Limites d'application de la norme de sécurité fonctionnelle CEI 61508 dans le cadre d'un projet complexe

Jean-Michel Dranguet, Benjamin Joguet

Limites d'application de la norme de sécurité fonctionnelle CEI 61508 dans le cadre d'un projet complexe

Application limits of functional safety standard IEC 61508 in a complex project

Jean Michel DRANGUET
INERIS
Parc Technologique Alata
BP 2 – 60550 Verneuil-en-Halatte

Benjamin JOGUET
DCNS
BP 30
16600 Ruelle sur Touvre

Résumé

La norme de sécurité fonctionnelle CEI 61508 est la norme de référence pour le développement de fonctions de sécurité instrumentées. Celle-ci ne fait pas de distinction entre des fonctions de sécurité simples à mettre en œuvre et celles réalisées pour des projets complexes, constituées de multiples lots et fournisseurs. En absence de déclinaison sectorielle la norme peut être appliquée directement. Dans ce cas, l'application de la norme peut faire l'objet d'adaptations ou interprétations en fonction du contexte. Il est donc nécessaire d'adopter une démarche spécifique pour contourner les difficultés de son application tout en gardant l'esprit de la norme.

Summary

The functional safety Standard IEC 61508 is the recognized standard used for safety instrumented function design. This standard does not make the distinction between simple safety functions and functions defined in complex projects built using multiple components and different providers. In the lack of sector version of the standard, IEC 61508 can be directly applied. In this case, the application of the standard is subject to adaptations or interpretations according to the context. It is necessary to adopt a specific approach to bypass the difficulties of application by keeping in head the spirit of the standard.

1 La norme CEI 61508

La norme CEI 61508 traite de la sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables pour exécuter des fonctions instrumentées liées à la sécurité dans la plupart des secteurs industriels. Cette norme dont le fondement est basé sur la gestion de la sécurité fonctionnelle repose sur un cycle de vie regroupant toutes les étapes allant de l'identification des dangers, à la réalisation du système jusqu'à son retrait.

Cette norme volumineuse donne beaucoup d'indications concernant les méthodes aussi bien matérielles que logicielles pour atteindre le niveau de sécurité requis. Un des points clefs de cette norme est l'approche en termes de quantification des défaillances correspondant aux quatre niveaux d'intégrité de sécurité (SIL).
Ce cycle de vie est constitué de 16 étapes allant de l'étape de conception à celui de ma mise hors service et repose sur deux pré-requis indispensables :

- Exigences de gestion documentaire,
- Exigences de sécurité fonctionnelle

Le cycle de vie comprend principalement les activités:

- d'identification des dangers et d'analyse de risques,
- d'allocation des exigences de sécurité,
- de planification globale des activités de conception, de validation, de maintenance,
- de réalisation du système.

En résumé, la norme définit un ensemble d'exigences permettant la maîtrise des systèmes de sécurité par :

- La réduction des défaillances systématiques qui sont traitées par des concepts de gestion et de développement, ainsi que d'organisation durant toute la vie du système.
- La réduction des défaillances aléatoires du matériel par la détermination de la probabilité moyenne de défaillance dangereuse, et des contraintes architecturales

Plus précisément, les attendus en termes d'évaluation :

- Pour la partie de réduction de défaillance systématique consiste à définir un ensemble cohérent de tâches de spécifications et de vérifications dans le cycle de développement.. Ces exigences se traduisent donc par l'émission de documents attestant d'une organisation rigoureuse dans le développement.
- Pour la partie quantitative consiste à identifier les défaillances dangereuses qui empêchent une action de sécurité de se réaliser ou diminuent sa probabilité de réalisation. Pour une application de sécurité, les défaillances sûres qui ont tendance à provoquer les actions en sécurité seront aussi un critère d'évaluation. Pour la partie matérielle, l'évaluation de ces défaillances est à mettre en relation avec la tolérance possible aux anomalies grâce a une architecture redondante, par exemple. En résumé, plus un système sera tolérant à la défaillance matérielle en favorisant des déclenchements en sécurité, mieux il sera considéré pour remplir des fonctions de sécurité.

2 Méthodologie d'évaluation selon de la norme IEC 61508

2.1 Démarche de l'évaluation

Une évaluation par rapport à la norme CEI 61508 couvre un ensemble d'activités : analyse de danger, spécification des fonctions de sécurité, conception de matériel électronique, conception du logiciel, détermination des probabilités de défaillances.

Suite à l'analyse de risque et à la définition des fonctions de sécurité, il s'agit pour le concepteur de réaliser ces fonctions de telle façon à remplir les exigences de la norme. Il est très important d'avoir une vision globale des fonctions de sécurité pour prétendre à définir un système qui devra répondre à l'ensemble de ses exigences fonctionnelles.

L'analyse fonctionnelle effectuée lors d'une évaluation doit permettre de comprendre cette vision globale et de cerner les limitations notamment en termes de tolérance à une défaillance simple et les mesures de diagnostics associés. C'est un point très important car toute l'étude permettant de statuer sur sa conformité repose sur la compréhension de cette analyse. Cette vision globale est le fil conducteur de l'étude. En cas de modifications, l'évaluation peut être caduque.

