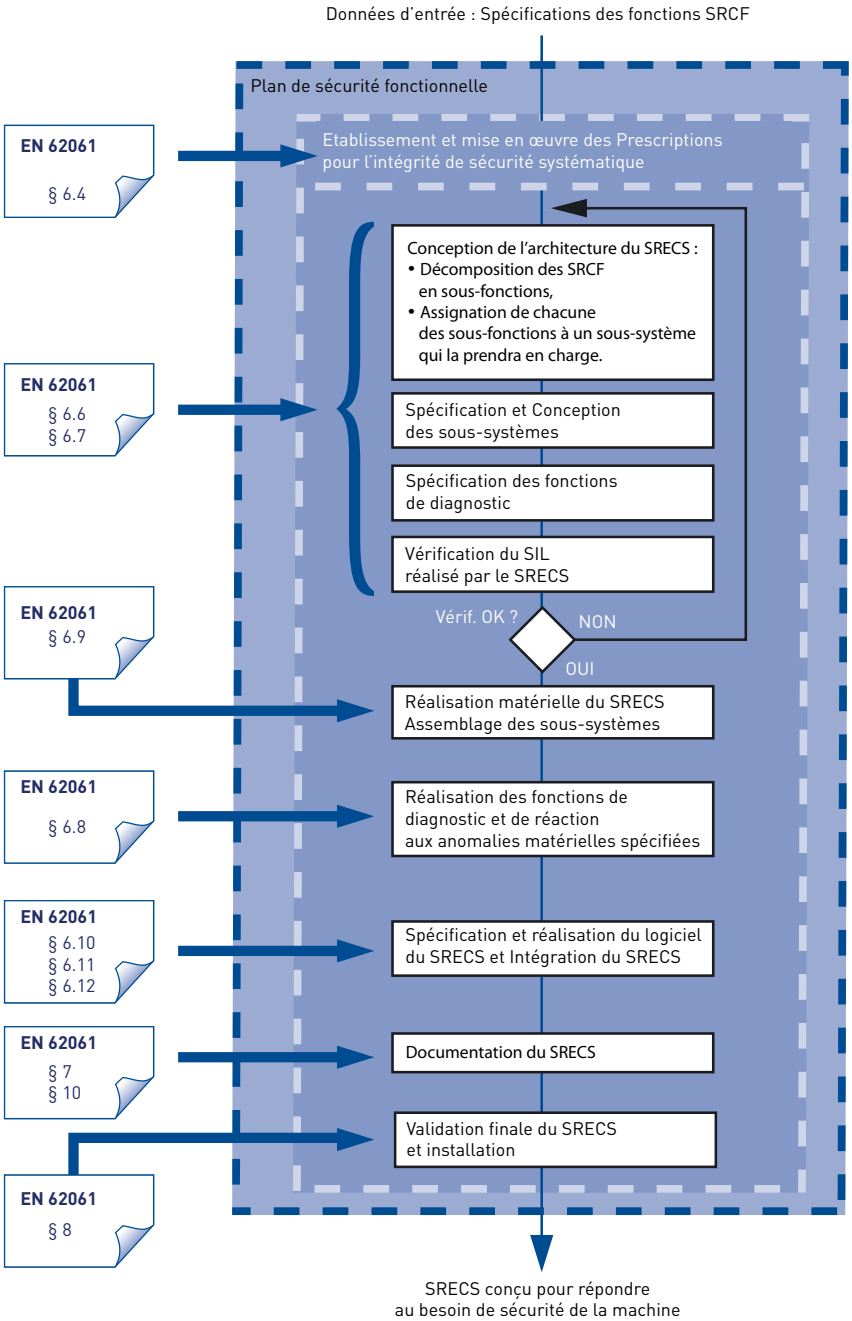
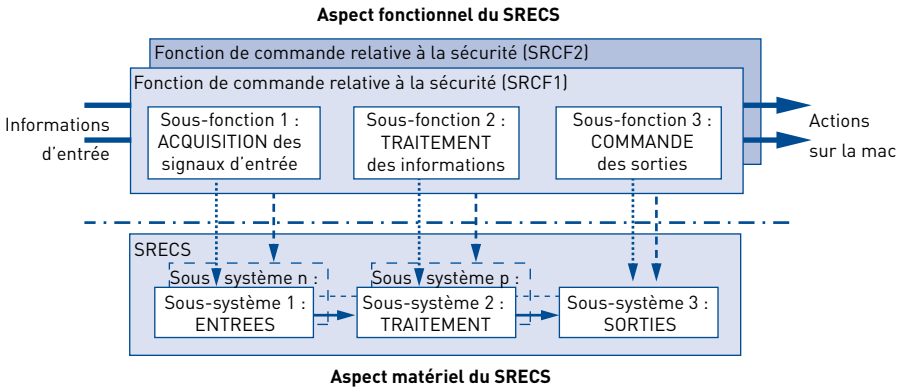


FIGURE 5

Principe pour la conception de l'architecture du SRECS, d'après NF EN 62061



La phase d'affectation de chacune des sous-fonctions (blocs fonctionnels) à un sous-système matériel va permettre d'élaborer la spécification fonctionnelle et de sécurité dudit sous-système.

La phase de vérification consistera en particulier à constater formellement :

- que chacune des sous-fonctions spécifiées a été effectivement attribuée à un sous-système,
- que les spécifications fonctionnelles et d'intégrité de sécurité édictées pour les sous-systèmes sont conformes aux spécifications de la SRCF et, donc, de chacune des sous-fonctions qu'ils auront à prendre en charge.

Objectif d'intégrité de sécurité à satisfaire par le SRECS

Le SIL à satisfaire par le SRECS dépendra donc du SIL spécifié pour chacune des SRCF qu'il a à traiter. Au terme de sa conception, l'objectif à atteindre par le SRECS est de permettre une réponse positive à la question essentielle suivante : le SRECS conçu répond-il aux prescriptions édictées pour les fonctions relatives à la sécurité spécifiées ?

