SECURITE FONCTIONNELLE DES SYSTEMES RELATIFS A LA SECURITE : 10 ERREURS A EVITER

FUNCTIONAL SAFETY OF SAFETY-RELATED SYSTEMS: 10 MISTAKES TO AVOID

Florent BRISSAUD
FMDS industrie
Florent.Brissaud@FMDSindustrie.fr
Tél. : 06 85 56 29 79

Didier TURCINOVIC
IR&IS
formation@securitefonctionnelle.com
Tél. : 06 08 92 98 70

Résumé

Les systèmes relatifs à la sécurité sont conçus pour mettre en œuvre des fonctions de sécurité, permettant d'assurer ou maintenir l'état de sécurité d'équipements/systèmes/installations par rapport à des événements dangereux spécifiques. Face au rôle critique de ces systèmes pour la maîtrise des risques industriels, des normes de sécurité fonctionnelle ont été élaborées. Celles-ci fournissent des prescriptions sur toutes les activités liées au cycle de vie de sécurité de ces systèmes, dont la CEI 61508 (générique) et la CEI 61511 (pour les industries de transformation). Partout dans le monde, elles sont devenues des références de bonnes pratiques de la sécurité fonctionnelle. Cependant, l'expérience de plus d'une décennie a permis de révéler que certains concepts utilisés dans ces normes sont toujours méconnus, mal interprétés ou mal appliqués. Cela conduit à une perte de sécurité causée par un défaut de contrôle des défaillances « systématiques » et/ou « aléatoires ».
L'objectif de cette communication est d'améliorer les bonnes pratiques en sécurité fonctionnelle autour des 10 thèmes suivants : le cycle de vie de sécurité (SLC) ; la gestion de la sécurité fonctionnelle (FSM) ; le niveau d'intégrité de sécurité (SIL) ; la spécification des exigences de sécurité (SRS) ; la probabilité moyenne de défaillance dangereuse en cas de sollicitation (PFDavg) ; les indisponibilités moyennes, maximales et par sollicitation ; la fréquence moyenne de défaillance dangereuse par heure (PFH) ; l'architecture du système « M-parmi-N » (MooN) ; la « proportion de défaillances en sécurité » (SFF) ; et la certification. Après une brève présentation de chacun de ces points et des exigences qui s'y rapportent, certaines erreurs rencontrées dans l'industrie sont expliquées afin d'inviter les potentiels acteurs à ne pas ou plus les reproduire.

Summary

Safety-related systems are designed to implement safety functions in order to achieve or maintain safe states of equipment items/systems/installations, in respect to specific hazardous events. Due to the critical role of safety-related systems for managing industrial risks, functional safety standards have been developed. These standards provide guidelines and requirements for all safety lifecycle activities of these systems, notably the IEC 61508 (generic) and the IEC 61511 (for the process industries). All around the world, they have become references for the best practice of functional safety. However, more than a decade of on-the-field experience has shown that several concepts used in these standards are still unrecognised, misinterpreted, or incorrectly implemented. This lead to a loss of safety caused by a loss of control of "systematic" and/or "random" failures.
This paper aims at contributing to a better practice of functional safety about the following 10 topics: Safety Lifecycle (SLC); Functional Safety Management (FSM); Safety Integrity Level (SIL); Safety Requirement Specification (SRS); Average Probability of dangerous Failure on Demand (PFDavg); Average, maximum, and on-demand unavailabilities; Average frequency of a dangerous failure per hour (PFH); System architecture "M-out-of-N" (MooN); "Safe Failure Fraction" (SFF); and Certification. Once each of these points is briefly presented, with the corresponding requirements, mistakes observed in the industry are explained in order to avoid to do or to reproduce them.

1. Introduction

Les systèmes relatifs à la sécurité sont conçus pour mettre en œuvre des fonctions de sécurité, permettant d'assurer ou maintenir l'état de sécurité d'équipements/systèmes/installations par rapport à des événements dangereux spécifiques. La sécurité fonctionnelle est alors le sous-ensemble de la sécurité globale qui se rapporte aux équipements/systèmes/installations et à leurs systèmes de commande, qui dépend du bon fonctionnement des systèmes relatifs à la sécurité.

Face au rôle critique des systèmes relatifs à la sécurité pour la maîtrise des risques industriels, des normes internationales ont été élaborées pour fournir des prescriptions sur toutes les activités liées à leur cycle de vie de sécurité. En particulier, la norme CEI 61508 (CEI, 2010) fournit une approche générique pour les systèmes électriques et/ou électroniques et/ou électroniques programmables (E/E/PE) relatifs à la sécurité. Des normes de produits et d'applications sectorielles sont aussi basées sur celle-ci, notamment la CEI 61511 (CEI, 2004) pour les Systèmes Instrumentés de Sécurité (SIS) utilisés dans le secteur des industries de transformation.

La première édition de la CEI 61508 a été publiée à la fin des années 1990 et la seconde édition est parue en 2010. La première édition de la CEI 61511 a été publiée au début des années 2000 et la seconde édition devrait paraître très prochainement. Ces normes, maintenant reconnues partout dans le monde, sont devenues des références pour la bonne pratique de la sécurité fonctionnelle. Cependant, l'expérience de plus d'une décennie de pratique a permis de révéler que certains concepts utilisés dans ces normes sont toujours méconnus, mal interprétés ou mal appliqués. Cela conduit à une perte de sécurité causée par un défaut de contrôle des défaillances « systématiques » (i.e. liées 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) et/ou « aléatoires » (i.e. survenant de manière aléatoire et résultant d'un ou de plusieurs mécanismes de dégradation potentiels au sein du matériel).

L'objectif de cette communication est d'améliorer les bonnes pratiques en sécurité fonctionnelle autour de 10 thèmes sélectionnés. Après une brève présentation de chacun de ces points et des exigences qui s'y rapportent, certaines erreurs rencontrées dans l'industrie sont expliquées afin d'inviter les potentiels acteurs à ne pas ou plus les reproduire.