Une évaluation de l'architecture doit être menée afin d'estimer la faisabilité. Différents critères sont à prendre en compte et concernent :

- Les objectifs de réduction de non fonctionnement des fonctions de sécurité en termes de sécurité,
- Les objectifs de comportement sur anomalie afin de garantir une disponibilité quitte à travailler dans des modes dégradés de sécurité.

Ces deux objectifs peuvent sembler contradictoires et ils sont souvent une affaire de compromis. Il est difficile de définir des règles générales, c'est souvent la complexité du process industriel à garantir qui impose ces exigences.

Une fois le concept d'architecture définie, il est important de connaître ses limites de fonctionnement par une évaluation dysfonctionnelle du système. L'architecture est évidemment une première étape dans cette connaissance, elle doit être complétée par la mise en place d'une politique de détections de défauts et d'une définition de toutes les exigences de comportement.

Ces deux étapes permettent de cerner clairement la maîtrise dysfonctionelle d'un système.
L'étape de conception du logiciel doit permettre de renforcer le niveau de confiance dans le développement. Les étapes de vérifications et de validations parachèvent le niveau de confiance que l'on peut estimer dans la maitrise du système.

La dernière étape de quantification qui nécessite une connaissance des différents éléments du système doit faire le lien avec toutes les dispositions précédentes pour évaluer les niveaux de probabilités atteignables.

2.2 Utilisation de la norme IEC 61508 par un certificateur

Dans le cadre d'une évaluation faite par un certificateur, les applications des normes CEI 61508/CEI 61511 sont possibles dans les cas suivants :

1. Vision complète du cycle de vie
2. Réalisation d'une partie du cycle de vie (partie réalisation)

Le premier cas est très rare. En effet dans le cadre de produits manufacturés, les constructeurs ne sont que rarement des acteurs dans la détermination des niveaux de sécurité de fonction car ils ne participent pas à la définition desdites fonctions. Leur préoccupation est donc de fournir à des clients potentiels des éléments qui pourront s'intégrer dans des fonctions de sécurité. Clairement, dans ce schéma, la responsabilité du niveau de sécurité pour une fonction de sécurité ne peut être de la responsabilité du manufacturier.

Le deuxième cas est le plus fréquent et correspond à la mise sur le marché de produits certifiés ou évalués par rapport à une exigence de niveau SIL. Dans ce cas, l'évaluation ou certification consiste à évaluer un produit dans une configuration définie.
Pour un organisme certificateur, les évaluations au titre de la CEI 61508 / CEI 61511 n'existent que par la volonté des manufacturiers qui cherchent à promouvoir leurs produits sur le marché. Les manufacturiers sont demandeurs de ce type de certification car cela leur permet de proposer des dispositifs utilisables par de nombreux clients. Leur proposition est plus orientée vers les produits pour lesquels la demande est la plus forte et la configuration est la plus standard. Certaines demandes spécifiques d'utilisateurs ne sont donc pas forcément intégrées dans leur processus de conception.

2.3 Utilisation de la norme IEC 61508 par un utilisateur/intégrateur

Dans le cas de domaines industriels non soumis à des contraintes normatives particulières, la norme 61508 permet des apports structurants :

- Pour l'intégration de systèmes complexes, l'utilisation de cette norme permet d'uniformiser le référentiel d'exigences pour des sous-systèmes déjà existants ou en développement spécifique.
- L'utilisation de la norme 61508, connue dans le monde entier, permet d'apporter une garantie supplémentaire aux clients, qui n'ont pas à s'approprier des référentiels spécifiques.
- Les gains de temps et de coût générés par l'intégration de COTS déjà certifiés sont intéressants

Ces avantages ne vont pas sans inconvénients, qui sont précisés dans les chapitres suivants.

3 Le découpage en lots et la reconsolidation

L'évaluation d'une fonction de sécurité au sens de la CEI 61508 suppose une évaluation complète incluant la partie capteur, traitement et l'élément final. Il faut donc maîtriser une chaîne complète pour se prononcer. Dans la mesure où la réalisation peut être partagée entre différents partenaires, la réalisation finale est donc faite par lots. Par exemple, à un partenaire numéro 1 il est confié la partie associant le traitement et l'actionneur. Un autre partenaire numéro 2 est choisi pour réaliser la partie des capteurs. Il en résulte que pour l'entité partenaire numéro 1, les informations disponibles dans certains cas sont résumées à l'expression d'un cahier des charges définissant un niveau d'intégrité requis.

Pour l'entité Numéro 1, le scope de l'évaluation se limite donc à une portion de chaîne de sécurité. Il est dans ces conditions difficile d'aborder tous les concepts de la norme dont l'application seulement partielle n'est pas "naturelle". Pour un évaluateur, la difficulté est du même ordre. Comment se positionner sur une partie d'une chaîne de sécurité sans maîtriser tous ses ensembles ?

Ce chapitre aborde donc cette problématique sous l'angle de la consolidation de la Safe Failure Fraction (SFF), de l'utilisation dite des "mécanos de SIL" puis des COTS.

