COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

ENTRAÎNEMENTS ÉLECTRIQUES DE PUISSANCE À VITESSE VARIABLE –

Partie 5-2: Exigences de sécurité – Fonctionnelle

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61800-5-2 a été établie par le sous-comité 22G: Systèmes d'entraînement électrique à vitesse variable, comprenant des convertisseurs à semi-conducteurs, du comité d'études 22 de la CEI: Systèmes et équipements électroniques de puissance.

La présente version bilingue (2013-01) correspond à la version anglaise monolingue publiée en 2007-07.

Le texte anglais de cette norme est issu des documents 22G/179/FDIS et 22G/182/RVD.

Le rapport de vote 22G/182/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 61800, publiées sous le titre général *Entraînements électriques de puissance à vitesse variable*, est disponible sur le site internet de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée; ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Du fait de l'automatisation, de la demande croissante de la production et de la réduction des efforts physiques produits par les opérateurs, les systèmes de commande des machines et des usines jouent un rôle croissant dans l'accomplissement de la sécurité globale. Ces systèmes de commande utilisent de plus en plus d'appareillages et de systèmes électriques/ électroniques/électroniques programmables complexes.

Bien placés, parmi ces appareillages et ces systèmes, se situent les entraînements électriques de puissance à vitesse variable (PDS), utilisables dans des applications relatives à la sécurité (PDS(SR)).

Exemples d'applications industrielles:

- machines-outils, robots, équipements d'essai en production, bancs d'essai;
- machines à papier, machines de production textile, calandres pour l'industrie du caoutchouc;
- lignes de processus des plastiques, de la production chimique ou métallique, moulins;
- machines de concassage du ciment, fours à ciment, mixeurs, centrifugeuses, machines d'extrusion;
- machines de forage;
- convoyeurs, machines de maniement de matériaux, équipements de levage (grues, portiques, etc.);
- pompes, ventilateurs, etc.

Les développeurs utilisant PDS(SR) peuvent également se référer à la présente norme pour d'autres applications.

Il convient que les utilisateurs de la présente norme aient connaissance du fait que certaines normes de type C applicables aux machines font actuellement référence à l'ISO 13849-1 pour les systèmes de commande relatifs à la sécurité. Dans ce cas, les fabricants de PDS(SR) peuvent être invités à fournir des informations supplémentaires (par exemple, le niveau de performance et/ou la catégorie) afin de faciliter l'intégration d'un PDS(SR) dans les systèmes de commande relatifs à la sécurité pour les machines concernées.

NOTE Les «normes de type C» sont définies dans l'ISO 12100-1 comme des normes de sécurité des machines traitant des exigences de sécurité détaillées s'appliquant à une machine particulière ou à un groupe de machines particulier.

Auparavant, en l'absence de normes, il y avait une réticence à accepter des appareillages et des systèmes électroniques dans des fonctions relatives à la sécurité, et en particulier des appareillages et des systèmes électroniques programmables, en raison de l'incertitude liée aux performances de sécurité d'une telle technologie.

Il existe de nombreuses situations où des systèmes de commande incorporant un PDS(SR) sont utilisés, en tant qu'élément de mesures de sécurité par exemple qui ont été prévues pour accomplir une réduction du risque. Le verrouillage de protection est un cas typique qui permet de sortir le personnel d'une situation dangereuse afin que l'accès à la zone dangereuse soit uniquement possible lorsque les parties tournantes ont atteint un état sûr. La présente partie de la CEI 61800 fournit une méthodologie afin d'identifier la contribution apportée par un PDS(SR) aux fonctions de sécurité identifiées, de permettre la conception appropriée du PDS(SR) et de vérifier qu'elle satisfait aux performances demandées

Des mesures sont indiquées afin de coordonner la performance de sécurité du PDS(SR) avec la réduction attendue du risque en prenant en compte les probabilités et les conséquences de ses défaillances systématiques et aléatoires.

ENTRAÎNEMENTS ÉLECTRIQUES DE PUISSANCE À VITESSE VARIABLE –

Partie 5-2: Exigences de sécurité – Fonctionnelle

1 Domaine d'application et objet

La présente partie de la CEI 61800 spécifie des exigences et donne des recommandations pour la conception et le développement, l'intégration et la validation des PDS(SR), en considération de leur sécurité fonctionnelle. Elle s'applique aux entraînements électriques de puissance à vitesse variable couverts par les autres parties de la série CEI 61800.

NOTE 1 Le terme «intégration» se rapporte au PDS(SR) lui-même, non pas à son incorporation dans l'application relative à la sécurité.