2. Dix erreurs à éviter

2.1. Cycle de vie de sécurité (SLC)

Le cycle de vie de sécurité (*Safety LifeCycle*, SLC) est fondamental pour l'application des normes CEI 61508 et CEI 61511 parce qu'il constitue un « cadre technique » pour « traiter de façon systématique toutes les activités nécessaires pour assurer l'intégrité de sécurité[1] requise pour les fonctions de sécurité » (CEI, 2010 : Partie 1, Paragraphe 7.1.1.1) exécutées par les systèmes relatifs à la sécurité. Le SLC, tel que décrit dans la CEI 61508 et la CEI 61511, est schématisé sur la Figure 1.

Le SLC peut être comparé à une feuille de route. Il fournit une description structurée de l'itinéraire à suivre, phase par phase, requis pour la bonne exécution d'un projet. Une phase correspond à une période durant laquelle des activités spécifiques sont réalisées. Chaque phase est alimentée par les précédentes dans un ordre précis matérialisé par des flèches (cf. Figure 1). Les différentes phases sont organisées en cinq catégories clef, fidèles au cycle de vie de tout projet d'ingénierie : conception (dont analyses), réalisation/installation, exploitation/maintenance, modification et mise hors service.

En plus de la description temporelle des phases d'un projet, l'intérêt d'avoir un SLC est d'identifier formellement pour chaque phase : (a) les activités à réaliser (décomposées en activités élémentaires) ; (b) les compétences requises pour réaliser les activités ; (c) la répartition des responsabilités parmi les acteurs du projet ; et (d) les documents requis, notamment les livrables devant être produits pour passer à la phase suivante.

La formalisation de l'approche est renforcée par deux « gardes » qui doivent être franchis à l'issu de chaque phase, avant de passer à la suivante : la vérification et l'évaluation. Ces activités sont destinées à être exécutées par des tierces parties, c'est-à-dire différentes de celles qui ont réalisées les activités ou qui en sont responsable, et non assujetties à la même ligne de management. Ces « gardes » permettent d'assurer : l'exactitude technique des livrables, tels qu'originellement spécifiés ; et la véracité de la sécurité fonctionnelle atteinte, qui résulte d'un suivi des procédures adoptées.

Dans l'industrie, le concept du SLC est généralement adopté mais sa mise en application est souvent en conflit avec la planification globale du projet. Lorsque le SLC n'est pas convenablement défini et intégré en amont du projet, il n'est souvent plus utilisé comme une feuille de route mais comme une « check-list ». Ainsi, une application erronée du SLC consiste à considérer comme « faites » toutes les activités requises (avec des documents fournis en tant que « preuve »), même si elles n'ont pas été réalisées (voire même définies) dans le bon ordre. Dans ce cas, certaines activités n'ont possiblement pas été réalisées sur la base des bonnes exigences et/ou informations d'entrée, ce qui induit de possibles défaillances « systématiques ». Ces défaillances étant ensuite très difficiles à identifier, la confiance attribuable aux produits de sortie est fortement réduite. C'est alors l'intérêt même de toute la démarche de sécurité fonctionnelle telle qu'elle a été appliquée qui peut être remise en cause.

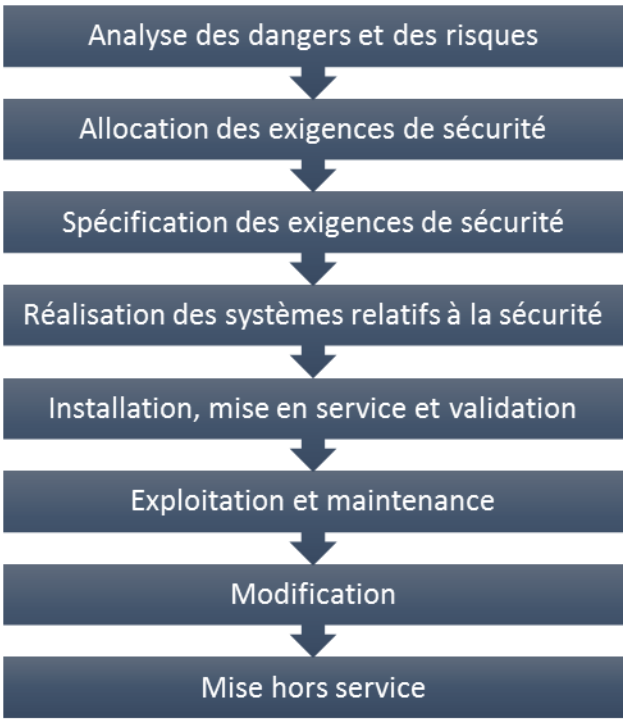

Figure 1. SLC synthétique, suivant les normes CEI 61508 et CEI 61511

[1] cf. Paragraphe 2.3 pour la définition d'"intégrité de sécurité".

2.2. Gestion de la sécurité fonctionnelle (FSM)

La gestion de la sécurité fonctionnelle (*Functional Safety Management*, FSM) est exigée tout au long du SLC (cf. Paragraphe 2.1), tel qu'il est établi dans les normes CEI 61508 et CEI 61511. Ceci implique une organisation et des ressources adéquates, ainsi que des activités spécifiques. Cependant, le rôle du « manageur sécurité fonctionnelle » n'est pas explicitement spécifié.

Dans la plupart des entreprises, les activités (e.g. opérations, ventes, ressources humaines, finances, etc.) et les ressources correspondantes sont généralement bien identifiées, avec des « manageurs » désignés qui en assure la responsabilité. « Être responsable » est souvent interprété comme « devoir rendre compte des actes (de ceux) dont on a la charge ». Lorsqu'une mésaventure se produit, cela est alors traduit par « être condamnable ». Cependant, « être responsable » devrait plutôt être vu sous un angle positif, notamment lorsque tout se déroule normalement, et alors plus justement interprété comme « être capable de répondre ». Ainsi, une personne responsable devrait avant tout être considérée comme celle qui est capable de produire ce qui est escompté, plutôt que comme celle qui est condamnable pour ce qui n'est pas escompté. Pour être responsable, une personne doit alors être compétente pour les tâches qui lui sont confiées, en possession des moyens suffisants pour leurs accomplissements, et investie de l'autorité requise pour cela.