3.1 La consolidation de la SFF

Une restriction majeure de la norme réside dans le concept **« FAIL SAFE »** mis en avant pour les systèmes de sécurité qui doivent remplir les fonctions de sécurité assignées. Par défaut, la norme privilégie une position de sécurité qui consiste à passiver les sorties. La position de sécurité est donc atteinte lors de la désactivation par perte d'énergie.

La maîtrise des défaillances aléatoires d'un système repose sur la connaissance précise des défaillances des composants. Cela suppose de bien définir la mission du système et de définir les événements redoutés. A partir d'une bonne connaissance du système, et l'identification des défaillances qui sont :

- Les dangereuses sûres qui mettent le système dans une position de sécurité définie
- Les défaillances dangereuses non détectées qui empêchent la fonction de sécurité de se réaliser
- Les défaillances dangereuses détectées qui impliquent que des mesures soit prises

Pour la plupart des quantifications faites selon la CEI 61508, l'évaluation de ces défaillances est réalisée sur des analyses prévisionnelles de fiabilité. Entre ces évaluations prévisionnelles et un véritable retour d'expérience, il peut exister une grande disparité car il est difficile d'imaginer les problèmes rencontrés en utilisation.

A partir de cette évaluation des défaillances, et si le critère **« FAIL SAFE »** est applicable, il est nécessaire d'estimer la proportion des défaillances en sécurité (**Safety Failure Fraction).** Ce critère est adapté en fonction des deux technologies électroniques identifiées de type A (électronique simple) et B (électronique complexe programmable).

Cette distinction a été établie pour privilégier les conceptions de type éprouvées par l'usage. Les progrès technologiques dans l'industrie électronique sont tels qu'il paraît difficile d'imaginer de nouveaux développements sans faire appel à des nouveaux composants sans véritable retour d'expérience. Par définition, la technologie de type A est donc réservée à la partie des composants électroniques dont la création date au mieux des années 70. A partir de l'avènement de technologies basées sur microprocesseur on peut considérer que l'électronique est du type B.

A partir de cette différenciation la norme établit des contraintes architecturales qui sont à respecter pour les différents sous systèmes qui composent le système de sécurité.

Safety Failure Fraction (SFF)	**Tolérance aux erreurs matérielles**		
(Proportion de défaillances en sécurité)	**0**	**1**	**2**
SFF< 60 %	SIL1	SIL2	SIL3
60 % < SFF ≤ 90 %	SIL2	SIL3	SIL4
90 % < SFF ≤ 99 %	SIL3	SIL4	SIL4
SFF > 99 %	SIL3	SIL4	SIL4

Tableau 1 : Intégrité de sécurité - Contraintes d'architecture pour les systèmes de sécurité de type A

Safety Failure Fraction	**Tolérance aux erreurs matérielles**		
(Proportion de défaillances en sécurité)	**0**	**1**	**2**
SFF< 60 %	non-autorisé	SIL1	SIL2
60 % < SFF ≤ 90 %	SIL1	SIL2	SIL3
90 % < SFF ≤ 99 %	SIL2	SIL3	SIL4
SFF > 99 %	SIL3	SIL4	SIL4

Tableau 2 : Intégrité de sécurité - Contraintes d'architecture pour les systèmes de sécurité de type B

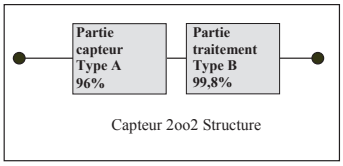

Figure 1 : Architecture capteur-traitement 2oo2

A titre d'exemple la figure ci-dessus représente la décomposition d'un capteur réalisée avec de l'électronique de traitement du signal (Ampli opérationnel, sortie courant) et la partie en charge du traitement. Les deux parties sont faits respectivement par de la technologie A et B. au sens de la CEI 61508. Les sous éléments sont conformes à l'exigence de SFF pour atteindre un niveau de SIL 3. Il est logique de considérer que le capteur est de type B car la partie programmée conditionne tout son fonctionnement.
Pour le capteur complet quel est l'impact des associations des deux parties ? D'une manière générale, les taux de défaillances de composants programmés sont meilleurs que ceux montés en interface. C'est assez logique car ils sont montés dans un environnement plus protégé que ceux en contact direct avec le monde extérieur. La partie de défaillances liées à la partie traitement est donc relativement plus faible.

Dans ces conditions, un calcul en intégrant l'ensemble des défaillances peut conduire à une réduction de la SFF de l'ensemble. Par exemple, la perte de 1 à 2 % de la SFF entraîne donc un déclassement possible du niveau de SIL si on considère l'ensemble comme de type B.

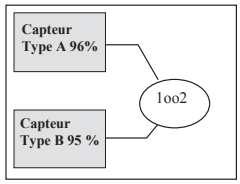

Figure 2 : Architecture capteur-traitement 1oo2

Les tableaux définis ci-dessus ne fonctionnent que pour des éléments de même type. Dans le cas de la figure n°2 et pour être conservateur, l'ensemble capteur étant composé d'au moins un capteur de type B, il est retenu que le tableau de type B est applicable. Dans ces conditions, le niveau de SIL atteignable est SIL 3. Ce niveau est celui potentiellement atteint par le seul capteur de type A. La redondance ne pourrait pas être valorisée !!