Cette norme internationale est applicable uniquement lorsque la sécurité fonctionnelle d'un PDS(SR) est exigée et que le PDS(SR) fonctionne en forte demande ou en mode continu (voir 3.10). Pour les applications à faible demande, voir la CEI 61508.

La présente partie de la CEI 61800, qui est une norme de produit, expose des considérations relatives à la sécurité des PDS(SR) prises dans le cadre de la CEI 61508 et présente des exigences pour les PDS(SR) en tant que sous-systèmes d'un système relatif à la sécurité. Elle est destinée à faciliter la réalisation des éléments électriques/ électroniques/ électroniques programmables (E/E/PE) d'un PDS(SR) en liaison avec la performance de sécurité d'une ou des fonctions de sécurité d'un PDS.

En se référant aux exigences normatives de la présente partie de la CEI 61800, les fabricants et les fournisseurs de PDS(SR) indiqueront aux utilisateurs la performance de sécurité pour l'équipement (intégrateurs de systèmes de commande, concepteurs de machines et d'usines, etc.). Ceci facilitera l'incorporation d'un PDS(SR) dans un système de commande relatif à la sécurité utilisant les principes de la CEI 61508 ou ses applications sectorielles spécifiques (par exemple la CEI 61511, la CEI 61513, la CEI 62061) ou l'ISO 13849.

La conformité à la présente partie de la CEI 61800 satisfait à toutes les exigences de la CEI 61508 nécessaires à un PDS(SR).

La présente partie de la CEI 61800 ne spécifie pas d'exigences pour:

- l'analyse des dangers et des risques pour une application particulière;
- l'identification des fonctions de sécurité pour cette application;
- l'attribution initiale des SIL pour ces fonctions de sécurité;
- l'équipement entraîné, à l'exception des aménagements de l'interface;
- des phénomènes dangereux secondaires (issus par exemple d'une défaillance d'un processus de production ou de fabrication);
- les considérations de sécurité électrique, thermique et d'énergie, qui sont couvertes par la CEI 61800-5-1;
- le processus de fabrication du PDS(SR);
- la validité des signaux et des commandes du PDS(SR).

NOTE 2 Les exigences en sécurité fonctionnelle d'un PDS(SR) sont dépendantes de l'application et il faut qu'elles soient considérées comme une partie de l'évaluation globale du risque de l'installation. Lorsque le fournisseur du PDS(SR) n'est pas responsable de l'équipement entraîné, le concepteur de l'installation est alors

responsable de l'évaluation du risque et de la spécification des exigences fonctionnelles et d'intégrité de sécurité du PDS(SR).

NOTE 3 Bien que des actions malveillantes puissent avoir un effet sur la sécurité fonctionnelle du PDS(SR), les considérations de sécurité ne sont pas abordées dans la présente norme.

La présente partie de la CEI 61800 s'applique uniquement aux PDS(SR) incorporant des fonctions de sécurité dont le SIL n'est pas supérieur au SIL 3.

La Figure 1 montre les éléments fonctionnels d'un PDS(SR) qui sont considérés dans la présente partie de la CEI 61800.

