ISA–The Instrumentation, Systems, and Automation Society
Section France

club AUTOMATION

GUIDE D'INTERPRÉTATION ET D'APPLICATION DE LA NORME IEC 61508 ET DES NORMES DÉRIVÉES IEC 61511 (ISA S84.01) ET IEC 62061

Contacts :

Bertrand RICQUE

bertrand.ricque@sagem.com

Jean VIEILLE

jean.vieille@isa-france.org

Version du 8 avril 2005

0 PREAMBULE

Ce document a été préparé conjointement par la cellule de liaison SP84 de la section ISA France et par le groupe de travail « Sécurité » du Club Automation.

0.1 LA SECTION FRANCAISE DE L'ISA

L'**ISA – the Instrumentation, Systems, and Automation Society** est une association a but non lucratif, comprenant environ 39 000 membres dans le monde, couvrant tous les secteurs de l'industrie dans plus de 100 pays.

Son but est de faire progresser la compétence et la carrière de ses membres dans les domaines de l'Instrumentation, des Systèmes et de l'Automation.

La section ISA France assiste ses membres en supportant en France les objectifs de l'ISA par ses actions et ses services dont :

- L'information technique,
- La communication,
- La formation et l'enseignement,
- Un réseau de professionnels,
- Des sites WEB,
- Des revues techniques (InTech),
- Un répertoire de l'instrumentation,
- La rédaction et la publication de normes et de guides.

0.2 LE CLUB AUTOMATION

Le **Club Automation** est une association " loi de 1901 ", créée en 1986, regroupant environ 300 adhérents, exerçant leur activité dans le domaine des automatismes et de l'informatique industrielle.

C'est un groupement de personnes physiques, indépendant des offreurs et des organisations professionnelles.

Le but du Club est de promouvoir, dans l'intérêt de ses membres, l'utilisation et le développement des techniques d'automatisation et de traitement de l'information industrielle.

Cet objectif se situe dans le contexte de l'amélioration des performances des entreprises, notamment par la mise en œuvre des nouvelles technologies de l'information et de la communication dans les systèmes de production.

La productivité, la qualité et surtout la réactivité des activités industrielles et de services sont en effet de plus en plus dépendantes des solutions mises en œuvre dans ces systèmes.

Le Club organise trois fois par an des journées d'information et de débat, au cours desquelles 5 à 6 intervenants invités présentent leurs réflexions et leurs réalisations relatives au thème choisi. La moitié du temps étant dédié aux discussions ,un dialogue ouvert entre tous les participants permet des échanges contradictoires fructueux. Le contenu des débats est enregistré, puis édité.

Le Club organise de plus des visites d'usines, et participe à certains salons professionnels.

Il publie 2 fois par an une " Lettre du club ", édite un annuaire électronique et offre en permanence les informations de son site Web et de son Forum électronique, accessibles à toutes les personnes intéressées.

0.3 POURQUOI CE DOCUMENT

Ce document a été rédigé pour répondre aux attentes des membres des 2 associations en particulier et du marché en général.

Ces attentes ont été constatées à travers les enquêtes réalisées lors des manifestations des 2 associations et à travers les questions posées de manière récurrente à leurs membres.

Ce document est une synthèse des travaux réalisés par :

- Le comité SP84 de l'ISA pour l'IEC 61511,
- Le groupe de travail STSARCES coordonné par l'INERIS pour l'IEC 62061, comprenant :
    - INERIS (Institut National de l'Environnement Industriel et des Risques, France)
    - BIA (Berufsgenossenschaftliches Institut fur Arbeitssicherheit, Allemagne)
    - HSE (Health & Safety Executive, Royaume Uni)
    - INRS (Institut National de Recherche et de Sécurite, France)
    - VTT (Technical Research Centre, Finlande)
    - CETIM (Centre Technique des Industries Mecaniques, France)
    - INSHT (Instituto Nacional de Seguridad e Higiene en el Trabajo, Espagne)
    - JAY (Jay Electronique SA, France)
    - SP (Swedish National Testing and Research Institute, Suède)
    - TUV (TUV Product Service GMBH, Allemagne)
    - SICK AG (SICK AG Safety Systems Division, Allemagne)
- Le Conseil National des Ingénieurs et Scientifiques de France
- Les membres du comité de liaison SP84 de l'ISA France
- Les membres du groupe de travail « sécurité » du Club Automation

Ce document n'a aucune valeur normative ou prescriptive.

Ses objectifs sont :

- D'informer les acteurs de la sécurité fonctionnelle de l'état de la normalisation et de la réglementation dans le domaine,
- Des enjeux techniques, économiques et comerciaux entourant les nouvelles normes,
- De fournir des conseils et des directives pour l'application des nouvelles normes,
- D'approfondir sur les plans techniques et théoriques certains aspects des normes afin de répondre de manière rigoureuse et détaillée à des questions fréquemment posées.

0.4 CLAUSE DE RESPONSABILITE

Ce document est purement informatif et se positionne comme un ouvrage de vulgarisation reprenant les conclusions de diverses publications citées ci-dessus.

Nous rappelons aux lecteurs que ce document ne saurait en aucun cas se substituer au contenu des textes normatifs et réglementaires en vigueur dont nous encourageons la lecture.

Le Club Automation et l'ISA France déclinent toute responsabilité en cas d'inexactitude de ce document avec les normes ou projets de normes sur lesquelles il est basé. Le Club Automation et l'ISA France n'apportent aucune garantie et ne sauraient être tenus responsables en cas d'incident ou de dommage en rapport avec l'utilisation qui peut être faite de ce guide.

1 GENERALITES

1.1 INTRODUCTION

Pourquoi ce guide d'interprétation et de mise en œuvre ?

Le terme « interprétation » peut prêter à confusion. En effet, les normes traitant de sécurité fonctionnelle auxquelles nous faisons référence ne laissent guère de possibilités d'interprétation. Les éléments qui font l'objet de discussions sont plutôt liés à des questions de domaine d'application ou de position réglementaire des textes.

En revanche, les lecteurs de ces normes ressentent rapidement la nécessité d'être guidés, tant les notions qui y sont exposées peuvent paraître complexes, inhabituelles ou difficiles à mettre en œuvre.

L'apparition de la norme IEC 61508 n'est pas récente. Les industriels en ont entendu parler depuis 1996. Elle est une norme française depuis 1999. Les normes filles que ce texte de base a pu générer et continue de générer sont plus récentes mais restent encore très peu connues des acteurs de la sécurité dans la plupart des secteurs industriels.

Ces nouvelles normes s'inscrivent dans une approche globalisée de la sécurité que l'on pourrait comparer au système ISO 9000 pour la qualité, et au système ISO 14000 pour l'environnement.