En conclusion, pour que la manipulation de ces tableaux ne puisse pas impacter les associations, il est fortement recommandé d'atteindre des SFF > 99% qui a priori serait plus favorable. Un élément de faiblesse de la SFF sur les composants de type B est à mettre en rapport à leur définition. Puisque les composants de type B sont ceux pour lesquels le retour d'expérience est insuffisant, comment est-il possible de définir une répartition qui favoriserait la sécurité ?

Evidemment plus la structure devient complexe (voir figure N°3), plus l'exercice est difficile. Si pour une fonction ne mettant en œuvre des structures simples, l'exercice est faisable, il devient très illusoire quand il est nécessaire d'associer des structures complexes.

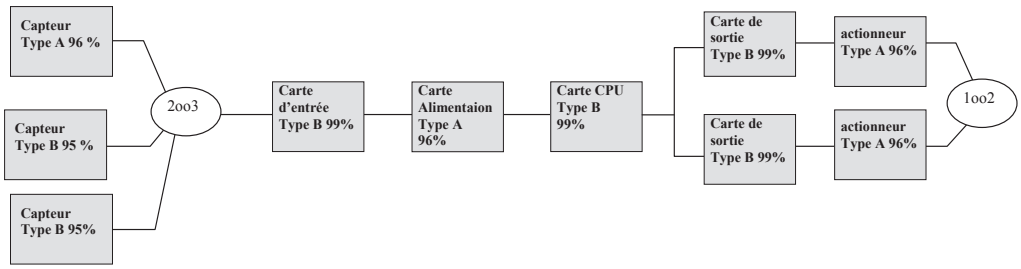

Figure 3 : Architecture plus complexe

En conclusion, dans les évaluations, un découpage d'une fonction complète de sécurité est réalisé dans les différents sous-systèmes avec une identification des sous ensembles en fonction d'une pseudo répartition en type A et Type B. Ce découpage n'offre pas plus de confiance dans l'évaluation de l'architecture et n'est qu'un artifice de présentation.
Le SFF qui a été introduit pour limiter les exagérations de la quantification n'est pas un indicateur suffisamment robuste et vérifiable. On peut tout aussi bien par des artifices de calcul trouver des valeurs de SFF favorables. En final, il n'apporte pas plus de clarté et d'une manière générale il est quasiment impossible à vérifier scientifiquement.

3.2 L'utilisation des "mécanos de SIL"

A partir d'une spécification de besoin déterminant un objectif de sécurité à atteindre, un intégrateur/utilisateur peut élaborer sa fonction de sécurité à partir de différents sous-ensembles, créant un ensemble complexe.
Les raisons sont multiples :

- Si l'objectif à atteindre est important, le système peut être décomposé en plusieurs sous-systèmes qui portent chacun des fonctions de sécurité, dont les objectifs unitaires alloués en niveau SIL peuvent ainsi être démontrés plus facilement.
- Si la technologie ne permet pas de répondre par un seul composant "SILé", l'utilisation de plusieurs composants en parallèle peut permettre de répondre à l'objectif.

Cette décomposition est permise par la première version de la norme CEI 61508 qui admet en résumé qu'un composant SIL"X" combiné en parallèle à un composant SIL"Y", quand Y est inférieur ou égal à X, donne un système SIL"X+1". Cette possibilité conduit à définir des solutions à partir de plusieurs composants "SILés", créant ainsi des "mécanos de SILs". L'Edition 2 de la norme a introduit une nouvelle notion de " capabilité systématique" qui doit limiter l'empilement successif de dispositif pour une combinaison définie d'éléments. Mais la détermination de SIL maximum atteinte pour une architecture est restée identique. La figure suivante est un exemple possible.

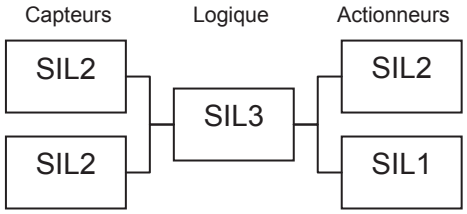

Figure 4 : Exemple de "mécano de SILs" pour une fonction SIL3

L'utilisation de tels montages induit plusieurs problèmes/questions :

- L'industrie n'admet pas certaines configurations : dans l'exemple ci-dessus, SIL2 + SIL1 ne feront pas un SIL3. Cependant ces configurations non admises ne font pas l'objet de documentations explicites.
- La consolidation des SFF pour les sous-ensembles sera compliquée (voir § ci-dessus).
- Jusqu'à quel niveau de décomposition peut-on/doit-on descendre en suivant cette logique ?