Pour permettre au concepteur de donner une réponse justifiée à cette question fondamentale, NF EN 62061 définit les trois volets de l'intégrité de sécurité auxquels devra satisfaire le SRECS. Pour pouvoir réaliser un SIL spécifié, le SRECS devra répondre à l'ensemble de ces trois aspects de l'intégrité de sécurité :

- la probabilité de défaillance dangereuse aléatoire du matériel,
- les contraintes architecturales,
- l'intégrité de sécurité systématique des sous-systèmes qui composent le SRECS.

De plus, pour une intégrité de sécurité systématique et des contraintes architecturales données, le niveau de SIL réalisé par le SRECS sera au mieux égal au plus faible SIL que peut revendiquer chacun des sous-systèmes constituant le SRECS.

Dans le paragraphe suivant, nous allons détailler ces trois volets de l'intégrité de sécurité, en insistant sur les méthodes proposées pour leur mise en œuvre et leur évaluation.

7 *Ce dernier niveau de décomposition n'est pas obligatoire, la décomposition pourra s'arrêter le cas échéant au niveau du sous-système.*

De la sous-fonction au sous-système...

Une fois les sous-fonctions relatives à la sécurité complètement spécifiées sur les plans fonctionnel et de l'intégrité de sécurité, l'architecture générale du SRECS est, de fait, définie. La phase de conception des sous-systèmes peut être engagée.

L'objectif fixé par la norme NF EN 62061 est de permettre la conception d'un sous-système qui satisfasse à toutes les prescriptions édictées pour chacune des sous-fonctions qu'il aura à traiter.

Pour ce faire, les exigences fonctionnelles et d'intégrité de sécurité édictées pour chacune des sous-fonctions devront être déclinées sous la forme d'exigences pour les sous-systèmes qui auront à les traiter, afin d'être prises en compte dans leur réalisation.

Les exigences fonctionnelles et d'intégrité de sécurité exprimées pour les sous-fonctions devront, en s'appuyant sur la norme NF EN 62061, être traduites pour le sous-système 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,
- pour définir son comportement lors de la détection d'une anomalie.

NF EN 62061 propose deux approches envisageables pour la réalisation matérielle du sous-système :

- la conception et le développement d'un sous-système particulier,
- ou le choix d'un sous-système existant.

Dans cette dernière alternative, le concepteur du circuit de commande devra s'assurer que le dispositif retenu remplit toutes les prescriptions établies pour les sous-fonctions correspondantes. Pour cette vérification, il devra s'appuyer sur une partie des prescriptions de la norme pour la conception du sous-système et sur les données fournies par le constructeur du dispositif pressenti.

En plus d'un certain nombre d'exigences générales concernant le sous-système, la norme insiste pour que les exigences comportementales lors de la détection d'anomalie ainsi que les exigences pour l'intégrité de sécurité systématique soient prises en compte même pour le choix du sous-système.

Documentation concernant le sous-système

Que ce soit dans le cas d'un choix ou le cas de la réalisation d'un sous-système, le constructeur d'un sous-système doit fournir toutes les informations le concernant comme par exemple :

- la spécification fonctionnelle des fonctions et des interfaces,
- le SIL maximum auquel il peut prétendre - SIL_{CL} - ou, si le sous-système a été conçu en application de la norme NF EN ISO 13849-1, la Catégorie,
- le taux de défaillance estimé,
- les contraintes liées à l'environnement et à la durée de vie,
- les tests et/ou les exigences de maintenance,
- la couverture de diagnostic et l'intervalle des tests de diagnostic si nécessaire,
- les limitations afin d'éviter les défaillances systématiques,
- l'identification de la configuration du matériel et du logiciel...

Elle précise par ailleurs qu'un sous-système mettant en œuvre des composants complexes doit satisfaire aux prescriptions de la norme NF EN 61508 parties 2 et 3

Comme on l'a déjà évoqué, les trois aspects de l'intégrité de sécurité à prendre en compte pour le SRECS, donc par voie de conséquence pour les sous-systèmes, sont les suivants :

- la probabilité de défaillance dangereuse aléatoire du matériel,
- les contraintes architecturales,
- l'intégrité de sécurité systématique des sous-systèmes que comprend le SRECS.

Ces trois aspects de l'intégrité de sécurité vont donc guider la démarche pratique de conception du sous-système.

Intégrité de sécurité systématique

Les mesures concernant l'intégrité de sécurité systématique s'appliquant au sous-système reprennent pour partie et complètent celles prescrites pour le SRECS. Les exigences formulées par la norme sont identiques quel que soit le SIL visé pour le sous-système. La satisfaction à l'ensemble des prescriptions permettra de revendiquer indifféremment un SIL 1, 2 ou 3. La norme ne prévoit en effet aucune dérogation pour un objectif de SIL 1 par rapport à un objectif de SIL 3.

L'application des mesures et méthodes préconisées par la norme est essentielle et leur mise en place, indispensable au bon déroulement du projet, ne pose pas de grandes difficultés techniques.

Conception de l'architecture du sous-système

Cette étape de la réalisation du sous-système est celle qui permettra le passage des sous-fonctions spécifiées (point de vue fonctionnel) aux entités matérielles qui constitueront le sous-système (point de vue matériel).

La *Figure 6* illustre cette phase de conception de l'architecture du sous-système.

La décomposition éventuelle des sous-fonctions (blocs fonctionnels) en éléments de blocs fonctionnels a déjà pu être faite en même temps que la décomposition des SRCF en sous-fonctions [9]. En effet, la norme NF EN 62061 prévoyant seulement trois niveaux matériels pour la conception du SRECS, il est essentiel d'avoir toujours une vue d'ensemble de l'architecture en cours de développement.

Chacune des sous-fonctions élémentaires devra ensuite être confiée à un élément de sous-système. La phase d'affectation de chacune des sous-fonctions éléments (éléments de blocs fonctionnel) à un élément de sous-système va permettre d'élaborer la spécification des éléments de sous-système afin de pouvoir soit choisir des éléments existants sur le marché, soit les concevoir.