Rappelons que le système ISO 18000 concernant la sécurité, et du même niveau de prescription, n'a jamais vu le jour en raison de l'opposition de quelques comités nationaux, dont le comité français. Cette norme mort-née a été remplacée par le système référentiel non normatif OSHAS 18000, dont l'adoption est volontaire et qui se répand rapidement, aussi bien parmi des grandes entreprises et des PMI/PME, que parmi des acteurs institutionnels comme les CRAM.

Par rapport au référentiel organisationnel OSHAS 18000, l'approche de l'IEC 61508 est une approche opérationnelle, bien qu'elle inclue à une large échelle des éléments de management qui lui permettent par exemple de s'insérer dans un schéma de réponse à la Directive Européenne Seveso II ou à la Directive Machines.

Le système IEC 61508 s'inscrit également en totale cohérence avec la convergence que l'on peut observer entre différents secteurs industriels. Le rapprochement qu'il crée directement entre les secteurs manufacturier, nucléaire, ferroviaire et des procédés continus trouve des échos dans les secteurs de la pharmacie, de l'aéronautique, du développement de logiciels et même de méthodes de gestion de projets complexes. Il est à ce titre intéressant d'examiner les dernières évolutions de la FDA et du référentiel GAMP en direction d'une approche semi-quantitative de la gestion du risque.

Le déploiement de l'IEC 61508 et de ses normes filles se heurte néanmoins à des difficultés diverses. La disparité des institutions réglementant la sécurité des installations, les intérêts contradictoires des acteurs industriels, les aspects juridiques et le manque de formation sont autant d'obstacles à une diffusion large et rapide de ces normes dont la mise en œuvre n'est déjà plus un choix.

Devant l'apparition de nouvelles normes, apportant des contraintes nouvelles, ou qui semblent nouvelles, les réactions naturelles sont une réticence générale et des tentatives d'éluder les contraintes une à une.

L'intérêt de ce référentiel est pourtant multiple. Système normatif mondial, il facilite les échanges en standardisant les pratiques dans un domaine ou les disparités normatives faisaient office de protectionnisme. En banalisant les produits et les services associés, il contribue à réduire le coût de la sécurité et à améliorer la disponibilité et donc la productivité des installations. En fixant les règles du jeu, il permet une meilleure visibilité sur les coûts des investissements.

L'ambition de ce guide est donc de défricher ce terrain, de donner les clés pour comprendre et déployer ces normes et de répondre à certaines questions plus pointues qui ont été fréquemment posées aux membres du Club Automation et de l'ISA France.

Il ne s'agit donc pas de développer les aspects mathématiques et théoriques que l'on peut facilement découvrir et approfondir à travers la lecture des normes et la formation continue, mais de plutôt de mettre en perspective les aspects pratiques et contextuels du référentiel IEC 61508.

1.2 CONTENU DU GUIDE

Ce document contient 11 chapitres :

- Chapitre 0, "PREAMBULE", présente les modalités d'élaboration du document,
- Chapitre 1, "GENERALITES", présente le contexte et le contenu du document et donne la définition des termes les plus employés,
- Chapitre 2, "LA SECURITE FONCTIONNELLE", rappelle les bases de la sécurité fonctionnelle dans le cadre des systèmes automatisés,
- Chapitre 3, "HISTORIQUE DES NORMES ET DES CULTURES", décrit les différentes cultures industrielles qui ont abouti aux normes récentes,
- Chapitre 4, "CONTEXTE REGLEMENTAIRE", donne la position légale des normes,
- Chapitre 5, "NORMES ACTUELLES ET EN DEVELOPPEMENT", décrit la structure du système de normes IEC 61508,
- Chapitre 6, "IEC 61508 – APPROCHE GENERALE", décrit les principes généraux de l'IEC 61508.
- Chapitre 7, «MISE EN ŒUVRE DE L'IEC 61508 DANS LES PROCEDES CONTINUS ET MANUFACTURIERS », synthétise les éléments importants de l'application du système IEC 61508 aux procéds continus et manufacturiers,
- Chapitre 8, « QUESTIONS FREQUENTES », contient les questions que les acteurs de la sécurité se posent fréquemment,
- Chapitre 9, « CONCLUSION », résume les enseignements à tirer de ce guide
- Chapitre 10, "BIBLIOGRAPHIE", donne des références bibliographiques,

Les réponses aux questions du chapitre 8 sont dans le document joint.

1.3 DEFINITIONS

1.3.1 GLOSSAIRE

ALARP – As Low As Reasonably Possible : Aussi faible que raisonnablement possible, concept britannique au départ pour définir le niveau d'exigence pour un système de sécurité.

GAME – Globalement Au Moins Equivalent : Concept utilisé principalement par le Ministère des Transports français (pour les transports aériens et ferroviaires essentiellement) stipulant qu'un nouveau système de transports ne doit pas induire plus de risque que le précédent.

BPCS – Basic Process Control System : Système de contrôle commande, habituellement à base de SNCC ou d'API contrôlant un processus industriel

EUC – Equipment Under Control : Installation, machine ou équipement commandé par le BPCS et/ou le SIS

E/E/PE – électrique / électronique / électronique programmable

FMEA / AMDE(C) – Failure Mode and Effects Analysis / Analyse des Modes de Défaillance et de leurs Effets (et de leur Criticité)

FPL – Fixed Programming Language : langage de programmation limité à du paramétrage

FSM / SGS – Functional Safety Management system : Système de Gestion de la Sécurité

SRS – Safety Requirements Specification : Exigences de sécurité ou Spécification Régissant la Sécurité

FTR – False Trip Rate : Taux de déclenchement intempestif

FVL – Full Variability Language : Langage de programmation à pleine variabilité (ADA, C++, Pascal, Fortran, IL…)

LVL – Limited Variability Language : Langage de programamtion à variabilité limitée (dans le cadre de l'IEC 61511, 3 des langages automates de l'IEC 61131-3)

Graphes de Markov – méthode de modélisation des états des systèmes complexes permettant de calculer algébriquement ou matriciellement les paramètres de fiabilité d'un système

MOC – Management Of Change : Gestion des modifications

MTBF – Mean Time Between Failure : Temps moyen entre pannes

SFF – Safe Failure Fraction : Taux de pannes sûres (non dangereuses)

PFD – Probability of Failure on Demand : Probabilité de défaillance sur sollicitation

PLC – Programmable Logic Controller : Automate programmable industriel

RRF – Risk Reduction Factor : Facteur de réduction du risque (= 1/PFD)

SIF – Safety Instrumented Function : Fonction instrumentée de sécurité

SIS – Safety Instrumented System : Système instrumenté de sécurité

SIL – Safety Integrity Level : Niveau d'intégrité de sécurité

1.3.2 CONCEPTS DE BASE

Sécurité Fonctionnelle

"Sous-ensemble de la sécurité globale, relatif aux équipements et aux systèmes de contrôle-commande associés, qui dépend du fonctionnement correct de systèmes électriques, électriques, programmables électroniques (E/E/PE) concernés par la sécurité".