Si la connaissance des probabilités de défaillance issues d'une démarche de certification facilite le travail de l'intégrateur qui n'a donc pas le besoin de faire une étude spécifique pour chaque sous ensemble, cette approche a une limite puisque chaque sous-ensemble, s'il s'agit de COTS par exemple, peut constituer une boîte noire. Leur connaissance se limite à leur interfaçage. Il en résulte une perte de connaissance et de maîtrise sur l'ensemble de la fonction de sécurité. Cette limite est inévitable dans la mesure où il n'y a pas de développement spécifique fait par l'utilisateur.

3.3 L'utilisation des COTS

Une fois l'architecture du système définie et l'expression de besoin clairement identifiée, il est nécessaire d'exprimer clairement les spécifications fonctionnelles de chaque sous-ensemble. Cette expression de besoin peut être satisfaite soit par la sélection de composants sur étagères (COTS) et plus rarement à l'expression d'un développement spécifique.
Dans le cas de sélection de sous ensembles, plusieurs types d'équipements sont disponibles :

- Des équipements électroniques ou mécaniques de faible complexité
- Des équipements électroniques programmables (automate, capteur intelligent …) qui peuvent inclure à la fois une fourniture électronique et des ressources logicielles.

Quelque soit le type de matériel, deux types de COTS peuvent être utilisés :

- **COTS non certifiés** :
  Dans le cas de sélection de COTS non certifiés, la justification de leur utilisation réside dans le retour d'expérience. Lorsque cela est possible, il est recommandé de choisir des solutions éprouvées. L'avantage de ce type de solution est la certitude de l'adéquation de l'équipement à la fonction. Si des retours formalisés existent sur ce type de matériel, il est certain de maîtriser leur comportement.

  Bien que ces équipements n'aient pas fait l'objet de processus de certification, ils ne sont absolument pas à négliger car leur fiabilité résulte d'une vraie expérience de terrain.

  La principale raison de l'utilisation de COTS non certifiés peut être liée au volume et à la disponibilité de produits mis sur le marché. Quand la demande se résume à quelques exemplaires, il n'est pas certain qu'une démarche de certification puisse se justifier pour un manufacturier. Dans ce cas, l'utilisateur/intégrateur n'a guère le choix : c'est le marché qui impose ses conditions de choix de produits non certifiés. Cela pourra avoir comme conséquence une absence de données précises en termes de défaillances et/ou dans les restrictions d'utilisations.

- **COTS certifiés :**
  Les COTS certifiés sont constitués par tous les produits qui ont fait l'objet d'une évaluation selon la CEI 61508.On parle de produits « SILés ». L'avantage pour un manufacturier est de promouvoir des produits certifiés SIL pouvant s'intégrer dans des fonctions de sécurité. Pour l'utilisateur, cela garantit que les recommandations des normes de sécurité fonctionnelles appliquées ont été respectées pour le développement matériel et logiciel du produit. Le produit est dit "SIL capable" pour un niveau donné (1 à 4).

La certification des COTS est souvent considérée comme un gage de qualité, Cependant la documentation (voir §5) est de complétude souvent inégale et il est nécessaire de faire une analyse approfondie des certificats. Ainsi un COTS SIL3 ne pourra probablement pas être réellement utilisé dans une fonction SIL3.

3.4 En bref, comment évaluer un découpage par lots ?

Dans le cas d'une évaluation partielle incluant le traitement et l'actionneur, il n'est possible de se prononcer que jusqu'à une étape précise. Elle correspond en général à la recette du système fait lors des FAT (Factory Acceptance Test). En effet cette étape se caractérise par une vérification fonctionnelle et dysfonctionnelle à l'aide de moyens qui ont pour but de simuler l'application. Une vraie évaluation complète nécessite l'intégration complète de tous les dispositifs qui ne sont possible que lors des SAT (Site Acceptance Test).

Il existe d'autres schémas possibles d'évaluation. Par exemple, un ensemble bloc logique de sécurité incluant la partie actionneur et traitement est évalué par un premier organisme. Un deuxième organisme est chargé de faire une évaluation globale de la fonction incluant le bloc capteur et logique de sécurité avec son actionneur. Un troisième est chargé d'émettre un certificat à partir des données fournies par les deux organismes.

Le concept de « mécano de SILs » peut conduire à vouloir dissocier la construction d'une fonction de sécurité en plusieurs morceaux en séparant par exemple le matériel (hardware) et le logiciel (Software). Il est envisageable de définir une spécification pour un matériel de niveau SIL2 dans une première étape. Le logiciel peut être réalisé dans une étape ultérieure avec la même exigence de sécurité. On peut également imaginer à terme des logiciels disponibles sur étagères répondant à des niveaux de SIL définis.

Dans ce cas, les évaluations successives perdent toute notion de la globalité de la fonction de sécurité.

Le découpage par lots est donc une source d'erreurs potentielles et d'interprétation dans leur évaluation.

En final, il est absolument nécessaire de définir les contours de l'évaluation et d'émettre des restrictions de l'utilisation de cette évaluation à des recommandations d'utilisation. La validation globale ne peut être faite qu'à l'étage supérieur en charge de la validation globale.