Si l'architecture du SRECS découlait implicitement du découpage fonctionnel des SRCF, la conception de l'architecture des sous-systèmes, caractéristique déterminante de la performance de sécurité maximale que pourra atteindre le sous-système, n'est pas elle implicite. Elle est le résultat d'une démarche spécifique présentée ci-après et illustrée par la *Figure 7*.

8 *§ 6.7.3 de NF EN 62061*

9 *§ 6.3.1 de NF EN 62061*

Quelques éléments pratiques pour la conception de l'architecture du sous-système

La démarche de réalisation des sous-systèmes proposée par la norme NF EN 62061 est itérative. Elle prévoit, si l'objectif d'intégrité de sécurité n'est pas satisfait lors de la détermination du SIL atteint au final par le sous-système, de le modifier en intervenant sur les paramètres pertinents qui sont accessibles à son concepteur, et ce, jusqu'à ce que le SIL visé soit atteint.

La norme présente **4 modèles types d'architecture**. Pour chacun des modèles d'architecture, les paramètres accessibles au concepteur pour atteindre le niveau de SIL prescrit sont plus ou moins nombreux et, de ce fait, le concepteur disposera de plus ou moins de possibilités d'intervention pour satisfaire les prescriptions édictées.

La norme présente seulement **4 modèles types d'architecture** [9]. Pour chacun des sous-systèmes, le concepteur devra donc se limiter à une de ces architectures. Tout autre choix ne pourra pas être qualifié dans le cadre de la norme NF EN 62061.

La norme ne donne aucune méthode pour le choix initial du modèle d'architecture. Dans les faits, ce premier choix dépendra de la « culture » du concepteur. En effet, un concepteur expérimenté « saura » quel modèle d'architecture répond le mieux aux spécifications d'intégrité de sécurité spécifiées. Pour les autres concepteurs, il restera la possibilité de choisir a priori l'architecture A puis, si la probabilité de défaillance dangereuse ne peut pas atteindre la spécification d'intégrité de sécurité du sous-système, il devra recommencer ses calculs sur la base d'une architecture B, etc.

Choix des éléments de sous-système

Une fois l'architecture du sous-système définie et les paramètres critiques inventoriés, le choix des éléments de sous-systèmes doit être arrêté en fonction de leurs spécifications.

Certaines de ces données restant souvent confidentielles, les concepteurs de SRECS risquent d'être confrontés à de grandes difficultés pour obtenir des données chiffrées fiables concernant certains composants. Toutefois, ces données étant indispensables, il sera parfois nécessaire de préférer tel composant dont les caractéristiques sont annoncées par son constructeur à tel autre dont les données sont indisponibles.

FIGURE 6

Principe pour la conception de l'architecture du sous-système, d'après NF EN 62061

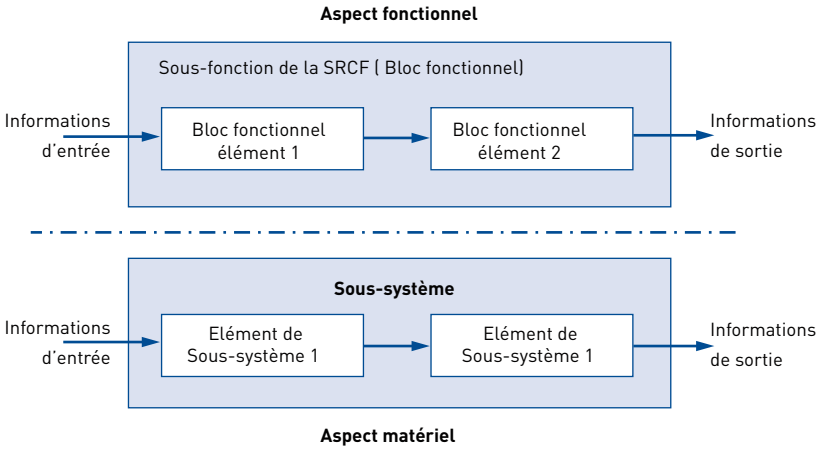
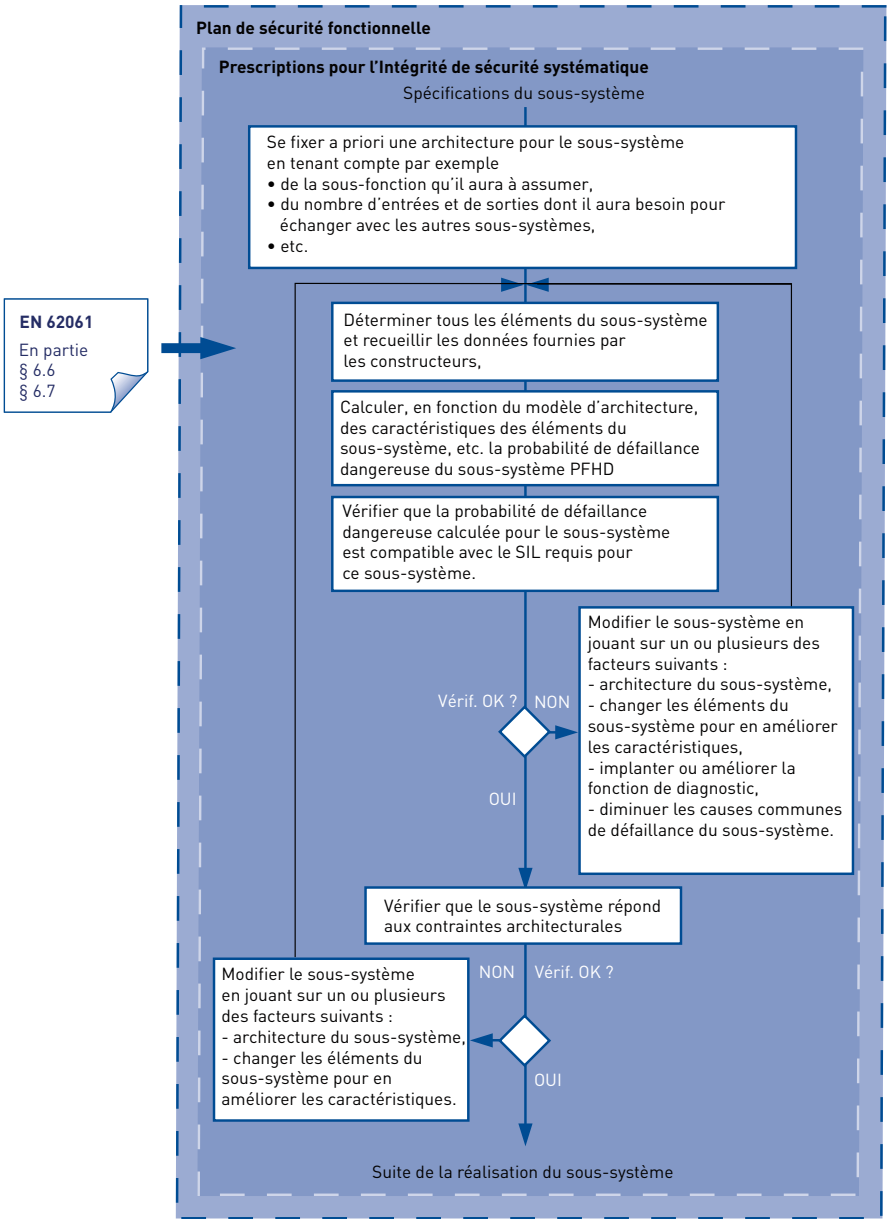