Les exemples suivants sont des systèmes E/E/PE concernés par la sécurité :

- un système de déclenchement dans une usine chimique dangereuse,
- un système de signalisation ferroviaire,
- des interverrouillages de protection et un arrêt d'urgence sur une machine,
- un variateur de vitesse utilisé pour contrôler une vitesse en tant que moyen de protection,
- autres systèmes concernés par la sécurité non dédiés à la sécurité.

Fonction de sécurité

- Fonction devant être implémentée dans un système E/E/PE concerné par la sécurité dont le but est d'atteindre ou de maintenir un état sûr pour les équipements contrôlés, dans le cadre d'un évènement dangereux particulier.

Système concerné par la sécurité

Système qui :

- Implémente les fonctions de sécurité nécessaires pour atteindre ou maintenir un état sûr pour les équipements contrôlés, et qui,
- Est destiné à atteindre, seul ou avec d'autres systèmes E/E/PE concernés par la sécurité, l'intégrité de sécurité requise par les fonctions de sécurité.

Intégrité de sécurité

- Probabilité qu'un système concerné par la sécurité exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et dans une période de temps donnée.

Niveau d'intégrité de sécurité (SIL)

Niveau discret parmi quatre niveaux possibles pour la spécification des exigences de sécurité des fonctions de sécurité à assigner aux systèmes concernés par la sécurité :

- 4 Le plus élevé,
- 1 Le plus bas.

Le concept de SIL s'applique donc au système concerné par la sécurité dans son intégralité et pas à un sous-ensemble (par exemple un capteur).

2 LA SECURITE FONCTIONNELLE

Extrats repris de : Functional safety and IEC 61508 A basic guide November 2002 : BSI

2.1 QU'EST-CE QUE LA SECURITE FONCTIONNELLE ?

Nous commençons par une définition de la *sécurité*. C'est l'absence de risque inacceptable, de blessure ou d'atteinte à la santé des personnes, directement ou indirectement, résultant d'un dommage au matériel ou à l'environnement.

La Sécurité Fonctionnelle est le sous-ensemble de la sécurité globale qui dépend du bon fonctionnement d'un système ou d'un équipement en réponse à ses entrées.

Un équipement de protection thermique, utilisant un capteur de température dans les enroulements d'un moteur électrique pour déclencher le moteur avant une surchauffe, est un exemple de sécurité fonctionnelle. En revanche, fournir une isolation pour supporter de hautes températures n'est pas un exemple de sécurité fonctionnelle (bien que ce soit néanmoins un exemple de sécurité et puisse protéger exactement du même risque).

2.2 FONCTIONS DE SECURITE ET SYSTEMES RELATIFS A LA SECURITE

En général, les risques significatifs pour les équipements et les éventuels systèmes de contrôle associés doivent être identifiés par le spécificateur ou le développeur au travers d'une analyse de risque.

L'analyse détermine si la sécurité fonctionnelle est nécessaire pour assurer une protection adéquate contre chaque risque significatif. Si c'est le cas, alors celà doit être pris en compte de manière appropriée lors de la conception.

La sécurité fonctionnelle est simplement une méthode de prise en compte des risques. D'autres moyens de réduction ou d'élimination des risques, tels que la sécurité intégrée dans la conception, sont également d'une importance essentielle.

Le terme "concerné par la sécurité" est utilisé pour décrire des systèmes qui doivent remplir une ou des fonctions spécifques pour garantir que les risques sont maintenus à un niveau acceptable . Ces fonctions sont par définition des fonctions de sécurité. Deux types d'exigences sont nécessaires pour réaliser la sécurité fonctionnelle.

- exigences des fonctions de sécurité (ce que fait la fonction) et
- exigences d'intégrité de la sécurité (la probabilité que la fonction de sécurité soit réalisée correctement).

Les exigences des **fonctions de sécurité** sont dérivées de l'**analyse de risque** et les exigences d'**intégrité de la sécurité** sont dérivées de l'**évaluation des risques**. Plus le niveau d'intégrité de la sécurité est élevé, plus la probabilité d'une panne dangereuse est faible.

Tout système, réalisé dans une technologie quelconque, qui remplit des fonctions de sécurité est un système concerné par la sécurité. Le système concerné par la sécurité peut être séparé d'un système de contrôle commande ou peut être inclus dans ce dernier. Des niveaux d'intégrité de la sécurité élevés nécessitent une plus grande rigueur dans l'ingénierie d'un système concerné par la sécurité.

2.3 EXEMPLES DE SECURITE FONCTIONNELLE

Considérons une machine avec une lame rotative protégée par un couvercle solide suspendu. L'accès à la lame pour le nettoyage périodique se fait en soulevant le couvercle. Le couvercle est interverrouillé de manière à ce qu'un circuit électrique désalimente le moteur et déclenche un frein dès que le couvercle est soulevé. De cette manière, la lame est arrêtée avant de pouvoir blesser la main de l'opérateur.

Pour garantir l'obtention de la sécurité, il est nécessaire d'utiliser l'analyse de risque et l'évaluation des risques.

1. L'analyse de risque identifie les risques associés au nettoyage de la lame. Dans le cas de cette machine, elle peut montrer qu'il ne devrait pas être possible de soulever le couvercle de 5mm sans que le frein soit activé et ait arrêté la lame. Une analyse plus approfondie pourrait montrer que le délai pour arrêter la lame doit être inférieur ou égal à une seconde. Ces deux aspects décrivent la fonction de sécurité.
2. L'évaluation des risques détermine les exigences de performances de la fonction de sécurité. Le but est de s'assurer que l'intégrité de la sécurité de la fonction de sécurité est suffisante pour garantir que personne n'est exposé à un risque inacceptable associé à cet évènement dangereux.

L'intégrité de la sécurité de la fonction de sécurité dépend de tous les équipements nécessaires pour que la fonction de sécurité soit réalisée correctement, c'est-à-dire l'interverrouillage, le circuit électrique associé, le moteur et le système de freinage.

La lésion résultant d'une panne de la fonction de sécurité pourrait être une amputation de la main de l'opérateur ou juste une contusion. Le risque dépend aussi de la fréquence d'ouverture du couvercle, qui peut être plusieurs fois par jour ou bien une fois par an. Le niveau d'exigence d'intégrité de la sécurité augmente avec la gravité de la blessure et la fréquence d'exposition au danger.