4 Les différences d'interprétation de la norme

4.1 Limitations liées à la norme

La norme en elle même n'est pas suffisamment structurée et précise pour constituer un guide d'utilisation. Le cadre de l'évaluation de la sécurité fonctionnelle est lui même laissé à l'interprétation. Pour la phase réalisation du système, il est toléré qu'un service indépendant puisse se prononcer sur un niveau SIL3. Ce n'est qu'au niveau SIL4 qu'il est demandé qu'une organisation indépendante soit impliquée dans l'évaluation fonctionnelle. Cela signifie que l'auto certification est possible. La deuxième version de la norme 61508 a officialisé la nécessité de fournir un Manuel de sécurité permettant à l'utilisateur de connaître les limites et les recommandations à respecter.

De nombreuses exigences font appel à des prescriptions "Recommandée", "Hautement Recommandée" avec des niveaux d'applications qui peuvent être du type Obligatoire, Faible, Moyenne ou Elevée correspondant à des degrés d'efficacité. Ces degrés font référence à une échelle quantitative pour laquelle l'unanimité de compréhension reste très subjective. Ainsi une prescription "Hautement Recommandée" a souvent valeur d'obligation : l'exemple est flagrant concernant le niveau SIL4 pour le logiciel dont la quantité d'exigence hautement recommandée est telle qu'un développement logiciel SIL4 est quasiment impossible à réaliser. De facto le logiciel est totalement exclu par l'industrie dans l'implémentation d'une fonction SIL4 selon la norme 61508.

Il n'est absolument pas certain que ces prescriptions correspondent à des exigences très précises. En conséquence cela signifie qu'en fonction des évaluateurs et des intégrateurs la perception des ces exigences soit très différente.

Cela implique que les rendus de la part de fournisseurs/ intégrateurs ou évaluateurs peuvent être très différents.

4.2 Différences de perception selon la culture aux applications des normes

La présence d'annexes classées normatives ou informatives est sujette également à interprétation. Les évaluateurs de différents pays peuvent avoir une position tout à fait différente sur l'application des annexes informatives. Au sens strict de la norme, elles ne sont pas d'application obligatoire, elles sont données à titre d'information. Néanmoins en fonction des évaluateurs, ces annexes puisqu'elles sont citées dans la norme sont considérées d'application obligatoire. Entre des évaluateurs de nationalité différente, il n'est absolument pas sûr d'avoir une convergence de point de vue sur ce sujet.

D'une manière générale cela traduit aussi le fait que culturellement les approches sont différentes. Par exemple en France, d'une manière générale l'adéquation aux normes se fait généralement dans un contexte réglementaire. En Allemagne, depuis très longtemps, les industriels et les services d'évaluation travaillent ensemble en dehors de contexte réglementaire. La recherche de l'adéquation aux normes est dans la culture allemande.

Par voie de conséquence, un certificat aura une "signification" différente selon la nationalité de son organisme émetteur et celle de son utilisateur.

4.3 Contexte réglementaire / volontaire

La construction de l'Europe se fait grâce à une démarche globale qui a pour vocation l'harmonisation des pratiques des différents pays la constituant. Par exemple, la directive machines 2006/42/CE a pour vocation d'assurer la sécurité des personnes sur le lieu de travail et à réduire les risques . Tous les systèmes ou composants de sécurité qui participent à l'élaboration de fonctions de sécurité dans ce cadre d'utilisation doivent faire l'objet d'un examen réglementaire classifié "de type". La conformité de ces systèmes ou composants est examinée en fonction des différentes normes applicables. Dans certains cas, le respect aux normes dites "harmonisées" suffit théoriquement à répondre aux exigences de la directive sans examen spécifique.

Un autre exemple de directive européenne harmonisant les pratiques des différents pays est la directive liée à l'utilisation des dispositifs utilisés en ATmosphères Explosibles (ATEX). Elle s'applique à tous les produits et équipements susceptibles d'être utilisés dans des conditions d'atmosphères explosives. Ces équipements sont donc soumis à des examens réglementaires.

Les manufacturiers ont pour but de proposer des produits pour lesquels les adaptations sont mineures et ont donc visé principalement le marché couvert par ces deux directives. La certification de leurs produits fait d'abord référence au contexte d'utilisation. Dans ce cas, l'évaluation de ces produits à la CEI 61508 est presque "automatique" car la norme reprend beaucoup des concepts de détermination de mise en repli d'une machine correspondant à son arrêt.

La norme IEC 61508 non conçue dans un esprit de certification n'est rattachée à aucune réglementation particulière et n'a donc pas de cadre d'application stricte. Les examens des différents systèmes ou partie de systèmes faisant référence à la CEI 61508 peuvent donc être sujettes à interprétation. En théorie, l'accréditation des organismes délivrant des certificats est effectuée par un organisme référent. Mais pour le cas de la CEI 61508, cette accréditation couvre essentiellement le processus de certification sans prendre en compte la partie évaluation technique.

Au niveau international, il n'existe pas de schéma de certification pour la norme IEC 61508 comparable au schéma de certification IECEx (International Electrotechnical Commission Explosive) reconnu à l'international dans le domaine de l'ATEX. Celui-ci procure un moyen pour les fabricants de matériels utilisables en atmosphère explosible d'obtenir un certificat de conformité accepté dans les pays participants qui reconnaissent ce schéma de certification.