La FSM est due tout au long du SLC. Cela peut communément représenter de 20 à 40 ans, ce qui est plus que la durée moyenne d'une carrière professionnelle au sein d'une même entreprise. Il est alors fondamental de réaliser la FSM avec continuité dans le temps et à travers toutes les organisations impliquées, pour maintenir la sécurité fonctionnelle. Malheureusement, certaines organisations ne sont pas suffisamment préparées ou « équipées » pour suivre le même projet sur une longue période sans discontinuité. Le défi est encore plus grand lorsque de nombreux sous-traitants sont impliqués. Par exemple, une simple action de maintenance implique des équipes d'opération, de maintenance, d'achat et de logistique pour l'exploitant du site, ainsi que des équipes de support technique, de maintenance et de transport pour le fournisseur. Théoriquement, toutes ces parties ont un impact direct ou indirect pour maintenir la PFDavg ou la PFH (cf. Paragraphes 2.5 et 2.7) telle qu'originellement calculée. La FSM nécessite alors de définir explicitement qui s'assure que toutes les informations requises sont connues de tous les acteurs et que les actions de maintenance sont réalisées telles qu'elles le devraient.

Une seconde problématique est que la gestion d'un projet est souvent menée avec une vision à court terme alors que le FSM est orienté sur le long terme, sur tout le SLC. De plus, lorsque l'attribution des efforts est conflictuelle, la priorité est souvent donnée au court terme via une autorité plus forte au sein des organisations, délaissant alors la FSM.

2.3. Niveau d'intégrité de sécurité (SIL)

L'intégrité de sécurité est un attribut d'un système relatif à la sécurité, au regard de fonctions de sécurité. Elle est définie par la probabilité pour que le système relatif à la sécurité exécute de manière satisfaisante les fonctions de sécurité spécifiées (dans toutes les conditions énoncées et dans une période de temps spécifiée). Les niveaux d'intégrité de sécurité (*Safety Integrity Level*, SIL) sont des classes, échelonnant l'intégrité de sécurité entre SIL 1 (pour la plus faible intégrité) et SIL 4 (pour la plus forte intégrité). Selon la norme appliquée, l'intégrité de sécurité (et donc le SIL) est un concept applicable aux systèmes électriques/ électroniques/ électroniques programmables (E/E/PE) relatifs à la sécurité (pour la CEI 61508) ou aux Systèmes Instrumentés de Sécurité (SIS) (pour la CEI 61511). Néanmoins, ce concept est aisément transposable à d'autres systèmes relatifs à la sécurité.

Basée sur l'analyse des dangers et des risques, la phase d'allocation des exigences de sécurité (cf. SLC, Figure 1) permet d'attribuer une valeur cible de SIL à chaque fonction de sécurité requise, afin d'obtenir les réductions de risque nécessaires. Le SIL est ensuite utilisé pour spécifier les exigences liées à l'intégrité de sécurité (qui sont reportées dans la SRS, cf. Paragraphe 2.4). Ces exigences concernent l'intégrité de sécurité systématique, l'intégrité de sécurité du matériel, ainsi que l'intégrité de sécurité du logiciel. C'est alors le rôle de la phase de réalisation/conception de vérifier que les systèmes relatifs à la sécurité répondent à ces exigences. Notamment, les exigences relatives à l'intégrité de sécurité du matériel couvrent à la fois des contraintes architecturales (pour lesquelles la SFF peut éventuellement être utilisée, cf. Paragraphe 2.9) et la quantification de l'effet de défaillances aléatoires du matériel (PFDavg ou PFH, cf. Paragraphes 2.5 et 2.7).

S'il est commun de voir des « rapports SIL » ou « certificats SIL » qui considèrent l'intégrité de sécurité du matériel, certaines autres exigences sont souvent omises, notamment celles relatives à l'intégrité de sécurité systématiques et celles relatives au logiciel. Dans certains cas, il est même observable qu'un SIL a été directement déduit d'un calcul de PFDavg (ou de PFH, cf. Paragraphes 2.5 et 2.7) ou même (bien que plus rarement) d'une simple vérification de contraintes architecturales[2]. Cette approche est erronée. En effet, pour un SIL donné, plusieurs autres exigences doivent aussi être respectées. Tout « rapport SIL » devrait ainsi définir précisément ces limites en termes d'exigences de sécurité. De plus, un « certificat SIL » ne peut pas prétendre qu'un certain SIL est atteint si la totalité des exigences de sécurité n'est pas respectée.

Enfin, il convient aussi de rappeler qu'un SIL se réfère toujours à une fonction de sécurité et qu'il est donc inapproprié d'attribuer un SIL à un système relatif à la sécurité sans définir explicitement et précisément la fonction considérée.

2.4. Spécification des exigences de sécurité (SRS)

La phase de spécification des exigences de sécurité (*Safety Requirement Specification*, SRS) succède à la phase d'allocation dans le SLC et fournit des informations requises pour la phase de réalisation/conception (cf. Figure 1). L'objectif de la SRS est de spécifier les exigences du système relatif à la sécurité, en termes de fonctions de sécurité et d'intégrité de sécurité. La norme CEI 61511 fournit notamment une liste de 27 exigences à spécifier[3] pour les SIS utilisés dans le secteur des industries de transformation (CEI, 2004 : Partie 1, Paragraphe 10.3.1).

---

[2] Par exemple, le guide "Evaluation des Barrières Techniques de Sécurité - Ω 10" (INERIS, 2008) propose une démarche qui ne retient que des aspects dits "qualitatifs" (correspondant à une vérification des contraintes architecturales), sans prise en compte des aspects dits "quantitatifs" (à savoir, la quantification de l'effet de défaillances aléatoires du matériel) – on parle alors de "niveau de confiance" (NC) et non de SIL. Une erreur répandue consiste alors à considérer qu'un NC est équivalent à un SIL.

[3] Il est prévu que cette liste soit légèrement étendue dans la seconde édition de la CEI 61511, à paraître prochainement.

Il est important que la SRS décrive les fonctions de sécurité et leurs performances de sécurité fonctionnelle requises (qui incluent l'intégrité de sécurité) en termes non spécifiques aux équipements. En effet, les concepteurs du système doivent ensuite utiliser la SRS comme base pour la sélection des équipements et des architectures du système relatif à la sécurité. Ensuite, les phases suivantes du SLC (et notamment la phase de réalisation/conception) permet de vérifier que le système relatif à la sécurité respecte toutes les exigences spécifiées dans la SRS. C'est pourquoi la SRS doit être « claire, précise, non ambiguë, vérifiable, testable, actualisable et réalisable » et « être rédigée de manière à faciliter la compréhension des personnes susceptibles d'utiliser les informations à toute étape » du SLC (CEI, 2010 : Partie 1, Paragraphe 7.10.2.4).