En résumé :

- L'analyse de risque identifie ce qui doit être fait pour éviter les évènements dangereux associés avec la lame.
- L'évaluation des risques donne l'intégrité de la sécurité exigée du système pour que le risque devienne acceptable.

Ces deux éléments, "quelle fonction de sécurité doit être réalisée" - les exigences des fonctions de sécurité - et "quel degré de certitude que la fonction de sécurité sera réalisée est nécessaire" - les exigences d'intégrité de la sécurité - sont les bases de la sécurité fonctionnelle.

2.4 OBTENIR LA SECURITE FONCTIONNELLE

Les fonctions de sécurité sont de plus en plus remplies par des systèmes électriques, électroniques ou électroniques programmables. Ces systèmes sont habituellement complexes, ce qui a pour conséquence de rendre pratiquement impossible la détermination de chaque mode de défaillance ou le test de tous les comportements possibles. Il est difficile de prédire la performance de sécurité, bien que les essais restent essentiels.

Le défi est de concevoir le système d'une manière qui évite les pannes dangereuses et qui les contrôle lorsqu'elles surviennent. Les pannes dangereuses peuvent survenir en conséquence de :

- spécifications du système incorrectes, pour le matériel ou pour le logiciel,
- ommissions dans la spécification des exigences de sécurité (par exemple le développement de toutes les fonctions de sécurité pertinentes dans tous les modes d'exploitation),
- panne matérielle aléatoire des mécanismes,

- panne matérielle systématique des mécanismes,
- erreurs sur le logiciel,
- pannes de mode commun,
- erreur humaine,
- influence de l'environnement (par exemple électromagnétique, température, phénomène mécanique),
- perturbations de la tension d'alimentation du système (par exemple perte d'alimentation, sous-tension, reconnection de l'alimentation).

La norme IEC 61508 contient les exigences nécessaires et suffisantes pour minimiser ces pannes.

3 HISTORIQUE DES NORMES ET DES CULTURES

3.1 USA

La culture industrielle des Etats-Unis a longtemps laissé l'initiative de l'organisation de la sécurité au travail aux entreprises, aux secteurs industriels et aux syndicats professionnels ou de travailleurs.

Il en résulte des habitudes et des textes dont la variété est comparable à ce que l'on pouvait trouver en France avant l'harmonisation européenne.

Ces réglementations sont soit d'ordre légal et peuvent alors être trouvées dans le Code of Federal Regulations (CFR). Le secteur Manufacturier est par exemple régit par la série 29CFRxxx, alors que la pharmacie est subordonnée à la 21CFRxxx. Il en va de même pour les secteurs nucléaires, aérien et ferroviaires.

Les procédés continus sont eux soumis à une double contrainte. L'hygiène et la sécurité au travail sont réglementés par l'OHSA alors que les aspects techniques étaient jusqu'à présent soumis à la norme ANSI/ISA S84 – 1996. Cette norme était l'héritage d'une approche de l'analyse quantitative du risque et d'une réponse adaptée en termes de performances, sans aller jusqu'à devoir prouver la réalité de ces performances. L'arrivée de l'IEC 61508 et de l'IEC 61511 ont bouleversé ce paysage. Les américains ont alors décidé de réviser totalement la S84.01 pour produire la S84.01 version 2000 qui reprend intégralement la norme IEC 61511 et ajoute des clauses permettant d'intégrer l'existant et le retour d'expérience. On peut noter à travers cette démarche, le souci des organisations de normalisation américaines de ne pas se mettre à l'écart des textes mondiaux, l'application de l'IEC 61511 n'étant pas évidente pour eux au départ.

Enfin, on ne note toujours pas de rapprochement entre les secteurs manufacturiers, très peu normalisés, et des procédés continus.

3.2 ALLEMAGNE

L'Allemagne a une longue tradition d'une approche prescriptive dans le domaine de la sécurité ainsi que de niveaux d'exigences particulièrement élevés. Cette approche a été concrétisée dans le passé par les normes DIN VDE 0801 et DIN 19250 par exemple, ainsi que par les travaux et les textes NAMUR.

L'approche prescriptive tend à transférer le résultat en matière de sécurité sur la qualité des produits utilisés. La charge de travail se reporte donc essentiellement sur les concepteurs des produits et sur les organismes de certification tels que les TÜV bien connus.

A travers cette approche, l'Allemagne a développé une solide culture de l'analyse semi-quantitative du risque et de la certification de produits qu'elle cherche à exploiter aujourd'hui. L'IEC 61511 a subi des influences significatives de la part de ces approches comme nous le décrirons plus loin dans le document.

3.3 FRANCE

3.3.1 Culture

La culture française est une culture déterministe et prescriptive. Ceci signifie qu'il n'y a pas de gradation ni de progressivité dans le risque. Soit le risque est présent, soit il est éliminé. Cette approche est cohérente avec une répugnance naturelle à l'appréhension du risque. Schématiquement, le citoyen français attend de l'Etat qu'il fasse le nécessaire pour qu'il ne subisse pas de risque. Ceci conduit à :

- ne pas parler des risques,
- rechercher des solutions techniques qui déchargent l'individu ou les organisations au maximum de la recherche et de la responsabilité de la réponse au risque.

Dans le cadre industriel des années 60 et 70, les moyens de recherche et de développement dans le domaine de la sécurité ont été concentrées dans de grandes organisations de l'industrie française (industrie automobile, EDF, CEA, SNCF, INRS, INERIS, etc…).

Les normes qui ont alors été publiées étaient le reflet des solutions trouvées et appliquées par ces organisations.

On peut déjà noter une différence entre les industries des procédés continus, très vite internationales et plus perméables aux normes étrangères souvent plus avancées (chimie, pétrole) et le secteur manufacturier, plus porté à développer des solutions nationales.

Les nouvelles normes, issues d'une tradition plus anglo-saxonne de recheche de la performance, heurtent de plein fouet cette culture.

Là où il s'agissait d'appliquer des recommandations, de choisir des produits sur catalogue en faisant confiance au travail de R&D d'agences publiques et de grands constructeurs de composants, il faut maintenant s'organiser, analyser, évaluer, faire des calculs et finalement prouver la pertinence et la justesse de son travail.

Nous reprenons et commentons ci-dessous des extraits des propositions d'action remises par le Conseil National des Ingénieurs et Scientifiques de France le 23 janvier 2002 au Ministre de l'Environnement et de l'Aménagement du Territoire.