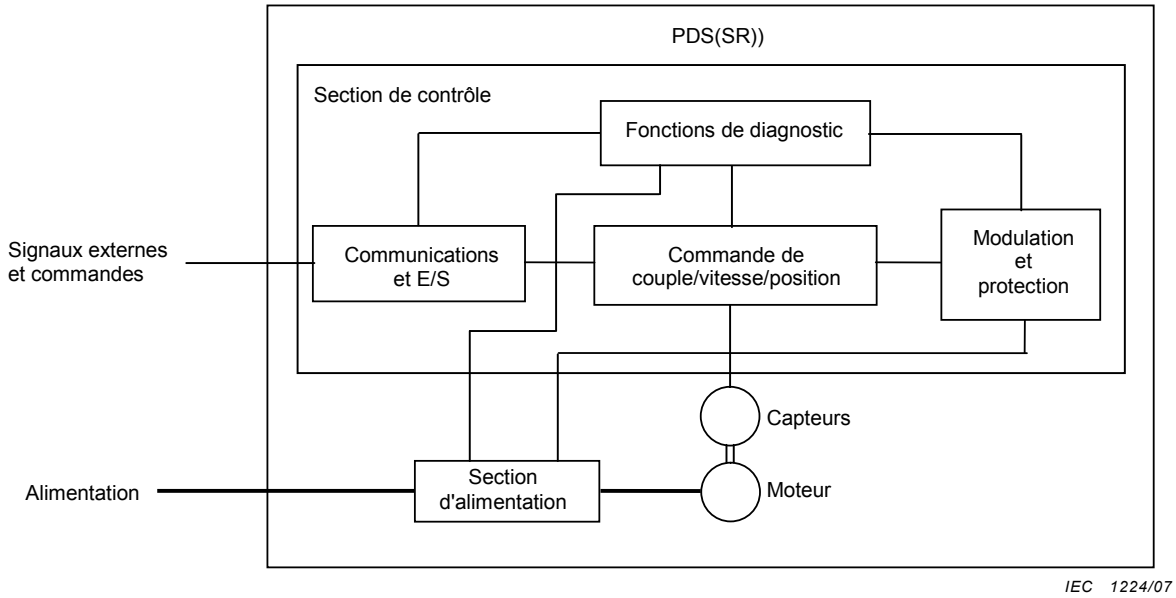

Figure 1 – Éléments fonctionnels d'un PDS(SR)

NOTE La Figure 1 n'est pas une description physique d'un PDS(SR) mais une représentation logique.

2 Références normatives

Les documents de référence suivants sont indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

NOTE 1 Cela ne signifie pas que la conformité à tous les articles des documents de référence soit exigée, mais plutôt que le présent document constitue une référence qui ne peut pas être comprise en l'absence des documents de référence.

NOTE 2 Les références aux diverses parties de la CEI 61508 sont non datées, sauf lorsque des articles spécifiques sont indiqués.

CEI 60204-1, *Sécurité des machines – Équipement électrique des machines – Partie 1: Règles générales*

CEI 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques / électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-1:1998, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 1: Exigences générales*

CEI 61508-2:2000, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-3:1998, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

CEI 61508-5, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité*

CEI 61508-6:2000, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

CEI 61508-7:2000, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

CEI 61800-1, *Entraînements électriques de puissance à vitesse variable – Partie 1: Exigences générales – Spécifications de dimensionnement pour systèmes d'entraînement de puissance à vitesse variable en courant continu et basse tension*

CEI 61800-2, *Entraînements électriques de puissance à vitesse variable – Partie 2: Exigences générales – Spécifications de dimensionnement pour systèmes d'entraînement de puissance à vitesse variable en courant alternatif et basse tension*

CEI 61800-3, *Entraînements électriques de puissance à vitesse variable – Partie 3: Exigences de CEM et méthodes d'essais spécifiques*

CEI 61800-4, *Entraînements électriques de puissance à vitesse variable – Partie 4: Exigences générales – Spécifications de dimensionnement pour systèmes d'entraînements de puissance en courant alternatif de tension supérieure à 1 000 V alternatif et ne dépassant pas 35 kV*

CEI 61800-5-1:2003, *Entraînements électriques de puissance à vitesse variable – Partie 5-1: Exigences de sécurité – Électrique, thermique et énergétique*

CEI 62280 (toutes les parties), *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

NOTE 1 Pour une liste alphabétique des définitions, voir le Tableau 1.

Tableau 1 – Liste alphabétique des définitions

Terme	Numéro de la définition	Terme	Numéro de la définition
capacité SIL	3.21	niveau d'intégrité de sécurité (SIL)	3.18
couverture du diagnostic (DC)	3.3	PDS(SR)	3.11
défaillance dangereuse	3.2	PFH	3.12
défaillance de cause commune	3.1	phénomène dangereux	3.7
défaillance en sécurité	3.14	proportion de défaillances en sécurité (SFF)	3.15
défaillance systématique	3.23	sécurité fonctionnelle	3.6
durée de mission	3.9	sous-système	3.22
fonction de réaction au défaut	3.5	spécification des exigences de sécurité (SRS)	3.20
fonction(s) de sécurité (d'un PDS(SR))	3.16	système relatif à la sécurité	3.19
installation	3.8	essai(s) de diagnostic	3.4
intégrité de sécurité	3.17	essai périodique	3.13
intégrité de sécurité systématique	3.24	validation	3.25
mode de fonctionnement	3.10	vérification	3.26

NOTE 2 Dans l'ensemble de la présente norme internationale, les références aux définitions suivantes sont indiquées en *italique*.