Lorsque la SRS est réalisée alors qu'un système relatif à la sécurité en particulier est déjà envisagé ou installé, une erreur commune consiste à décrire le choix technologique actuel sans impartialité envers les exigences de sécurité. Par exemple, l'exigence sur le temps de réponse est alors parfois incorrectement définie par le temps de réponse actuel de la fonction de sécurité à la place de la « durée de réalisation nécessaire de la fonction de sécurité » (CEI, 2010 : Partie 1, Paragraphe 7.10.2.6). Dans ce cas, la SRS est inutile et, surtout, certaines défaillances systématiques ne peuvent pas être évitées. Concernant les exigences sur l'intégrité de sécurité, il est aussi curieux de voir certaines SRS spécifier une « contribution cible au PFDavg » (cf. Paragraphe 2.5) pour chaque sous-système du système relatif à la sécurité (par exemple, 30% pour les capteurs, 20% pour l'unité logique et 50% pour les éléments terminaux[4]) sans justification en termes de sécurité.

2.5. Probabilité moyenne de défaillance dangereuse en cas de sollicitation (PFDavg)

La quantification de la probabilité moyenne de défaillance dangereuse en cas de sollicitation (*average Probability of a dangerous Failure on Demand*, PFDavg) est requise pour les fonctions de sécurité faiblement sollicitées (réalisées uniquement sur sollicitation, avec une fréquence de sollicitations inférieure à une par an). Cette exigence est relative à l'intégrité de sécurité du matériel, et plus spécifiquement à la quantification de l'effet de défaillances aléatoires du matériel (cf. Paragraphe 2.3). La PFDavg représente alors l'intégrité de sécurité obtenue du système relatif à la sécurité due aux défaillances aléatoires du matériel ; et doit être inférieure à la valeur spécifiée dans la SRS (cf. Paragraphe 2.4).

La PFDavg est calculée par l'indisponibilité moyenne de sécurité (CEI, 2010 : Partie 4, Paragraphe 3.6.18), et doit tenir compte de certaines caractéristiques (CEI, 2010 : Partie 2, Paragraphe 7.4.5.2) : architecture du système, taux de défaillance, défaillances de cause commune, intervalles et efficacité des essais/tests, temps de réparation, erreurs humaines aléatoires… Pour cette quantification, plusieurs méthodes peuvent être utilisées, dont : des équations approchées, des blocs diagrammes de fiabilité, des arbres de défaillance, des modèles markoviens (multi-phase) et des réseaux de Petri (stochastiques à prédicats). Sous certaines conditions, toutes ces méthodes sont capables de fournir de « bons » résultats, en tenant compte des caractéristiques requises par la CEI 61508. Pour cela, il est néanmoins nécessaire de maîtriser la méthode utilisée (ce qui implique notamment de connaître leurs hypothèses intrinsèques) et d'utiliser un outil logiciel adapté et performant. À ce sujet, la CEI 61508 précise notamment qu' : « il est essentiel que l'utilisateur soit compétent dans l'utilisation de la technique retenue, ce qui revêt une plus grande importance que la technique réellement appliquée » ; « il incombe à l'analyste de vérifier la conformité des hypothèses sous-jacentes à toute méthode particulière » ; et « lorsque des programmes logiciels sont utilisés pour les calculs, l'analyste doit alors avoir une bonne connaissance des formules/techniques utilisées par le progiciel pour garantir qu'elles sont correctement utilisées pour l'application spécifique » (CEI, 2010 : Partie 6, Paragraphe B.1). Le choix d'une méthode doit alors se faire sans *a priori*, sur la base d'un accord entre les efforts de modélisation, les objectifs et les propriétés du système (Brissaud *et al.*, 2012).

En particulier, si les équations approchées fournissent un moyen simple et rapide d'évaluer de nombreux systèmes simples/basiques, cette approche est aussi, par nature, la moins flexible. Malheureusement, certains utilisateurs sont tentés d'appliquer de telles formules sans prendre convenablement les hypothèses sous-jacentes en considération. Des situations dangereuses peuvent alors apparaître lorsque des hypothèses « non-conservatives » sont faites. Dans les faits, lorsque des équations approchées sont utilisées, il est même rare de voir une description convenable de toutes les hypothèses considérées.

2.6. Indisponibilités moyennes, maximales et par sollicitation

Fondamentalement, les systèmes relatifs à la sécurité sont conçus pour réduire la fréquence (ou probabilité) d'un évènement dangereux et/ou sa gravité. Cette réduction de risque permet alors d'atteindre un niveau de risque tolérable, par rapport à un événement dangereux spécifique.

La PFDavg (cf. Paragraphe 2.5) fournit un indicateur intéressant de réduction de risque, mais cet indicateur n'est pas exhaustif. En effet, la PFDavg est basée sur une valeur moyenne de l'indisponibilité d'un système relatif à la sécurité à exécuter de manière satisfaisante la fonction de sécurité spécifiée en cas de sollicitation. La PFDavg prend tout son sens lorsque les sollicitations de la fonction de sécurité se produisent uniformément dans la période considérée. S'il y a des intervalles de temps (e.g. démarrage, maintenance, mode manuel, etc.) où les sollicitations sont plus fréquentes, alors des indisponibilités moyennes spécifiques (calculées dans ces intervalles) doivent être considérées. Par exemple, si dans un intervalle de temps très court par rapport à la durée de vie du système (e.g. 30 secondes sur 4 ans), la probabilité qu'une sollicitation se produise est très proche de 1 (à cause de conditions spécifiques dans cet intervalle) et que l'indisponibilité du système relatif à la sécurité est aussi très proche de 1, alors le risque est très élevé. Cependant, en tant que valeur moyenne, la PFDavg peut toujours conduire à de « très bons résultats » (l'ordre de grandeur de 30 secondes sur 4 ans est de 10^{-7}, ce qui est compatible avec un SIL 4).