FIGURE 7

Organisation des principales activités pour la conception de l'architecture du sous-système, d'après NF EN 62061



Documentation concernant les éléments de sous-système

Pour permettre au concepteur du SRECS d'effectuer ce choix, les constructeurs de composants doivent fournir un certain nombre d'informations sur leurs composants comme par exemple :
- les spécifications fonctionnelle et d'interfaçage,
- les modes de défaillance et leur probabilité d'occurrence,
- les contraintes liées à l'environnement et à la durée de vie,
- les limitations afin d'éviter les défaillances systématiques,
- la tolérance aux anomalies du matériel...

Des bases de données peuvent également permettre de pallier à ces difficultés en délivrant des valeurs pour des composants génériques, des textes de normes peuvent indiquer des valeurs par défaut pour certains types de composants, mais ces sources d'informations sont toujours à utiliser avec précaution. En effet, la norme NF EN 62061 prévoit un calcul de probabilité de défaillance dangereuse du sous-système et, si la rigueur de la méthode de calcul prônée est incontestable, la réalité des résultats de ce calcul dépendra donc de la validité des données d'entrée.

Il faudra donc toujours veiller à ce que ces calculs soient représentatifs du sous-système réellement conçu et non pas d'un hypothétique sous-système théorique idéal qui n'aurait d'autre finalité que de servir le besoin des calculs.

Calcul de la probabilité de défaillances dangereuses du sous-système – cas général

NF EN 62061 propose deux approches pour aborder cette tâche, selon que le sous-système réponde ou non à une catégorie donnée selon l'ISO 13849-1. La dernière possibilité est considérée par la norme comme étant le cas général.

Le texte présente une méthode simplifiée de calcul de la probabilité de défaillance dangereuse – PFH_D – du sous-système en cours de réalisation. Le premier critère intervenant dans ce calcul est l'architecture que le concepteur a retenue pour son sous-système.

Ce choix de l'architecture retenue est essentiel car il rendra certaines des données d'entrée de ce calcul accessibles au concepteur pour améliorer, si besoin est, la probabilité de défaillance dangereuse de son sous-système.

En effet, dans l'hypothèse où la probabilité de défaillance dangereuse par heure d'un sous-système ne serait pas compatible avec le SIL requis, il conviendra alors que le concepteur modifie ses choix de conception et intervienne sur les paramètres qui lui sont accessibles pour pouvoir atteindre l'objectif fixé.

▣ Les données d'entrée pour le calcul de la probabilité de défaillance dangereuse du sous-système et leurs origines

La méthode de calcul simplifiée de la probabilité de défaillance dangereuse proposée par le texte de norme nécessite deux types de données d'entrée en fonction de leur origine :
- Les données dépendant de l'élément du sous-système (repérées 1* dans le *Tableau III*). Elles doivent être fournies par le constructeur de l'élément du sous-système ou calculées par le concepteur du SRECS sur la base des données fournies.
- Les données dépendant des spécifications de la SRCF et des choix de conception du sous-système (repérées 2* dans le *Tableau III*). Elles doivent être déterminées par le concepteur du SRECS.

Pour compléter les informations contenues dans le Tableau III et aider le concepteur dans la détermination des différentes valeurs d'entrée de ce calcul, la norme fournit deux outils permettant d'estimer les valeurs de SFF et ß.

Estimation de la proportion de défaillances en sécurité – SFF

Pour estimer la SFF, la norme propose de réaliser une analyse (arbre de panne, analyse des modes de défaillance et de leurs effets) de chaque sous-système. La dangerosité des défaillances, dépendant du SRECS et des SRCF, devra être déterminée. Ensuite, la probabilité d'occurrence de chacune des défaillances devra être déduite des différentes sources accessibles (données constructeur, retour d'expérience, annexe D de la norme, etc.). Toute défaillance non prise en compte lors de cette analyse devra être justifiée.

La SFF doit être calculée sur la base de la formule suivante :

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$

où λ_S est le taux de défaillances en sécurité, λ_D le taux de défaillances dangereuses et λ_{DD} est le taux de défaillances dangereuses qui est détecté par les fonctions de diagnostic.

Estimation de la sensibilité aux défaillances de cause commune – ß

Dans son annexe F, la norme propose une approche simple pour l'estimation des CCF.
Elle s'appuie sur un tableau[11] dans lequel un score est associé à différents critères d'estimation, en fonction de leur efficacité. Il restera au concepteur à sommer les scores correspondant aux différents critères qu'il a retenu pour la conception de son sous-système puis de déterminer, sur la base du *Tableau IV*, la valeur de ß à retenir pour le calcul de probabilité de défaillance dangereuse.