3.1
défaillance de cause commune
défaillance résultant d'un ou de plusieurs événements qui, provoquant des défaillances simultanées de deux ou de plusieurs canaux séparés dans un système multicanal, conduit à la défaillance de la *fonction de sécurité*

[CEI 61508-4:1998, définition 3.6.10]

3.2
défaillance dangereuse
défaillance qui a la potentialité de mettre le *système relatif à la sécurité* dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

[CEI 61508-4:1998, définition 3.6.7]

3.3
couverture du diagnostic
DC (diagnostic coverage)
fraction exprimant la décroissance de la probabilité de défaillance dangereuse du matériel résultant du fonctionnement des *essais de diagnostic* automatiques

[CEI 61508-4:1998, définition 3.8.6]

NOTE 1 Cette couverture peut également être exprimée par le rapport entre la somme des taux de *défaillance dangereuse* λ_{DD} détectés et la somme des taux de *défaillance dangereuse* totaux λ_D: $DC = \Sigma\lambda_{DD}/\Sigma\lambda_D$.

NOTE 2 La *couverture du diagnostic* peut se rapporter à tout ou partie du *système relatif à la sécurité*. Elle peut, par exemple, être disponible pour les capteurs et/ou le système logique et/ou les éléments terminaux.

3.4
essai(s) de diagnostic
essai(s) visant à détecter d'éventuels défauts ou défaillances et à produire des informations ou activités spécifiques au moment de la détection d'un défaut ou d'une défaillance

3.5
fonction de réaction au défaut
fonction initiée au moment de la détection, au sein du PDS(SR), d'un défaut ou d'une défaillance susceptible de causer une perte de la fonction de sécurité. La fonction de réaction au défaut vise à maintenir la sûreté de l'installation ou à prévenir l'émergence de situations dangereuses dans l'installation

3.6
sécurité fonctionnelle
sous-ensemble de la sécurité globale se rapportant à l'EUC (équipement sous contrôle) et au système de commande de l'EUC qui dépend du fonctionnement correct des systèmes E/E/PE (électriques/électroniques/électroniques programmables) relatifs à la sécurité, des systèmes relatifs à la sécurité basés sur une autre technologie et des dispositifs externes de réduction de risque

[CEI 61508-4:1998, définition 3.1.9]

NOTE La présente norme ne prend en considération que les aspects de la définition de la sécurité fonctionnelle qui dépendent du fonctionnement correct du PDS(SR).

3.7
phénomène dangereux
source potentielle de dommage

[définition 3.5 de l'ISO/CEI Guide 51:1999]

NOTE 1 Le terme prend en compte les dangers à court terme envers les personnes (par exemple, les incendies et explosions) ainsi que ceux qui ont un effet à long terme sur la santé d'une personne (par exemple, la libération d'une substance toxique).

NOTE 2 La CEI 61508-4:1998 (modifiée) donne la définition suivante d'une **situation dangereuse**: situation dans laquelle une personne, une propriété ou un environnement est exposé à un ou des phénomènes ou événements dangereux.

3.8
installation
équipement ou équipements incluant au moins le PDS(SR) et l'équipement entraîné

NOTE Le terme «installation» est également utilisé dans la présente norme internationale pour désigner le processus d'installation d'un PDS(SR). Dans ces cas-là, le terme n'apparaît pas en italique.

3.9
durée de mission
durée spécifiée de fonctionnement du PDS(SR), cumulée au cours de l'ensemble de son cycle de vie

3.10
mode de fonctionnement
utilisation prévue d'un système relatif à la sécurité, en rapport avec la fréquence des demandes

[CEI 61508-4:1998, définition 3.5.12, modifiée]

NOTE 1 La CEI 61508 considère les deux modes de fonctionnement suivants:

- **mode de demande faible:** lorsque la fréquence des demandes de fonctionnement sur un système relatif à la sécurité n'est pas plus grande que une par an et au plus égale à deux fois la fréquence des essais périodiques;
- **mode de demande élevée ou mode continu**: lorsque la fréquence des demandes de fonctionnement sur un système relatif à la sécurité est plus grande que une par an ou supérieure à la fréquence des essais périodiques.

En général, le mode de fonctionnement de demande faible est considéré inadapté aux applications PDS(SR). De ce fait, la présente norme considère que les PDS(SR) fonctionnent uniquement dans les modes de demande élevée ou continu.

NOTE 2 Le mode de demande signifie qu'une fonction de sécurité n'est effectuée qu'en cas de demande de transfert de l'installation dans un état spécifié.

NOTE 3 Le mode continu signifie qu'une fonction de sécurité est effectuée en continu. Ainsi, le PDS(SR) contrôle continuellement l'installation et une défaillance (dangereuse) de sa fonction peut entraîner un phénomène dangereux.