En tant qu'indicateur complémentaire, il est ainsi souvent utile de considérer la valeur maximale de l'indisponibilité d'un système relatif à la sécurité à exécuter de manière satisfaisante la fonction de sécurité spécifiée en cas de sollicitation (généralement notée PFDmax).

Enfin, notons aussi qu'il peut exister des dépendances entre les valeurs d'indisponibilité (PFDavg et PFDmax) et les sollicitations elle-même. Notamment, la CEI 61508 précise que, en plus des défaillances dépendantes du temps caractérisées par des taux de défaillance, il existe aussi des défaillances causées par les sollicitations de la fonction de sécurité (CEI, 2010 : Partie 4, Paragraphe 3.6.18). Cette dernière est, par exemple, caractérisée par une probabilité de défaillance par sollicitation (notée γ).

[4] Il est souvent supposé que ces contributions sont "observables" dans la pratique. Cependant, cela ne constitue pas une justification de leurs spécifications dans la SRS.

2.7. Fréquence moyenne de défaillance dangereuse par heure (PFH)

Le terme « probabilité d'une défaillance dangereuse par heure » (*Probability of dangerous Failure per Hour*, PFH) a été introduit dans la première édition de la CEI 61508. Ce terme est inapproprié parce qu'une probabilité est toujours sans unité et ne peut donc par être exprimée « par heure »[5]. En fait, la PFH n'est pas une probabilité mais une fréquence. C'est pourquoi, dans la seconde édition de la CEI 61508, la PFH a été redéfinie par « fréquence moyenne de défaillance dangereuse par heure ». L'abréviation PFH a alors été gardée pour des raisons de continuité mais le terme « probabilité d'une défaillance dangereuse par heure » ne doit plus être utilisé.

La PFH est utilisée à la place de la PFDavg lorsque les fonctions de sécurité ne sont pas faiblement sollicitées[6] (i.e. sollicitation élevée ou continu). La PFH est définie par une fréquence moyenne de défaillance (dangereuse). Une fréquence de défaillance est équivalente à une « intensité inconditionnelle de défaillance » et ne doit pas être confondue avec un « taux de défaillance ». Pour faire simple, lorsque les valeurs sont constantes, l'intensité inconditionnelle de défaillance est l'inverse du temps moyen entre défaillances (*Mean Time Between Failures*, MTBF) tandis que le taux de défaillance est l'inverse du temps moyen (de bon fonctionnement) avant défaillance (*Mean Time To Failure*, MTTF). C'est-à-dire que la première prend le temps de rétablissement[7] (*Mean Time To Restoration*, MTTR) en compte, contrairement au second.

Lorsque le taux de défaillance est constant et que les défaillances sont détectée et réparées rapidement, ces deux mesures sont proches l'une de l'autre. De plus, le taux de défaillance moyen est plus élevé que l'intensité inconditionnelle moyenne de défaillance. Ainsi, il n'est pas vraiment « dangereux » de considérer que la PFH est un taux de défaillance moyen à la place d'une intensité inconditionnelle moyenne de défaillance. Cependant, il est curieux d'observer que plusieurs références (dont certains guides[8] « officiels » et/ou très utilisés) utilisent des définitions erronées. De plus, il est toujours regrettable que certaines références alimentent des confusions telles que probabilité (sans unité) et fréquence (par unité de temps), ou fréquence (qui tient compte des réparations) et taux de défaillance (qui ne se rapporte qu'à la fiabilité et ne tient donc pas compte des réparations).

2.8. Architecture du système « M-parmi-N » (MooN)

L'architecture du système doit être prise en compte pour la quantification de l'effet de défaillances aléatoires du matériel (PFDavg ou PFH, cf. Paragraphes 2.5 et 2.7). Classiquement, un système (instrumenté) relatif à la sécurité est considéré comme un système constitué de trois sous-systèmes en série : capteur(s), unité(s) logique(s) et élément(s) terminal(aux). Le système est alors capable d'exécuter de manière satisfaisante sa fonction de sécurité si et seulement si tous ces sous-systèmes sont capables d'exécuter leurs (sous-)fonctions de sécurité. De plus, chaque sous-système est souvent défini par une architecture « M-parmi-N » (*M-out-of-N*, MooN). Cela signifie qu'il est composé de N éléments (i.e. canaux) et qu'il est capable d'exécuter sa (sous-)fonction de sécurité si et seulement si M éléments, n'importe lesquels, ou plus (parmi N) ne sont pas dans un état de panne dangereuse. Par définition, une architecture 1ooN correspond à un sous-système parallèle (i.e. techniquement la plus sûre) et une architecture NooN correspond à un sous-système série (i.e. techniquement la moins sûre). Il est important de souligner que la logique de succès d'une architecture MooN est « M éléments, n'importe lesquels, ou plus ». Les mots « n'importe lesquels » sont importants. Cela implique notamment que tous les N éléments doivent être sollicités par la (sous-)fonction de sécurité, quel que soit les scénarios considérés.

En tant que premier exemple, prenons 8 capteurs qui mesurent les vibrations d'un compresseur : 4 dans la partie A et 4 dans la partie B. La logique de l'instrumentation est définie de telle sorte que 2 mesures de sur-vibration suffisent à commander l'arrêt du compresseur. L'architecture de ce sous-système serait-elle donc 2oo8 ? La réponse est oui uniquement si tous les scénarios possibles de sur-vibration impliquent systématiquement des sur-vibrations à la fois dans la partie A et dans la partie B du compresseur (sur la base des seuils de détection définis pour chaque capteur). S'il existe un scénario où une seule partie du compresseur est sujette à des sur-vibrations, alors l'architecture du sous-système devient 2oo4 (parce que seulement 4 capteurs sur les 8 seraient sollicités). En tant que deuxième exemple, prenons un système de protection incendie qui utilise 4 capteurs de fumée dans une même pièce. La logique de l'instrumentation est définie de telle sorte qu'une seule détection de fumée suffit à commander l'alarme. En cas d'incendie, si la fumée atteint tous les 4 capteurs, alors l'architecture du sous-système est 1oo4. Cependant, il peut être trop tard d'attendre que tous les capteurs soient sollicités et, dans la plupart des cas, il peut être requis d'activer l'alarme dès qu'un premier capteur détecte de la fumée. Dans ce cas, l'architecture du sous-système doit être définie en 1oo1 (même si 4 capteurs sont installés).