▣ Le calcul de la probabilité de défaillance dangereuse du sous-système

Le *Tableau V* présente les formules de calcul simplifié de la probabilité de défaillance dangereuse en fonction de l'architecture du sous-système. Les paramètres et les mesures accessibles au concepteur du SRECS pour, le cas échéant, améliorer la performance de son sous-système figurent également dans ce tableau.

Calcul de la probabilité de défaillances dangereuses du sous-système – cas particulier

Dans l'hypothèse où un sous-système de faible complexité est conçu selon l'ISO 13849-1 et validé selon l'ISO 13849-2 [13], le calcul de sa probabilité de défaillances dangereuses – PFH_D – en appliquant la méthode précédente n'est pas nécessaire. La valeur seuil de la PFH_D sera alors estimée sur la base de la catégorie du sous-système (des caractéristiques qui en découlent : tolérance aux anomalies et couverture de diagnostic du sous-système) et déduite directement de la norme EN 62061 *(cf. Tableau VI)*.

Si la valeur de PFH_D déduite de la norme n'est pas compatible avec le SIL requis pour le sous-système, il faudra

[10] *La norme n'exclut pas d'autres types d'architecture ; par contre elle ne les traite pas. Elle renvoie en effet à la norme NF EN 61508 pour les calculs de probabilité de défaillance dangereuse et les contraintes architecturales.*

[11] *Tableau F.1 de l'annexe F non reproduit ici.*

TABLEAU III

Données d'entrée pour le calcul de la probabilité de défaillance dangereuse du sous-système

données d'entrée pour le calcul des PFHD		Commentaires	Origine des données	
			1*	2*
λ	Taux de défaillance par heure de l'élément de sous-système	λ =1/MTTF		
MTTF	Temps moyen de fonctionnement avant une défaillance de l'élément	MTTF = 1/ λ		
B10	Nombre de cycles après lequel 10 % des éléments en test sont défaillants	Pour les composants électromécaniques : λ = 0,1 x C/B10		
λ_{De}	Taux de défaillances dangereuses par heure de l'élément de sous-système	λDe = λ x DFF		
DFF	Proportion de défaillances dangereuses de l'élément de sous-système	DFF= 1 – SFF Pour estimer ces valeurs pour un composant donné il faut connaître : - la nature des défaillances dangereuses de l'élément dans le sous-système (1*), - la proportion, par nature des défaillances, sur l'ensemble des défaillances possibles pour l'élément du sous-système (2*).		
SFF	Proportion de défaillances en sécurité de l'élément de sous-système			
T1	Plus petite valeur entre : - la durée de vie de l'élément de sous-système (2*), - l'intervalle de test périodique (1*).			
T2	Intervalle de test périodique			
C	Nombre d'activations de l'élément de sous-système par heure			
β	Susceptibilité du sous-système aux défaillances de causes communes – CCF	La norme propose dans son annexe F, une méthodologie simplifiée pour déterminer ce paramètre (valeur comprise entre 0 et 1) en fonction des choix retenus par le concepteur du SRECS.		
Modèle d'architecture	A, B, C ou D	Les formules de calcul de λD du sous-système dépendent du modèle d'architecture retenu par le concepteur.		

1* : fournies par le constructeur de l'élément
2* : dépendant des choix de conception du sous-système

TABLEAU IV

Estimation du facteur de CCF (ß) – D'après le tableau F.2 de la norme NF EN 62061

Score global	Facteur de défaillance et de cause commune (ß)
< 35	10 % (0,1)
35 - 65	5 % (0,05)
65 - 85	2 % (0,02)
85 - 100	1 % (0,01)

renoncer au sous-système en question pour traiter la SRCF spécifiée et avoir recours à un sous-système de catégorie supérieure.

Vérification de la probabilité de défaillances dangereuses du sous-système

Au terme de cette estimation, que ce soit dans le cas général ou le cas particulier, la valeur de la probabilité de défaillance dangereuse par heure du sous-système doit être compatible avec le SIL requis. Dans ce cas, la démarche de conception pourra se poursuivre en vérifiant la compatibilité du sous-système avec les contraintes architecturales. En cas de probabilité de défaillance dangereuse non compatible avec le SIL requis, le concepteur devra intervenir sur les choix de conception ou de matériel qui lui sont offerts pour modifier son sous-système et recommencer cette étape de calcul.

Contraintes architecturales pour le sous-système

La norme NF EN 62061 propose deux approches pour vérifier que le sous-système satisfait aux contraintes architecturales, selon qu'il réponde ou non à une catégorie selon l'ISO 13849-1. La dernière possibilité est considérée par la norme comme étant le cas général..

Cas général

Le *Tableau VII* résume les prescriptions de la norme EN 62061 et définit le SIL maximum relatif aux contraintes architecturales auquel peut prétendre un sous-système – et donc par voie de conséquence le SIL maximal de la SRCF qui le mettra en œuvre – en fonction de :

- la tolérance aux anomalies du sous-système,
- la proportion de défaillance en sécurité (SFF) résultante du test de diagnostic.

Cas particulier

Lorsqu'un sous-système est conçu selon l'ISO 13849-1 et validé selon l'ISO 13849-2, le *Tableau VIII* s'applique. Il résume les prescriptions de la norme EN 62061 et définit le SIL maximum relatif aux contraintes architecturales auquel peut prétendre un sous-système – et donc par voie de conséquence le SIL maximal de la SRCF qui le mettra en œuvre – en fonction de :

- la catégorie du sous-système,
- la proportion de défaillance en sécurité (SFF) résultant du test de diagnostic.

Assemblage des éléments de sous-systèmes

C'est la phase de réalisation du sous-système proprement dite.

L'assemblage des différents éléments doit se faire conformément aux spécifications et aux informations fournies avec les éléments de sous-système. La conformité du fonctionnement du sous-système réalisé doit être vérifiée par rapport à ses spécifications.

Détermination du SIL atteint par le sous-système

C'est la phase finale de vérification du niveau d'intégrité de sécurité que peut atteindre le sous-système conçu.