Extraits repris de : CNISF : propositions d'action au Ministre de l'Environnement et de l'Aménagement du Territoire 23 janvier 2002 (extraits)

La sécurisation maximale des sites industriels et une identification aussi précise que possible des risques qu'ils sont susceptibles de faire courir à l'extérieur constituent un objectif essentiel. Les principales pistes d'action et de réflexions proposées sont les suivantes :

- La mise en œuvre de la directive SEVESO II implique que toutes les études de danger existantes soient révisées au plus vite.
- La catastrophe de Toulouse incite cependant à penser que leur méthodologie actuelle n'est pas satisfaisante. Certains spécialistes estiment que la France a pris du retard dans ce domaine par rapport à certains pays étrangers. Il serait donc souhaitable de la revoir en profondeur et de mobiliser sur ce thème toute la communauté des spécialistes, qu'ils exercent dans l'entreprise, dans l'administration ou dans la recherche, en s'inspirant des meilleurs exemples étrangers.

Note : Le Club Automation et l'ISA France participent à travers leurs manifestations et ce document à cette mobilisation et à la diffusion du savoir faire de nos collègues étrangers.

- Une importante différence entre l'approche française et celle de certains pays réputés plus avancés est que la première est déterministe alors qu'elle est probabiliste chez les seconds et prend en compte plusieurs scénarios avec pour objectif la répartition spatiale du couple gravité/probabilité et non une frontière stricte entre zone à risque et zone sans risque. Cette orientation devrait être prise en considération dans ce réexamen.
- Il faut avoir conscience que cette approche conduit à admettre et à définir un risque résiduel accepté. Les citoyens, qui exigent de l'Etat une garantie absolue de sécurité, et le système judiciaire y sont-ils prêts ? Dans le contexte actuel de judiciarisation croissante, c'est une question d'une extrême importance pour les ingénieurs aussi bien que pour les chefs d'entreprises et les décideurs publics.
- Si c'est bien aux entreprises de conduire les études de danger, car elles seules ont la connaissance de détail des risques liés aux procédés et aux produits - les PME pourraient trouver avantage à mutualiser les moyens d'étude -il serait hautement souhaitable d'imposer que toute étude de danger soit accompagnée d'une tierce expertise, indépendante et habilitée par les pouvoirs publics à le faire, destinée à éclairer à la fois l'entreprise, son CHSCT, les organismes de contrôle, la CLI et les élus.
- L'administration n'a pas vocation à réaliser elle-même ces tierces expertises car elles demandent un haut niveau de spécialisation dans de nombreux domaines et parce que l'administration ne serait plus alors à même d'assumer son rôle fondamental d'instance de contrôle et de recours, avec l'appui de l'INERIS pour les cas les plus difficiles.
- La généralisation de la pratique de la tierce expertise suppose qu'il y ait une capacité d'expertise privée suffisante, ce qui n'est probablement pas le cas actuellement, même en prenant en compte l'expertise internationale pour les cas les plus délicats. Le basculement vers de nouvelles formes d'organisation ne pourra donc pas être instantané. Il suppose un sensible renforcement de la capacité de formation spécialisée dans le risque industriel, actuellement très déficitaire.

La directive Seveso II insiste sur la notion de gestion de la sécurité et préconise la prise en compte d'un certain nombre de principes: transparence, formalisation et obligation de rendre compte. Les propositions et avis reçus conduisent aux commentaires suivants :

- Le management de la sécurité ne se conçoit pas sans l'appropriation d'un état d'esprit sécurité par tous les intervenants des différentes équipes de travail. C'est à cela que doivent contribuer les efforts conjoints du management et du CHSCT, travaillant en totale transparence.
- Les principes énoncés par les normes ISO 9000 en matière de gestion de la qualité et par la norme ISO 14001 pour la gestion de l'environnement constituent un cadre conceptuel dont l'intérêt est maintenant reconnu par tous. Les unes et les autres ne traitent cependant que de façon marginale des questions de sécurité. Il serait essentiel et urgent qu'un cadre similaire soit mis au point pour la sécurité puis rendu obligatoire pour les usines à risque, sous le contrôle des pouvoirs publics. qui devront avoir accès aux comptes-rendus écrits et aux conclusions des audits périodiques imposés par ces procédures.

Note : Ce cadre est justement l'objet du référentiel OSHAS 18000 pour la partie organisationnelle et des normes de la série IEC 61508 pour la partie technique concernant les secteurs industriels et ferroviaires. Il est d'ailleurs intéressant de se demander pourquoi la Directive Seveso II n'a pas de normes harmonisées associées.

- Dans les industries à risque, l'externalisation d'un nombre croissant de tâches (production, entretien et maintenance, gardiennage, logistique, transports...) suscite des interrogations. La juxtaposition de systèmes de management distincts et la présence sur le site de personnels occasionnels peut, sans mesures appropriées, être génératrice de risques.

Note : Des référentiels comme le MASE prennent cet aspect particulier en compte de manière efficace.

3.3.2 Intérêts en présence

Les cinq groupes d'acteurs présents sur le marché français sont :

- Les **institutions** représentant l'intérêt des **citoyens**,
- Les **constructeurs** de **composants** pour les systèmes de sécurité (capteurs, actionneurs, solveurs logiques et logiciels),
- Les **intégrateurs** de **systèmes** de sécurité, se présentant souvent comme les intermédiaires entre les constructeurs et les utilisateurs finaux, ainsi que les **prestataires de services**,
- Les **utilisateurs finaux** propriétaires et responsables des installations ou machines dangereuses,
- Les **organismes tiers** de contrôle et de certification.

Les intérêts de ces cinq groupes d'acteurs sont rarement convergents comme le décrit le tableau ci-dessous :