Une erreur dans la définition de l'architecture d'un sous-système peut conduire à une dangereuse sous-estimation de la PFDavg ou PFH (cf. exemples précédents). De plus, il est à noter que les équations approchées fournies par la CEI 61508 (Partie 6) sont limitées à des architectures MooN où tous les N éléments ont des taux de défaillance identiques et sont soumis aux mêmes tests et actions de réparation. Dans de nombreux cas, il peut alors être nécessaire d'utiliser une méthode plus appropriées, comme des arbres de défaillance ou des réseaux de Petri pour quantifier l'effet de défaillances aléatoires du matériel.

Enfin, il est aussi important de rappeler que tous les éléments définis dans l'architecture d'un sous-système (dans le cas d'une architecture MooN : les N éléments) doivent être directement impliqués dans l'exécution de la fonction de sécurité spécifiée. En effet, une étude de sécurité fonctionnelle concerne toujours une fonction de sécurité spécifique. Notamment, une erreur commune consiste à inclure des éléments terminaux de « cascade » dans la définition des architectures. Par exemple, il est évident que l'arrêt d'un compresseur ou la fermeture du flux de sortie d'un réservoir nécessite d'autres actions comme l'isolation d'unités connexes, la dépressurisation, ou des envois de gaz à la torche afin de prévenir des effets collatéraux. Néanmoins, ces scénarios « collatéraux » doivent être couverts par d'autres fonctions de sécurité spécifiques (avec des SRS dédiées) et être étudiées en tant que telles. En particulier, ces fonctions de sécurité de « cascade » n'ont pas forcément les mêmes exigences en termes de valeur cible de SIL (cf. Paragraphe 2.3).

---

[5] Eventuellement, il pourrait s'agir d'une probabilité de défaillance "en une heure" (Brissaud *et al.*, 2009).
[6] cf. Paragraphe 2.5 pour la définition de "faiblement sollicitée".
[7] En accord avec la CEI 61508, le MTTR est la somme du temps moyen de détection de la panne (*Mean Fault Detection Time*, MFDT) et du temps moyen de réparation (*Mean Repair Time*, MRT). De plus, MTBF = MTTF + MTTR.
[8] Par exemple, le "PDS Method Handbook" (SINTEF, 2013) stipule que la PFH est la "*probability of failure per hour*" et qu'elle est égale au "*dangerous undetected failure rate*".

2.9. « Proportion de défaillances en sécurité » (SFF)

La « proportion de défaillances en sécurité » (SFF) a été introduite dans la première édition de la CEI 61508 comme critère de contraintes architecturales, dont la vérification fait partie des exigences relatives à l'intégrité de sécurité du matériel (cf. Paragraphe 2.3). La SFF est définie par la somme des taux de défaillance moyens des défaillances en sécurité (détectées ou non en ligne) et dangereuses détectées en ligne, divisée par la somme des taux de défaillance moyens des défaillances en sécurité (détectées ou non en ligne) et dangereuses (détectées ou non en ligne). Par définition, seules les défaillances dangereuses empêchent (ou diminuent la probabilité de) l'exécution satisfaisante de la fonction de sécurité spécifiée, lorsque nécessaire ; tandis que les défaillances « en sécurité » conduisent à (ou augmentent la probabilité de) l'exécution « parasite » de la fonction de sécurité spécifiées. Les autres défaillances, comme celles dites « partielles[9] » ou « sans effet », n'interviennent pas dans le calcul de la SFF (cf. CEI 61508, Partie 4, pour toutes les définitions).

En pratique, une SFF élevée peut « justifier » (selon la CEI 61508) une plus faible redondance (i.e. « tolérance aux anomalies du matériel ») pour un SIL visé. La SFF est ainsi devenue un argument commercial de fabricants/fournisseurs de matériel parce que, pour une fonction de sécurité avec un SIL spécifié, un utilisateur qui sélectionne un matériel dont la SFF est élevée peut éviter l'ajout de redondances (par exemple, un seul matériel à la place de deux ou trois en redondance). Cependant, l'utilisation de la SFF en tant que critère de sécurité est insensée. En effet, il est facile de voir que la SFF peut être artificiellement augmentée uniquement en ajoutant (ou surestimant) des défaillances « en sécurité ». Par exemple, si un fabricant ajoute dans son matériel une sorte de « module » qui crée aléatoirement des déclenchements intempestifs de la fonction de sécurité, alors la SFF s'en trouvera augmentée. Pour des taux de défaillance dangereux identiques, il est inapproprié de considérer qu'un matériel est « meilleur » (avec une plus faible exigence en termes de redondances) si les taux de défaillance « en sécurité » sont plus élevés – ce qui est l'hypothèse intrinsèque de la SFF. En pratique, des défaillances « en sécurité » qui se produisent trop fréquemment peuvent d'ailleurs devenir dangereuses pour deux raisons : des actions de maintenance supplémentaires sont requises, avec des expositions additionnelles de personnes et de nouvelles possibilités d'erreurs humaines ; et lorsqu'un matériel provoque trop souvent des déclenchements intempestifs, il est tentant d'ignorer les « alarmes » associées[10], voire même de les court-circuiter. Donner du crédit à la SFF est donc, au mieux inutile et, au pire contre-productif et donc dangereux[11].