La détermination du SIL atteint par le sous-système, permettant de vérifier qu'il répond aux SIL requis, doit prendre en compte trois objectifs:

TABLEAU V

Formules du calcul de la probabilité de défaillance dangereuse du sous-système en fonction du modèle d'architecture retenu

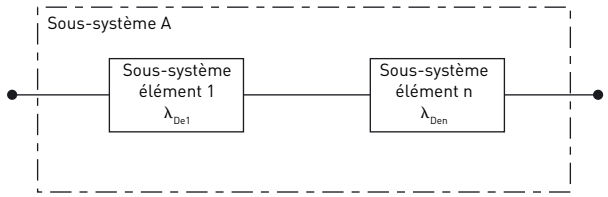
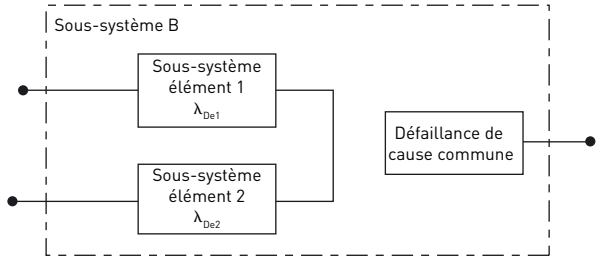
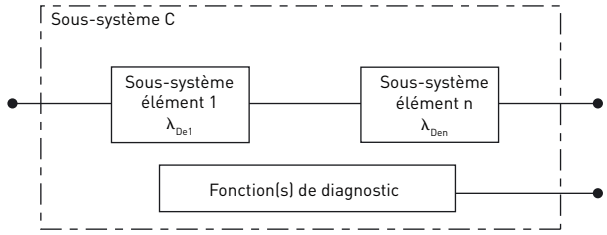
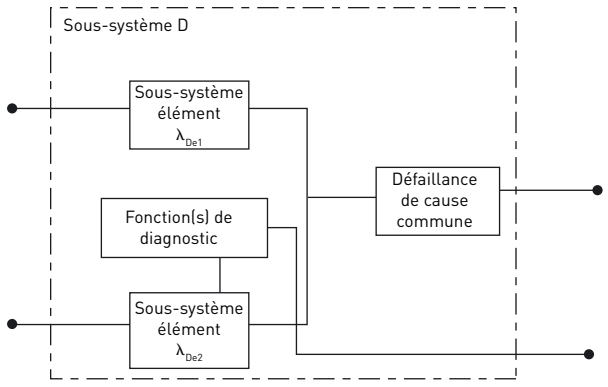
Modèle d'architecture	Représentation schématique Formules	Choix accessibles au concepteur pour améliorer le SIL du sous-système
A : Série sans fonction de diagnostic Tolérance aux anomalies : 0	 $\lambda_{DssA} = \lambda_{De1} + ... + \lambda_{DeN}$ $PFH_{DssA} = \lambda_{DssA} \times 1$ heure Paramètres accessibles au concepteur du SRECS : λ_{De}	• choix de matériel - plus fiable, - dont la proportion de défaillances dangereuses soit plus faible.
B : Parallèle sans fonction de diagnostic Tolérance aux anomalies : 1	 $\lambda_{DssB} = (1 - ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2}) / 2$ $PFH_{DssB} = \lambda_{DssB} \times 1$ heure Paramètres accessibles au concepteur du SRECS : λ_{De}, β, T_1	• choix de matériel - plus fiable, - dont la durée de vie est supérieure, - dont la proportion de défaillances dangereuses soit plus faible. • amélioration de l'immunité du sous-système aux défaillances de cause commune.
C : Série avec une fonction de diagnostic Tolérance aux anomalies : 0	 $\lambda_{DssC} = \lambda_{De1} (1 - DC_1) + ... + \lambda_{Den} (1 - DC_n)$ $PFH_{DssC} = \lambda_{DssC} \times 1$ heure Paramètres accessibles au concepteur du SRECS : λ_{De}, DC	• choix de matériel - plus fiable, - dont la proportion de défaillances dangereuses soit plus faible. • amélioration du taux de couverture des tests de diagnostic spécifiés pour chacun des éléments du sous-système.
D : Parallèle avec fonction de diagnostic Tolérance aux anomalies : 1	 $\lambda_{DssD} = (1 - ß)^2 \times \{ [\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2)] \times T_2/2 + [\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2)] \times T_1/2 \} + ß \times (\lambda_{De1} + \lambda_{De2})/2$ $PFH_{DssD} = \lambda_{DssD} \times 1$ heure Paramètres accessibles au concepteur du SRECS : λ_{De}, β, T_1, DC, T_2	• choix de matériel - plus fiable, - dont la durée de vie est supérieure, - dont la proportion de défaillances dangereuses soit plus faible. • amélioration de l'immunité du sous-système aux défaillances de cause commune. • amélioration du taux de couverture et la fréquence d'exécution des tests de diagnostic spécifiés pour chacun des éléments du sous-système.

TABLEAU VI

Correspondance entre Catégories - ISO 13849-1 - et valeur seuil de PFHD D'après le tableau 7 de NF EN 62061

Catégorie selon ISO 13849-1	Valeur minimale de PFHD pouvant être revendiquée par le sous-système
B	Insuffisante même pour réaliser le niveau SIL1.
1	A indiquer par le fournisseur ou utiliser des données génériques.
2	$\geq 10^{-6}$
3	$\geq 2 \times 10^{-7}$
4	$\geq 3 \times 10^{-8}$

Encadré 2

Tolérance aux anomalies

Le calcul de la probabilité de défaillances dangereuses ou la prise en compte des contraintes architecturales pour le sous-système repose sur la notion de tolérance aux anomalies (ou aux fautes) matérielles, caractéristique représentant le nombre d'anomalies tolérées par le sous-système pour continuer à remplir sa fonction, la SRCF dans le cas qui nous occupe. La tolérance aux anomalies dépend de l'architecture du sous-système.