Il manque certainement au niveau de l'IEC 61508 un cadre d'évaluation technique reconnu au niveau international qui aplanirait toutes les divergences d'interprétations et d'évaluations.

5 La documentation

L'élaboration d'une fonction de sécurité ne peut se résumer à la juxtaposition de produits commercialisés, et les difficultés de mise œuvre ne sont pas à négliger. Tout d'abord, chaque élément peut constituer une boîte noire, leur connaissance se limitant à leur interfaçage comme vu précédemment. Le cœur de chaque produit est donc inconnu. La connaissance de chaque élément via une documentation précise est alors absolument nécessaire. Cette connaissance est vitale pour garder une maîtrise technique de l'ensemble de la fonction de sécurité. Comme d'une manière générale, les produits mis sur le marché ont pour vocation de cibler les applications le plus demandées, il n'est pas certain que les éléments choisis sont optimum pour la fonction de sécurité. Il est alors indispensable d'avoir accès à une information adéquate.
Il y a trois types de documentation potentiellement accessible :

- Les certificats
- Le safety manual
- Les rapports d'évaluations

Les certificats sont ceux qui sont les plus accessibles. Comme ils ne sont pas soumis à une exigence précise en terme de contenu et qu'ils font l'objet d'un document de 1 à 2 pages, les informations sont très synthétiques. D'une manière générale, il est précisé quel niveau de SIL est atteint et en théorie sous quelle structure (redondance type A ou type B). Il y a dans ce type de document peu d'informations par rapport aux consignes d'utilisation et les informations liées aux défaillances sont souvent absentes.

Pour avoir de plus amples informations, il est nécessaire d'avoir accès au manuel de sécurité s'il existe, a des rapports annexes fournis par le manufacturier ou au rapport d'évaluation qui a conduit à l'émission du certificat. Pour ce dernier rapport, il est parfois difficile de se le procurer, ce qui est paradoxal puisque c'est souvent ce document qui donnera les limites d'applications dans le cadre du certificat, car il est la propriété du manufacturier. L'organisme certificateur ne peut donc le transmettre. Il est donc nécessaire de faire la demande au manufacturier pour y accéder. Dans certains cas, l'utilisateur peut donc être dans l'obligation de rencontrer le manufacturier et l'organisme certificateur pour obtenir des informations plus précises. La mise en œuvre des différents produits peut donc être compliquée surtout en fonction de leur complexité.

Les systèmes fournit avec des suites logicielles sont des cas exemplaires. Dans certains cas, les explications et recommandations fournies sont relativement succinctes. Il peut s'avérer nécessaire de demander une prestation auprès du fournisseur pour envisager de faire un développement qui soit conforme aux recommandations de la norme.
Pour conclure, cela signifie que l'utilisation de produits certifiés n'est pas forcément un sésame de facilité dans le développement de fonctions de sécurité. L'intégrateur n'a d'autres choix que de développer en fonction des informations reçues, et finalement la conformité du développement repose sur son niveau d'expertise technique.

6 La customisation et les adaptations nécessaires

L'utilisation des COTS ou sous ensembles certifiés impose théoriquement un mode d'utilisation prévue. Comme la plupart des systèmes certifiés sont orientés dans un mode de fonctionnement particulier (notamment position de sécurité à manque), il est difficile pour un intégrateur de les agencer afin de pouvoir remplir ses propres exigences de fonctionnement.

Les nécessités d'adaptation s'imposent lorsque par exemple :

1. Les concepts d'architectures ne peuvent s'appliquer ;
2. La position de sécurité ne correspond pas à la position de sécurité à manque qui est bien souvent le cadre d'évaluation des automates de sécurité. Cela est vrai également sur les capteurs 4-20 mA pour lesquels la position de sécurité est la mise à l'état de la sortie > 20mA et que ceux-ci ne disposent pas d'alimentation suffisante.
3. Lorsque les actions nécessaires au système de sécurité ne peuvent pas se faire avec des informations dédiées à la sécurité.
4. Il ne peut y avoir de réaction automatique à des dysfonctionnements.

Les solutions envisageables pour ces adaptations sont :

1. Mettre en place une architecture spécifique afin de garantir la disponibilité de service. Dans certain cas, il faudra admettre simplement que la redondance n'est pas toujours applicable. Dans ces conditions, les critères de la Safe Failure Fraction ne sont donc plus franchement un critère de justification. Il est absolument nécessaire de développer une solution spécifique robuste qui réduira les défaillances à un niveau acceptable. C'est exactement le sens de la route 2_H de l'édition 2 de la norme IEC 61508 qui est théoriquement basée sur un retour d'expérience. En cas de nouveau développement, il sera nécessaire de l'adapter à des produits neufs.
2. Si cela est possible configurer le système pour lui définir une position différente en cas de défaillance. Il faudra s'assurer que les dispositifs ont bien envisagé cette possibilité lors de leur évaluation/certification et cerné leurs limites d'utilisation. Ce ne sera donc pas toujours facile à réaliser et demandera peut être du développement spécifique.
3. Mettre en place un contrôle de cohérence de ces informations dans la mesure du possible.
4. Ne plus favoriser une action automatique pour la fonction de sécurité, mais générer une alarme afin de transférer la responsabilité de la sécurité à un système de secours et à un opérateur.