	Forces	Faiblesses	Opportunités	Menaces
Institutions	Capacité à interdire l'exploitation d'unités de production	Compétence des inspecteurs, Budgets des organismes de contrôle, Sensibilité au lobbying des industriels (chantage à l'emploi).	Rationaliser la maîtrise des risques indépendamment des secteurs, Communiquer sur une meilleure maîtrise des risques.	Difficulté à inculquer la culture du risque aux citoyens, Difficulté à être crédible dans les prescriptions techniques, Décorrélation entre l'attente de l'obligation de résultat imposée aux industriels et l'obligation de moyens prescrites par la réglementation.
Constructeurs	Expérience sur les produits, Capacité de R&D, Maîtrise des données sur les produits sans lesquelles aucune évaluation des performances n'est possible.	Offre composants et certification face à des normes systèmes et performances, La vente est décorrélée du produit. Pour vendre il faut s'engager dans l'analyse de risque sur un procédé / machine donné.	Marché en développement, la compétence "sécurité" permet d'accrocher de nouveaux clients, Vendre plus cher des produits ordinaires aux bonnes performances.	Les données nécessaires aux calculs permettent de comparer des produits, Surcoût sur la vente.
Intégrateurs	Connaissance des procédés, Présence chez le client, Connaissance des composants, Niveaux de prix.	Méthodes d'analyse du risque, Outils d'ingénierie, Savoir-faire en développement de logiciels critiques, Ressources humaines.	Prise de nouveaux marchés	Prise des marchés directement par les constructeurs, Prise des marchés par les prestataires, Surcoûts sur des niveaux de prix déjà tendus.
Prestataires de services spécialisés	Connaissance des méthodes d'analyse du risque, Outils associés, Développement de logiciels critiques, Ressources humaines.	Ingénierie des systèmes, Mise en œuvre des composants, Présence limitée en dehors des secteurs aéronautique, nucléaire et défense, Niveaux de prix	Prise de nouveaux marchés	Prise des marchés directement par les constructeurs, Prise des marchés par les intégrateurs.
Utilisateurs finaux	Connaissance des procédés.	Capacité à prescrire et à évaluer les systèmes.	Les analyses de risques permettent souvent au passage des améliorations de la productivité des procédés.	Surcoûts.
Organismes de certification	Point de passage obligé.	Compétence technique sur les nouvelles normes embryonnaire.	Prise de nouveaux marchés	Surcoûts, Risque de prise de responsabilité, Marché hautement concurrentiel.

3.3.3 Evolution à moyen terme

L'approche des nouvelles normes correspond à une tendance lourde dans l'industrie. Cette tendance est la convergence des approches d'analyse du risque, d'estimation et d'évaluation du risque et de réponse au risque sur des bases d'obligation de performances et non pas sur la base de la prescription de solutions toutes faites.

On peut notamment noter les convergences suivantes :

- La nouvelle approche « gestion du risque » de la FDA, qui apparaît révolutionnaire ou tout au moins bouleversante pour l'industrie pharmaceutique, ne fait que reprendre les principes de base de l'approche IEC 61508,
- Les secteurs de l'aéronautique et de la défense s'intéressent maintenant à la classification des systèmes de sécurité en niveaux SIL, mais se heurtent aux faiblesses de l'approche IEC 61508 dans les domaines du logiciel,
- Les secteurs des industries intermédiaires, qui ont des aspects tant manufacturiers que continus comme les industries pharmaceutiques ou agro-alimentaires, voient leurs contraintes consolidées (une machine dans un process est traitée de manière cohérente avec le process).

La pluralité des institutions ne simplifie pas la mise en œuvre des nouvelles normes :

- La Direction des Relations du Travail (DRT) (Ministère de l'Emploi, du Travail et de la Cohésion Sociale) à travers les Directions Départementales du Travail, de l'Emploi et de la Formation Professionnelle (DDTEFP) s'intéresse au respect de la Directive Machine,
- La Direction de la Prévention des Pollutions et des Risques (DPPR) (Ministère de l'Ecologie et du Développement Durable) à travers le Bureau des Risques Technologiques et des Industries Chimiques et Pétrolières (BRTICP) et des Diections Régionales de l'Industrie, de la Recherche et de l'Environnement (DRIRE) s'intéresse à l'application de la Directive Sevso II,
- La Caisse Nationale d'Assurance Maladie (CNAM),
- L'INERIS est sous tutelle de la DPPR,
- L'INRS est sous-tutelle de la CNAM avec une coordination avec la DRT.

On peut s'attendre à une fusion progressive de certaines de ces organisations dans une agence unique de la sécurité. Ceci simplifierait la tâche des industriels

4 CONTEXTE REGLEMENTAIRE

Nous fournissons ci-dessous un rappel synthétique du contenu des principales directives européennes et réglementations ayant un lien direct ou indirect avec la sécurité fonctionnelle.

Il est intéressant de noter la convergence technique entre tous ces textes, notamment dans les domaines du logiciel et de l'analyse de risque.

4.1 DIRECTIVE SEVESO II

La directive européenne 82/501/CEE du 24 juin 1982, nommée Seveso I, porte sur la prévention des accidents majeurs dans les installations industrielles. Elle prévoit la mise en place par les Etats d'un dispositif de maîtrise des risques présentés par les industries telles que la chimie, les raffineries, les stockages de produits toxiques ou de gaz liquéfiés susceptibles d'être à l'origine d'incendies, d'explosions ou de relâchements de gaz toxiques.

En France, le dispositif législatif et réglementaire de l'environnement répondait aux exigences de la directive. Ainsi ces exigences se retrouvaient déjà dans les dispositions des loi de 1976 et décret de 1977 modifiés relatifs aux installations classées pour la protection de l'environnement. La tâche de transposition des textes a donc été d'autant facilitée. Par ailleurs, la directive imposait aux Etats membres de mettre en place un contrôle des établissements à risque, incluant le respect des exigences précédemment citées. Le système d'inspection des installations classées répondait effectivement à ces exigences.

On recense de l'ordre de 400 établissements à risques dits " Seveso " en France. Avec la directive SEVESO 2 leur nombre devrait augmenter modérément. Dans les années qui ont suivi la parution de la directive SEVESO, les inspecteurs ont veillé à ce que chacun des établissements déjà existants fournisse, avant juin 1994, une étude des dangers identifiant les risques de l'activité et proposant des moyens de le maîtriser. 720 études avaient été fournies en 1996 (un établissement comportant plusieurs installations).

La directive « Seveso II » a remplacé la directive 82/501/CEE, Des changements importants ont été effectués et de nouveaux concepts ont été introduits. Elle met l'accent sur la protection de l'environnement en introduisant pour la première fois dans son champ d'application les substances considérées comme dangereuses pour l'environnement (notamment les substances aquatoxiques). De nouvelles exigences portant notamment sur les systèmes de gestion de la sécurité, sur les plans d'urgence, sur l'aménagement du territoire ou sur le renforcement des dispositions relatives aux inspections ou à l'information du public ont été incluses.

Champ d'application

Le champ d'application de la directive est à la fois élargi et simplifié. Elle s'applique à tout établissement où des substances dangereuses sont présentes ou sont susceptibles d'être produites en cas d'accident. La liste des substances désignées a été réduite de 180 à 50 substances mais elle est assortie d'une liste de catégories de substances, ce qui conduit, dans la pratique, à élargir le champ d'application.

La directive 2003/105/CE a étendu le champ d'application de la directive « Seveso II » de manière à inclure les opérations de traitement et de stockage des matières minérales réalisées par des industries extractives et impliquant la présence de substances dangereuses, ainsi que les installations d'élimination de terres stériles utilisées dans ces opérations.