Tolérance aux anomalies	Type d'architecture matérielle	Nombre d'anomalies conduisant à la perte de la fonction de sécurité
0	canal unique	1
1	Redondance double canal	2
2	Redondance triple canal	3
n	Redondance n+1 canal	n+1

TABLEAU VII

SIL maximal pouvant être revendiqué par le sous-système d'après le tableau 5 de la norme NF EN 62061

Proportion de défaillances en sécurité	Tolérance aux anomalies du matériel		
	0	1	2
< 60 %	Non autorisé [12]	SIL1	SIL2
60 % - < 90 %	SIL1	SIL2	SIL3
90 % - < 99 %	SIL2	SIL3	SIL3
≥ 99 %	SIL3	SIL3	SIL3

TABLEAU VIII

SIL maximal pouvant être revendiqué par le sous-système - Tableau 6 de NF EN 62061

Catégorie selon ISO 13849-1	SIL maximal pouvant être revendiqué par le sous-système
B et 1	Non autorisé
2	SIL1
3	SIL1 si SFF < 60%
	SIL2 si SFF 60% - 90%
4	SIL3

- le SIL maximal qui peut être atteint par le sous-système – SIL_{Cl} – déterminé par ses contraintes architecturales, est compatible avec le SIL requis,
- le SIL maximal qui peut être atteint par le sous-système – SIL_{Cl} – dû à l'intégrité systématique, est compatible avec le SIL requis,
- la probabilité de défaillances dangereuses du matériel, est compatible avec le SIL requis pour le sous-système ainsi qu'avec la probabilité de défaillances dangereuses du SRECS.

Si le SIL requis ne peut pas être atteint par le sous-système en l'état, il conviendra de modifier un ou plusieurs des paramètres évoqués ci-dessus et de reprendre le processus de réalisation du sous-système.

Réalisation des fonctions de diagnostic prescrites

Les fonctions de diagnostic nécessaires à ce que les sous-systèmes puissent atteindre le SIL requis ont été spécifiées lors de la conception des sous-systèmes. Elles doivent maintenant être implémentées dans le SRECS conformément à la norme NF EN 62061.

Si ces fonctions dépendent exclusivement du logiciel du SRECS, elles devront figurer dans la spécification du logiciel.

La norme prévoit que les fonctions de diagnostic, fonctions séparées des SRCF, puissent être réalisées par :

- le même sous-système qui requiert des diagnostics ou
- d'autres sous-systèmes du SRECS ou
- des sous-systèmes du SRECS n'effectuant pas la SRCF.

Elle énumère ensuite [13] un certain nombre de spécifications pour leur réalisation, concernant en particulier leur intégrité de sécurité :

- l'intégrité de sécurité systématique doit être identique à celle spécifiée pour la SRCF correspondante ;
- la probabilité de défaillance aléatoire du matérielle
  - doit être identique à celle spécifiée pour la SRCF correspondante, ou
  - l'effectivité de la fonction de diagnostic doit être vérifiée à une période

[12] *Pour les exceptions voir le tableau 5 de EN 62061.*

maximale égale à dix fois celle de la fonction de diagnostic du sous-système correspondant ;

- les contraintes architecturales du sous-système correspondant ne s'appliquent pas.

Détermination du SIL atteint par le SRECS pour chaque SRCF

C'est la phase finale de vérification du niveau d'intégrité de sécurité du SRECS conçu.

Chacun des sous-systèmes constituant le SRECS ayant été soit choisi soit réalisé, il faut vérifier que ces éléments répondent effectivement aux différentes spécifications du SRECS et des SRCF et qu'ils prennent en compte les trois objectifs à atteindre :

- le SIL maximal qui peut être atteint par le SRECS déterminé par le plus petit des SIL_{Cl} relatif aux contraintes architecturales de chacun des sous-systèmes mis en œuvre pour la réalisation de la SRCF, est compatible avec le SIL requis pour la SRCF,
- le SIL maximal qui peut être atteint par le SRECS déterminé par le plus petit des SIL_{Cl} relatif à l'intégrité de sécurité systématique de chacun des sous-systèmes mis en œuvre pour la réalisation de la SRCF, est compatible avec le SIL requis pour la SRCF,
- la probabilité de défaillances dangereuses du matériel pour le SRECS, résultant du calcul de la somme des PFHD des sous-systèmes mis en œuvre pour la réalisation de la SRCF, est inférieure à la PFHD requise pour la SRCF.

Cette vérification devra être effectuée pour toutes les SRCF prise en charge par le SRECS.

Réalisation matérielle du SRECS conçu

C'est la phase de réalisation du SRECS proprement dite. L'assemblage des différents sous-systèmes doit se faire conformément aux informations fournies avec les sous-systèmes et conformément aux prescriptions pour l'intégrité de sécurité systématique.

Spécification des exigences de sécurité du logiciel - conception et développement du logiciel

Contrairement à ce que pourrait laisser à penser la structure de la norme NF EN 62061, le travail de spécification du logiciel s'effectue tout au long de la réalisation du SRECS et de ses différents sous-systèmes. En effet, cette spécification doit être complétée et enrichie en permanence pour prendre en compte, non seulement les besoins fonctionnels des SRCF, mais également les fonctions de diagnostic, etc. dont la nécessité est apparue pour garantir le SIL requis pour les sous-systèmes.

Les mesures préconisées par la norme s'appliquent, que le logiciel soit situé au niveau du SRECS ou d'un quelconque de ses sous-systèmes. Les prescriptions de la norme couvrent l'ensemble des aspects du développement du logiciel applicatif et relèvent du génie logiciel classique.

Ne posant pas de difficultés techniques particulières, elles ne seront pas détaillées ici [14].

La norme propose, dans son annexe C, un « Guide pour la conception et le développement de logiciel intégré » (logiciel embarqué ou logiciel système) reprenant les prescriptions de la norme NF EN 61508-3. Cette partie de la norme NF EN 62061 concerne uniquement le concepteur qui développerait un sous-système autour d'un composant logique complexe (microprocesseur, microcontrôleur, etc.). Or, la norme NF EN 62061 précise par ailleurs qu'un sous-système mettant en œuvre des composants complexes doit satisfaire au prescriptions de la norme NF EN 61508 parties 2 et 3. En conséquence, ces derniers référentiels devront être préférés pour la conception d'un tel sous-système et de son logiciel intégré.