L'utilisation de la SFF a déjà été remise en cause plusieurs fois dans des références techniques et scientifiques (Langeron *et al.*, 2007 ; Innal *et al.*, 2006). Ainsi, la seconde édition de la CEI 61508 a mis en place un « parcours » alternatif (dit « 2H »[12]) où les contraintes architecturales ne tiennent pas compte de la SFF. Néanmoins, une restriction de ce « parcours » est que « les données de fiabilité utilisées pour quantifier l'effet des défaillances aléatoires du matériel » (PFDavg ou PFH, cf. Paragraphes 2.5 et 2.7) doivent être « basées sur les retours d'exploitations concernant les équipements utilisés dans une application et un environnement similaires » et collectées « conformément aux normes internationales » afin d' « estimer la moyenne et le niveau d'incertitude » (CEI, 2010 : Partie 2, Paragraphe 7.4.4.3.3). Cette approche alternative n'est donc applicable qu'aux systèmes déjà en utilisation et avec un retour d'expérience spécifique disponible. En conséquence, la SFF est toujours fréquemment utilisée via le premier « parcours » (dit « 1H »[13]). Une raison pour avoir conservé la SFF est probablement la continuité avec la première édition de la CEI 61508, cependant, des lobbies plus « commerciaux » pourraient aussi y avoir contribué. Quoiqu'il en soit, le « parcours 2H » doit être préféré au « parcours 1H » autant que possible et, à terme, l'utilisation de la SFF devrait être supprimée pour des questions de sécurité.

2.10. Certification

Aujourd'hui, dans l'industrie, presque tout est certifié ou « certifiable »: composants, équipements, systèmes, professionnels, organisations et, dans certains cas, même des installations complètes. Cependant, il convient de rappeler que la certification n'est pas une exigence de la CEI 61508 ou de la CEI 61511. D'ailleurs, le terme « certification » ne peut être trouvé que dans l'avant-propos de la CEI 61508 pour rappeler que « des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI » et que « la CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants » (CEI, 2010 : Avant-propos). Ces normes fournissent simplement des « guides de bonnes pratiques » en sécurité fonctionnelle, censés refléter un certain « état de l'art ». Selon l'AFNOR, « la certification est une activité par laquelle un organisme reconnu, indépendant des parties en cause, donne une assurance écrite qu'une organisation, un processus, un service, un produit ou des compétences professionnelles sont conformes à des exigences spécifiées dans un référentiel »[14]. Précisons que cette « conformité » est évaluée à un instant donné et selon un certain niveau de vérification possible.

Le SIL (cf. Paragraphe 2.3) établi dans un certificat devrait être considéré comme un simple « visa » d'entrée dans le monde industriel, rendant ainsi un produit « éligible » à son intégration dans un projet, mais non suffisant. Une erreur commune consiste à se satisfaire d'un certificat sans autre considération, interprétant celui-ci comme une décharge de responsabilité en cas de problème. Cependant, lorsqu'un produit est accepté sur l'unique base d'un certificat, il est difficile d'identifier *a posteriori* d'éventuels points qui ne répondraient finalement pas aux exigences particulières d'un projet. Les conséquences pour un projet peuvent alors être critiques, surtout si les non-conformités sont révélées en phase d'opération. Un deuxième « visa » doit ainsi être considéré afin de vérifier la comptabilité effective du produit avec les particularités du projet. Pour cela, tous les critères des normes doivent ainsi être revus, en y incluant notamment les aspects concernant le matériel, le logiciel, la FSM et la documentation (cf. Paragraphes 2.2 et 2.3). Cela nécessite une analyse minutieuse de la cohérence des informations fournies, ainsi que leurs implications pratiques, tout au long du SLC (cf. Paragraphes 2.1). Des informations cruciales peuvent ainsi être trouvées dans les rapports de certification et les manuels de sécurité. Ces documents doivent notamment fournir le détail des activités réalisées, les données, les limites et les conditions utilisées pour évaluer la conformité du produit. Toutes ces informations doivent être comparées avec la réalité du projet.

---

[9] "Défaillance partielle" est une traduction ambigüe de "*no part failure*", telle qu'utilisée dans la CEI 61508.

[10] Par exemple, dans le cas de l'explosion de la raffinerie de BP Texas City en 2005 (ARIA, 2010), une alarme a été ignorée alors qu'elle avait convenablement détecté l'évènement dangereux qui a conduit à la catastrophe.

[11] À noter que la SFF ne doit pas être confondue avec la couverture du diagnostic (DC), dont la pertinence n'est pas remise en cause.

[12] Ce parcours est "basé sur le retour d'exploitation par l'utilisateur final", une confiance plus élevée dans les données de fiabilité et "une tolérance aux anomalies du matériel (HFT) pour les niveaux d'intégrité de sécurité spécifiés".

[13] Ce parcours est "basé sur les concepts de tolérance aux anomalies du matériel et de proportion de défaillances en sécurité".

[14] http://www.afnor.org/metiers/certification/enjeux

3. Conclusion

En 2010, lorsque la seconde édition de la CEI 61508 a été publiée, elle est entrée dans le top 10 des meilleures ventes de normes de la CEI[15]. Il n'y a donc pas de doute que la sécurité fonctionnelle intéresse les industriels et que ceux-ci sont impatients de connaître les évolutions de ces normes. Cependant, la lecture de celles-ci révèle un contenu dense et complexe.

Cette communication a présenté 10 thèmes de sécurité fonctionnelle pour lesquels certaines erreurs sont couramment rencontrées dans l'industrie. Ces erreurs peuvent notamment être dues à une méconnaissance, une mauvaise interprétation ou une mauvaise application de certains concepts des normes de sécurité fonctionnelle. Dans de nombreux cas, cela peut conduire à une perte de sécurité causée par un défaut de contrôle des défaillances « systématiques » et/ou « aléatoires ». Ainsi, cette communication a pour vocation de contribuer à l'amélioration des bonnes pratiques en sécurité fonctionnelle.

Les dix points traités dans cette communication sont rappelés par les règles de bonnes pratiques présentées dans la Table 1.

Aujourd'hui, plusieurs produits industriels sont conformes aux exigences des normes de sécurité fonctionnelle. Ce succès est souvent ce que retiennent les acteurs. Néanmoins, ce point n'est pas suffisant. En effet, au-delà de la sécurité fonctionnelle des produits, la sécurité exige aussi l'implication de tous les acteurs. Ceux-ci doivent ainsi être pleinement impliqués, conformément aux exigences des normes, afin d'atteindre les performances requises et de les maintenir dans le temps. Il s'agit là d'un des principaux défis de la sécurité fonctionnelle, car tous les acteurs d'un projet n'ont pas nécessairement les mêmes intérêts. De plus, les contributions de chacun ne sont pas toujours en ligne avec certains objectifs financiers.