Sont exclus du champ d'application de la directive:

- les installations militaires,
- les dangers liés aux rayonnements ionisants,
- les transports de substances dangereuses par route, rail, air et voies navigables,
- les transports de substances dangereuses par pipelines à l'extérieur des établissements visés par la présente directive,
- les décharges de déchets.

La directive 96/82/CE a été adoptée en anticipant l'approbation, par la Communauté, de la convention de la Commission économique des Nations Unies pour l'Europe sur les effets transfrontières des accidents industriels. Cette approbation est survenue le 23 mars 1998, par la décision du Conseil concernant la conclusion de la convention sur les effets transfrontières des accidents industriels (décision 98/685/CE). La directive 96/82/CE constitue l'instrument pour transposer les obligations de la Convention au niveau communautaire.

À la suite des accidents industriels qui se sont produits à Baia Mare, en Roumanie, en janvier 2000 (déversement de cyanure dans la Tisza), à Enschede, aux Pays-Bas, en mai 2000 (explosion dans un entrepôt pyrotechnique) et à Toulouse, en France, en septembre 2001 (explosion dans une usine d'engrais), le Parlement et le Conseil ont adopté la directive 2003/105/CE. Celle-ci modifie la directive « Seveso II » afin, notamment :

- d'élargir le champ d'application de la directive « Seveso II »,
- d'améliorer la définition des produits pyrotechniques et des explosifs,
- d'inclure les matières rejetées au cours du processus de fabrication ou renvoyées au fabricant (matières « off-specs ») dans les catégories de nitrate d'ammonium et d'engrais à base de nitrate d'ammonium couvertes par la directive « Seveso II ».

On compte, en moyenne, un inspecteur de la DRIRE par site Seveso dans une région comparable à la Haute-Normandie, sachant que l'activité de l'inspecteur ne se limite pas au contrôle des établissements Seveso.

Le contexte industriel de cette directive est celui des industries des procédés continus. Ces industries possèdent déjà une culture de la sécurité et des systèmes de sécurité. Les normes existantes, dans les secteurs de la pétrochimie et de l'énergie sont très homogènes et ont beaucoup inspiré le corpus IEC 61508. Ce dernier point lui est d'ailleurs amplement reproché par les industries manufacturières.

La Directive n'est pas prescriptive sur le plan technique mais organisationnelle.

Les solutions techniques et donc le choix des normes à appliquer sont le problème des industriels. Ceci décrit assez précisément la position actuelle des DRIRE.

En l'absence de normes harmonisées, les normes de référence qui s'imposent en priorité sont les normes EN et donc l'IEC 61511 (voir chapitre 5.2.1).

4.2 DIRECTIVE MACHINES

L'appellation " machines " s'applique à un ensemble de pièces ou d'organes liés entre eux dont au moins un est mobile et, le cas échéant, d'actionneurs, de circuits de commande et de puissance réunis de façon solidaire en vue d'une application définie, notamment pour la transformation, le traitement, le déplacement et le conditionnement d'un matériau.

Est également considéré comme « machine » un ensemble de machines qui, afin de concourir à un même résultat, sont disposées et commandées de manière à être solidaires dans leur fonctionnement.

Est également considéré comme machine un équipement interchangeable modifiant la fonction d'une machine, destiné à être assemblé à une machine par l'opérateur lui-même, dans la mesure où cet équipement n'est pas une pièce de rechange ou un outil.

Sont exclues :

- les machines dont la seule source d'énergie est la force humaine (pinces, ciseaux),
- les machines à usage médical, les tracteurs agricoles et forestiers, les matériels spécifiques pour fêtes foraines, les appareils à pression, les armes à feu, les appareils à câbles pour le transport des personnes (funiculaires, téléphériques, etc.), les ascenseurs.

Le contexte industriel de cette directive est essentielelment celui des industries manufacturières. Ces industries n'ont au départ pas une culture homogène de la sécurité, due à des normes éparses par secteur d'activité.

La directive est **prescriptive**. C'est à dire qu'elle préconise et impose des normes harmonisées qui elles-mêmes décrivent des solutions techniques valant présomption de conformité.

4.3 AUTRES DIRECTIVES

On peut remarquer la grande cohérence des Directives entre elles et leur homogénéité technique.

4.3.1 Directive Equipements sous Pression

La directive porte sur les équipements sous pression et les ensembles dont la pression maximale admissible est supérieure à 0,5 bar.

Elle détermine les objectifs ou "exigences essentielles" auxquels doivent répondre, lors de leur fabrication et avant leur mise sur le marché, les équipements susmentionnés ; ces exigences remplacent les dispositions nationales correspondantes.

Des normes européennes harmonisées sont élaborées sur la base des exigences essentielles par les organismes européens de normalisation. Ces normes seront publiées au Journal officiel de l'Union européenne.

Les procédures d'évaluation se font en fonction du danger inhérent aux équipements sous pression. Chaque catégorie d'équipements sous pression est assortie d'une procédure adéquate ou d'un choix entre plusieurs procédures adéquates. Quant aux ensembles, leur conformité fait l'objet d'une procédure globale d'évaluation.

Une période transitoire (29 novembre 1999 - 29 mai 2002) a été accordée pendant laquelle les États membres autorisaient:

- la mise sur le marché des équipements et ensembles sous pression conformes aux réglementations en vigueur sur leur territoire,
- la mise en service des ces équipements ou ensembles au-delà de cette date.

4.3.2 Directive ATEX

Cette directive s'applique aux appareils et aux systèmes de protection destinés à être utilisés en atmosphères explosibles. Elle concerne également les atmosphères explosibles formées par des gaz, vapeurs et poussières combustibles.

Les dispositifs de sécurité, de contrôle et de réglage destinés à être utilisés en dehors des atmosphères explosibles et qui contribuent au fonctionnement sûr des appareils et des systèmes de protection, au regard des risques d'explosion, entrent également dans le champ d'application de la directive.

Le champ d'application de cette directive est très vaste, puisqu'il couvre tous les équipements, qu'ils soient électriques, mécaniques, hydrauliques, ou pneumatiques.

Les procédures d'évaluation de la conformité dépendent de la nature du matériel (électrique, thermique ou mécanique ...) et de l'emplacement (zone à risques d'explosion) pour lequel il est destiné.

4.3.3 Directive Equipements Médicaux

La Directive 93/42/CEE du Conseil, du 14 juin 1993, relative aux dispositifs médicaux est obligatoire d'application depuis le 14 juin 1998. Les 22 articles de la directive 93/42 statuent sur :

- La classification des produits déterminés par rapport au risque encouru par le patient,
- La conformité aux exigences essentielles,
- La référence à un système qualité (de la naissance du produit à la mise sur le marché),
- Le maintien des dossiers techniques à la disposition des autorités compétentes,
- Les investigations cliniques,
- La mise en place d'un système de vigilance.