Intégration et test du SRECS

L'intégration du logiciel d'application relatif à la sécurité dans le SRECS doit comprendre les tests qui sont spécifiés lors de la phase de conception afin de vérifier la compatibilité entre le logiciel et le matériel et la satisfaction des prescriptions fonctionnelles et de sécurité. La norme propose également des tests pour déterminer l'intégrité de sécurité systématique, comprenant des essais de compatibilité électromagnétique, lors de l'intégration d'un SRECS.

INSTALLATION DU SRECS

L'installation du SRECS sur la machine devra permettre de s'assurer qu'il est approprié à l'usage prévu et qu'il est prêt pour la validation.

DOCUMENTATION ASSOCIEE AU SRECS

Un certain nombre de préconisations sont formulées dans le texte de la norme NF EN 62061 concernant la documentation qui doit accompagner le SRECS. Ces préconisations viennent compléter les exigences listées tout au long du texte.

La documentation devra inclure toutes les informations nécessaires à l'installation, l'utilisation et l'entretien du SRECS.

En plus de son caractère non facultatif, elle devra :

- être précise et concise,
- être facile à comprendre par les personnes ayant à l'utiliser,
- s'adapter aux besoins pour lesquels elle est prévue,
- être accessible et actualisable.

VALIDATION DU SRECS

La validation du SRECS doit être effectuée conformément au plan préparé dans le cadre du plan de sécurité fonctionnelle. En particulier, chaque SRCF spécifiée ainsi que toutes les procédures d'exploitation et d'entretien du SRECS doivent être validées par test et/ou par analyse.

Pour ce faire, la norme spécifie les exigences pour la procédure de validation à appliquer au SRECS qui « *comprend l'examen et l'essai du SRECS mis en service afin de s'assurer qu'il réalise les exigences établies dans la spécification des exigences de sécurité* ».

La norme liste par ailleurs un certain nombre de tests à effectuer pour valider l'intégrité de sécurité systématique comme, par exemple, des essais de compatibilité électromagnétique.

MODIFICATION DU SRECS

Le dernier chapitre de la norme spécifie les procédures à mettre en œuvre lors de modifications à appliquer au SRECS en cours de conception, intégration et validation. Le recours à ces mesures est essentiel pour assurer la garantie du respect des différentes spécifications établies à toutes les étapes de la conception du SRECS.

[13] *§ 6.8 de la norme NF EN 62061*

Ne posant pas de difficultés particulières, ces mesures ne seront pas détaillées ici.

CONCLUSION

La norme NF EN 62061 est difficile à lire en raison du sujet traité. De plus, si pour une grande partie du texte les activités réelles de développement du SRECS suivent le déroulement du texte, ce n'est pas le cas pour ce qui concerne l'activité principale du développement : la conception des sous-systèmes.

Ces réserves mises à part et moyennant les quelques informations complémentaires que nous avons tenté de transmettre dans cet article, la méthode préconisée par NF EN 62061 est applicable, sans de trop grandes difficultés. En outre, la norme fournit les outils qui permettront de conduire le développement d'un SRECS dans un cadre maîtrisé, où les différents choix techniques pourront être tracés et justifiés, ce cadre étant primordial pour la garantie de la performance de sécurité finale du SRECS.

Deux règles importantes faciliteront l'usage de la norme par les concepteurs :

- en rester toujours à une application « à la lettre » du texte, en en limitant les interprétations trop souvent préjudiciables risquant de compliquer inutilement la compréhension d'un texte déjà ardu ;
- toujours avoir une vue d'ensemble sur la partie en cours en ayant une bonne connaissance :
  - de l'ensemble de la démarche proposée par la norme,
  - des différentes alternatives envisageables pour le développement du SRECS,
  - des composants et des solutions techniques disponibles sur le marché.

À ce prix, l'objectif de concevoir un SRECS satisfaisant aux besoins de sécurité exprimés est accessible. Sans doute pas aisément à la première tentative, mais l'expérience montre que l'application de cette norme permet de traiter des cas complexes, dans un cadre maîtrisé, et sans forcément aboutir à des solutions techniques abstruses. Pour peu bien sûr que les informations nécessaires au développement du SRECS et les données d'entrée des différents calculs soient disponibles avec les composants retenus par les concepteurs.

BIBLIOGRAPHIE

[1] NF EN 62061 – Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité. Juillet 2005, 106 p.

[2] Directive 98/37/CE du Parlement Européen et du Conseil du 22 juin 1998 concernant le rapprochement des législations des États membres relatives aux machines

[3] NF EN 954-1. Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1 : principes généraux de conception. Février 1997, 39 p.

[4] NF EN ISO 13849-1. Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1 : principes généraux de conception. Février 2007, 102 p.

[5] NF EN 61508 parties 1 à 7. Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité. Mars 2002, 439 p.

[6] NF EN 60204-1. Sécurité des machines - Équipement électrique des machines - Partie 1 : règles générales ; Septembre 2006, 130 p.

[7] Systèmes de commande. Quelles normes pour leur conception ? Fiche pratique de sécurité ED 120, 2007, INRS.

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

[9] PR NF EN ISO 14121-1 : Sécurité des machines - Appréciation du risque - Partie 1 : principes. Décembre 2005, 45 p.

[10] Liste de contrôle. Phénomènes dangereux mécaniques liés aux machines. réf. 67113.f., Caisse nationale suisse d'assurance en cas d'accidents (SUVA), 2005, 5 p.

[11] Sécurité des machines : phénomènes dangereux, situations dangereuses, événements dangereux, dommages. DC 900-337-1, 2006, CSST.

[12] NF EN 61000-6-2 : Compatibilité électromagnétique (CEM) - Partie 6-2 : normes génériques - Immunité pour les environnements industriels. Février 2002, 17 p.

[13] NF EN ISO 13849-2. Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 2 : validation. Janvier 2004, 56 p.

[14] P. LAMY - Utilisation des automates programmables industriels dédiés à la sécurité. Guide pour le développement du logiciel applicatif – INRS, Hygiène et sécurité au travail - Cahiers de notes documentaires, n°197, 2004.