La sécurité implique que tous les professionnels soient compétents et responsables. Pour cela, chaque professionnel doit avoir reçu une formation théorique et pratique adéquate et doit disposer des moyens et de l'autorité requis pour s'assurer que la sécurité fonctionnelle est atteinte et maintenue. « L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique.[16] »

Références

ARIA, 2010. Fiche détaillée N° 29598 : Explosion dans une unité d'isomérisation, 23 mars 2005, Texas City, Etats-Unis. Retour d'expérience sur accidents technologiques (ARIA).

Brissaud F., Lanternier B., 2009. Les Probabilités de Défaillance comme indicateurs de performance des Barrières Techniques de Sécurité – Approche analytique. Actes du 8ème congrès international pluridisciplinaire en Qualité, Sûreté de Fonctionnement et Développement Durable.

Brissaud F., Oliveira L.F., 2012. Average probability of a dangerous failure on demand: Different modelling methods, similar results. Proceedings of the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012: 6073-6082.

CEI, 2010. CEI 61508 : Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, 2ème édition. Genève : Commission Electrotechnique Internationale (CEI).

CEI, 2004. CEI 61511 : Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation, 1ère édition. Genève : Commission Electrotechnique Internationale (CEI).

INERIS, 2008. Rapport d'étude N° DRA-08-95403-01561B : Evaluation des performances des Barrières Techniques de Sécurité (DCE DRA-73), Evaluation des Barrières Techniques de Sécurité - Ω 10, Version 2. Verneuil-en-Halatte : Institut National de l'Environnement Industriel et des Risques (INERIS).

Innal F., Dutuit Y., Rauzy A., Signoret J.P., 2006. An attempt to understand better and apply some recommendations of IEC 61508 standard. Proceedings of the 30th ESReDA seminar: 1-16.

Langeron Y., Barros A., Grall A., Bérenguer, C., 2007. Safe failure impact on safety instrumented systems. Proceedings of the European Safety and Reliability Conference 2007: 641- 648.

SINTEF, 2013. Reliability Prediction Method for Safety Instrumented Systems, PDS Method Handbook, 2013 Edition. Trondheim : SINTEF Technology and Society.

[15] www.iec.ch/about/annual_report/2010/financial/sales.htm
[16] Citation attribuée à Albert Einstein.

Thème	Règles de bonnes pratiques	Défaillances principalement concernées[17]
Cycle de vie de sécurité (SLC)	Définir et intégrer le SLC suffisamment en amont des projets. Utiliser le SLC comme une feuille de route (les activités sont réalisées dans le bon ordre) et non comme une simple « check-list ».	Systématiques
Gestion de la sécurité fonctionnelle (FSM)	Définir comme « responsable » celui ou celle qui est capable de produire ce qui est escompté (plutôt que comme celui ou celle qui est « condamnable »), ce qui nécessite d'avoir les compétences, les moyens et l'autorité requise. Réaliser la FSM avec continuité dans le temps et à travers toutes les organisations impliquées.	Systématiques et aléatoires
Niveau d'intégrité de sécurité (SIL)	Considérer à la fois l'intégrité de sécurité systématique, l'intégrité de sécurité du matériel (en incluant les contraintes architecturales et la quantification de l'effet de défaillances aléatoires du matériel), et l'intégrité de sécurité du logiciel, pour un SIL donné. Définir explicitement et précisément la fonction de sécurité à laquelle se réfère le SIL.	Systématiques et aléatoires
Spécification des exigences de sécurité (SRS)	Exprimer la SRS en termes non spécifiques aux équipements. Spécifier les exigences de sécurité avec impartialité, sans *a priori* sur l'éventuelle solution envisagée.	Systématiques
Probabilité moyenne de défaillance dangereuse en cas de sollicitation (PFDavg)	Maîtriser la méthode utilisée pour la quantification de la PFDavg et utiliser un outil logiciel adapté et performant. Choisir la méthode sans *a priori*, sur la base d'un accord entre les efforts de modélisation, les objectifs et les propriétés du système. Décrire convenablement toutes les hypothèses considérées.	Aléatoires
Indisponibilités moyennes, maximales et par sollicitation	Calculer des indisponibilités moyennes dans chaque intervalle de temps où les sollicitations de la fonction de sécurité sont (éventuellement) plus fréquentes (démarrage, maintenance, modes manuels, etc.). Utiliser les valeurs maximales d'indisponibilité comme des indicateurs complémentaires des indisponibilités moyennes. Prendre en compte les (éventuelles) défaillances causées par les sollicitations de la fonction de sécurité.	Aléatoires
Fréquence moyenne de défaillance dangereuse par heure (PFH)	Ne pas (ou plus) utiliser le terme « probabilité d'une défaillance dangereuse par heure », qui fait l'amalgame entre fréquence et probabilité. Ne pas confondre la PFH, qui est une fréquence moyenne de défaillance (dangereuse), avec un taux de défaillance.	Aléatoires
Architecture du système « M-parmi-N » (MooN)	Considérer une architecture MooN uniquement si tous les N éléments sont sollicités par la (sous-)fonction de sécurité, quel que soit les scénarios considérés. Ne pas utiliser les équations approchées fournies par la CEI 61508 lorsque les N éléments d'une architecture MooN sont « hétérogènes ». Traiter les scénarios « collatéraux » (avec éléments de « cascade ») via des fonctions de sécurité spécifiques (avec des SRS dédiées).	Aléatoires
« Proportion de défaillances en sécurité » (SFF)	Ne pas considérer que, pour des taux de défaillance dangereux identiques, un matériel est « meilleur » si les taux de défaillance « en sécurité » sont plus élevés (ce qui est une l'hypothèse intrinsèque de la SFF). Préférer le « parcours 2H » au « parcours 1H » pour la vérification des contraintes architecturales. Ne pas (ou plus) utiliser la SFF, pour des questions de sécurité.	Aléatoires
Certification	Ne pas se satisfaire d'un certificat pour choisir une solution industrielle. Vérifier la comptabilité effective des produits envisagés avec les particularités du projet, en comparant les informations des rapports de certification et des manuels de sécurité avec la réalité du projet.	Systématiques et aléatoires

Table 1. Synthèse des règles de bonnes pratiques

[17] cf. Introduction (Paragraphe 1) pour les définitions de "défaillances systématiques" et "défaillances aléatoires".