Face à ces difficultés d'adaptation, il faudra clairement admettre que quelles que soient les solutions envisageables, la conformité aux recommandations de la norme pourra difficilement être applicable.

Par exemple, on peut toujours imaginer qu'un logiciel de surveillance d'informations non sécuritaire réponde à des exigences de développement logiciel de haut niveau (par exemple SIL3). Néanmoins pour l'application incluant l'ensemble de la chaîne, il faudra réduire le niveau global de sécurité à un niveau plus modeste du type alarming sur des contrôle/commande. En clair ce n'est pas parce qu'un logiciel est SIL3 qu'une fois intégré il est possible d'affirmer que la fonction de sécurité est du même niveau. Il est nécessaire d'inclure toutes les exigences de construction de la norme IEC 61508. On ne peut faire le raccourci un système matériel et logiciel de SIL 3 font un système de sécurité de SIL3.

Il paraît utopique de trouver dans la norme toutes les solutions techniques détaillée et précises pour chaque cas particulier. Quelles que soientt les adaptations, il sera nécessaire de respecter **«l'esprit de la norme »** à défaut de disposer sur le marché des solutions techniques développées conformément à la CEI 61508. Ces adaptations ne peuvent être réalisées qu'avec des solides compétences globales et techniques liées à la connaissance du système à sécuriser. La gestion de la sécurité fonctionnelle repose plus sur cette connaissance que sur l'application aveugle de la CEI 61508.

Au final pour l'utilisateur, la mise en place de système de sécurité doit être faite de telles façons à garantir la maîtrise technique tout en ayant une bonne connaissance de ses limites de fonctionnement.

7 Conclusions

L'évaluation de fonctions de sécurité complexes faisant appel à de multiples partenaires est un long processus qui nécessite de nombreuses adaptations. Entre les spécifications insuffisamment précises, des résultats ou attendus pas toujours exploitables, le cycle de développement n'est pas une suite d'activités idéalement planifiées et il est nécessaire de procéder de façon interactive. Bien que vérifier complètement des fonctions de sécurité soit difficile, l'évaluation ne doit pas trop limiter son champ afin de rendre son exploitation possible.

L'évaluation d'une fonction ou partie de fonction de sécurité doit permettre de cerner les limitations de performances et de comportement de la configuration étudiée. La conjonction des vérifications quantitatives et qualitatives est un exercice intéressant car il permet de juger du niveau de crédibilité de la fonction ou partie de fonction évaluée. C'est le principal enseignement à retenir de l'application de la norme IEC 61508. Les difficultés de l'application de la norme sont liées en partie à ces concepts fondamentaux. Celle-ci n'a pas été écrite dans la nécessité de fournir un service mais plutôt pour pallier l'absence de service. Certains critères sont donc sujets à controverse et pas toujours adaptés. Par exemple la séparation drastique entre système de contrôle et de sécurité implique des difficultés ainsi que l'évaluation de critères qualitatifs pas assez factuels. Les solutions techniques permettant de répondre à la philosophie de la norme ne sont pas toujours existantes ou réalistes.

Il faut donc s'adapter tout en gardant **« l'esprit de la norme ».** La philosophie de base reste inchangée : mettre en place des solutions techniques permettant de discerner les limites de fonctionnement et qui permettront d'accroître le niveau de crédibilité des fonctions de sécurité.

Evidemment un évaluateur préfère des solutions simples à évaluer. La complexification est une source d'ennui. Mais ne l'est elle pas pour un industriel qui met en œuvre des fonctions de sécurités à partir de COTS ? La question posée est : **« Comment**

garantir malgré tout un développement qui permettra de garantir un bon niveau de qualité de réalisation ». L'association de composants **« SILés »** n'est pas suffisante en soi, elle amène des interrogations du fait de leur utilisation. Cela signifie qu'il faut absolument garder une vision globale pour espérer garder le contrôle technique des fonctions de sécurité.

Que ce soit pour l'évaluateur ou l'industriel, la seule voie disponible est donc de partager une vision commune sur la nécessité de maîtriser au mieux les limites de fonctionnement. Il est inutile de vouloir à tout prix coller absolument à toutes les exigences de la norme. Il est certainement plus important de mettre en évidence les restrictions que de les cacher. La norme ne peut être appliquée d'une façon aveugle, elle a besoin d'un **certain degré de liberté** dans son application pour ne pas être **inapplicable.**

8 REFERENCES

[1] IEC 61508, Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité, 2002.
[2] IEC 61508, Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité, 2010.
[3] Directive européenne Atmosphères Explosibles 94/9/CE
[4] Schéma de Certification Volontaire IECEx (International Electrotechnical Commission Explosive)