3.11
PDS(SR)
entraînement électrique de puissance à vitesse variable, utilisable dans des applications relatives à la sécurité

3.12
PFH
probabilité de panne matérielle dangereuse aléatoire par heure

NOTE Dans la CEI 62061:2005, l'abréviation PFH_D est utilisée.

3.13
essai périodique
essai périodique destiné à détecter les défaillances d'un système relatif à la sécurité de telle sorte que, lorsque nécessaire, le système peut être rétabli dans une condition "comme neuf'' ou dans une condition aussi proche que possible de celle-ci

NOTE En temps normal, les essais périodiques sont effectués dans le but de révéler des défaillances dangereuses qui ne sont pas détectées par les *essais de diagnostic*. L'efficacité d'un essai périodique dépend de jusqu'à quel point le système est rétabli dans une condition «comme neuf». Pour que l'essai soit complètement efficace, il est nécessaire de détecter 100 % des défaillances dangereuses. Bien que dans la pratique il ne soit pas facile d'atteindre 100 % pour tout système autre qu'un système de faible complexité, il convient de garder cet objectif.

[CEI 61508-4:1998, définition 3.8.5, modifiée]

3.14
défaillance en sécurité
défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

(CEI 61508-4:1998, définition 3.6.8)

3.15
proportion de défaillances en sécurité
SFF (safe failure fraction)
rapport entre le taux moyen de défaillance en sécurité, ajouté aux *défaillances dangereuses* détectées d'un sous-système PDS(SR), et le taux total moyen de défaillances de ce sous-système

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

NOTE Voir l'Annexe C de la CEI 61508-2:2000.

3.16
fonction(s) de sécurité (d'un PDS(SR))
fonction(s), selon une performance de sécurité spécifiée, dont tout ou partie est à réaliser par un PDS(SR) et qui vise à maintenir l'état sûr de l'installation ou à prévenir l'émergence de toute condition dangereuse dans l'installation

3.17
intégrité de sécurité
probabilité pour qu'un PDS(SR) exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées

NOTE 1 Plus le niveau d'intégrité de sécurité des PDS(SR) est élevé, plus la probabilité d'une défaillance des PDS(SR) dans l'exécution des fonctions de sécurité requises est faible.

NOTE 2 L'intégrité de sécurité peut ne pas être la même pour chaque fonction de sécurité réalisée par le PDS(SR).

(CEI 61508-4:1998, définition 3.5.2, modifiée)

3.18
niveau d'intégrité de sécurité
SIL (safety integrity level)
niveau discret (parmi quatre possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer (tout ou partie) à un PDS(SR)

NOTE 1 Le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité; le niveau 1 possède le plus bas.

NOTE 2 Le SIL 4 n'est pas pris en compte dans la présente norme car il ne s'applique pas aux exigences de réduction des risques qui sont normalement associées aux PDS(SR). Pour les exigences relatives au SIL 4, voir la CEI 61508.

(CEI 61508-4:1998, définition 3.5.6, modifiée)

3.19
système relatif à la sécurité
système qui, à la fois

– met en œuvre les fonctions de sécurité requises pour atteindre un état de sécurité de l'EUC ou pour maintenir un tel état; et
– est prévu pour atteindre, par lui-même ou grâce à des systèmes E/E/PE relatifs à la sécurité ou des systèmes relatifs à la sécurité basés sur une autre technologie ou des dispositifs externes de réduction de risque, le niveau d'intégrité de sécurité nécessaire à la mise en œuvre des fonctions de sécurité requises

3.20
spécification des exigences de sécurité
SRS (safety requirements specification)
spécification contenant l'ensemble des exigences des fonctions de sécurité que le PDS(SR) est tenu d'assurer

3.21
capacité SIL
SIL maximal pouvant être atteint grâce à la conception d'un PDS(SR), en tenant compte de l'intégrité de sécurité systématique et des contraintes architecturales ayant une influence sur l'intégrité de sécurité du matériel

NOTE Une capacité SIL différente peut être associée à chacune des fonctions de sécurité désignées, qu'un PDS(SR) est censé assurer.

3.22
sous-système
partie de la conception supérieure de l'architecture d'un système relatif à la sécurité; une défaillance de ce sous-système entraîne la défaillance d'une fonction de sécurité

NOTE 1 Un PDS(SR) peut être un sous-système en soi, ou être constitué de plusieurs sous-systèmes distincts qui, une fois assemblés, réalisent la fonction de sécurité attendue. Un sous-système peut disposer de plusieurs canaux.

NOTE 2 Les codeurs, les sections d'alimentation et les sections de commande sont des exemples de sous-systèmes d'un PDS(SR) (voir la Figure 1).