La directive définit la notion de "dispositif médical" comme "Tout instrument, appareil, équipement, matière ou autre article, utilisé seul ou en association, y compris le logiciel nécessaire pour le bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins :

- de diagnostic, de prévention, de contrôle, de traitement ou d'atténuation d'une maladie,
- de diagnostic, de contrôle, de traitement, d'atténuation ou de compensation d'une blessure ou d'un handicap,
- d'étude ou de remplacement ou modification de l'anatomie ou d'un processus physiologique,
- de maîtriser la conception,
- et dont l'action voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens."

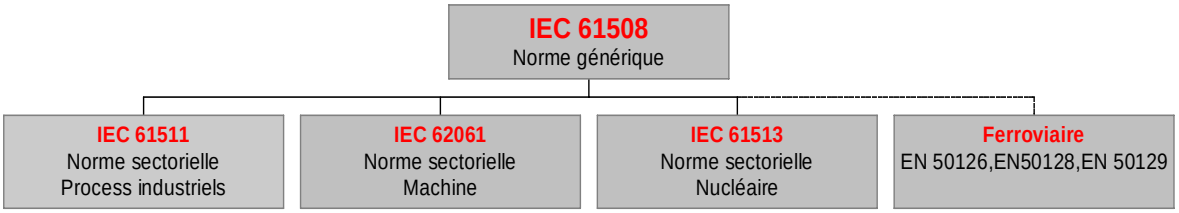
La directive européenne organise les dispositifs médicaux en 4 classes définies selon la destination, la durée, les risques encourus par le patient qui permettent de déterminer la classe d'un produit.

Quelle que soit la classe, les dispositifs médicaux doivent satisfaire certaines exigences qui couvrent tous les aspects concernant la sécurité et la fonctionnalité d'un dispositif dont notamment les conditions d'utilisation, la fonctionnalité du dispositif, l'évaluation et l'acceptabilité des risques, l'évaluation des performances....

5 NORMES ACTUELLES ET EN DEVELOPPEMENT

5.1 SYSTEME REFERENTIEL IEC 61508

Le système IEC 61508 est constitué d'une norme générique et de normes filles par secteur d'activité.



Extraits repris de : Functional safety and IEC 61508 A basic guide November 2002 : BSI

5.1.1 L'IEC 61508 base pour d'autres normes

Les parties 1, 2, 3 et 4 de l'IEC 61508 sont les publications de base de l'IEC dans le domaine de la sécurité fonctionnelle. Une des responsabilités des comités techniques de l'IEC est de baser, chaque fois que cela est réalisable, la rédaction de leurs propres normes sectorielles ou produit sur ces parties de la norme IEC 61508 dès que des systèmes E/E/PE concernés par la sécurité font partie de leur périmètre.

L'IEC 61508 est la base d'autres normes sectorielles (ex : machines, procédés continus, ferroviaire, nucléaire) ou de produits (ex : variateurs de vitesse). Elle influence donc le développement des systèmes E/E/PE et des produits concernés par la sécurité à travers tous les secteurs. La rédaction de normes sectorielles est facilitée par la distinction faite entre l'application du système E/E/PE concerné par la sécurité (qui dépend souvent du secteur), et les spécifications détaillées de conception (qui sont la plupart du temps indépendantes du secteur).

Les spécifications indépendantes des secteurs se situent entre l'allocation des prescriptions de sécurité, et les phases d'installation et de réception du cycle de vie de sécurité complet. Les normes sectorielles ou produit font habituellement référence à ces spécifications plutôt que de les répéter. En conséquence, la plupart des utilisateurs ont systématiquement besoin de l'IEC 61508.

Le statut de norme de base de l'IEC 61508 ne s'applique pas dans le contexte de systèmes E/E/PE concernés par la sécurité de faible complexité. Ces derniers sont des systèmes E/E/PE concernés par la sécurité pour lesquelles le mode de défaillance de chaque composant est clairement défini et pour lesquels le comportement du système peut être totalement déterminé dans le cas d'une défaillance. Un exemple peut être un système comprenant un ou plusieurs fin de course, reliés à un ou plusieurs contacteurs pour désalimenter un moteur électrique, éventuellement au travers de relais électromécaniques.

Attention toutefois à ne pas utiliser abusivement cette possibilité dans le but d'éviter d'appliquer la norme. Il faut de toute façon être capable de prouver ce que l'on avance.

5.1.2 L'IEC 61508 - norme auto-portante

Toutes les parties de l'IEC 61508 sont susceptibles d'être directement utilisée par l'industrie en tant que publications "autoportantes". Ceci permet d'utiliser la norme pour :

- disposer d'exigences génériques pour des systèmes E/E/PE concernés par la sécurité lorsqu'il n'existe aucune norme sectorielle ou produit, ou lorsqu'elles ne sont pas appropriées,
- les constructeurs de composants ou de sous-systèmes E/E/PE dans tous les secteurs (par exemple, matériel et logiciel pour capteurs, actionneurs intelligents, contrôleurs programmables),
- les constructeurs / intégrateurs de systèmes pour atteindre les exigences des systèmes E/E/PE concernés par la sécurité,
- les utilisateurs pour spécifier les exigences en termes de fonctions de sécurité à réaliser ainsi que des performances de ces fonctions de sécurité,
- faciliter la maintenance des systèmes E/E/PE concernés par la sécurité au niveau d'intégrité de la sécurité "tel que construit",
- fournir un cadre technique pour des services d'évaluation et de certification,
- disposer d'une base pour réaliser des évaluations des activités du cycle de vie de la sécurité

5.1.3 Informations complémentaires

Des informations complémentaires sur l'IEC 61508 et sur la sécurité fonctionnelle sont disponibles sur le site http://www.iec.ch/functionalsafety. On peut également y acheter la norme.

Si vous possédez la norme, mais n'êtes pas familiarisé avec son contenu, vous pouvez commencer par lire les chapitres suivants en premier :

- Le chapitre A de l' IEC 61508-5, qui présente les concepts de risque et d'intégrité de la sécurité,
- La figure 2 et tableau 1 de l'IEC 61508-1, qui illustre le cycle de vie de sécurité complet et qui liste les objectifs de chaque phase du cycle de vie. Les objectifs et les phases du cycle de vie sont les clés pour comprendre les exigences du cycle de vie de la sécurité de l'IEC 61508-1,
- Les clauses 6 et 8 de l'IEC 61508-1, qui contiennent les exigences reliant le management de la sécurité fonctionnelle et l'évaluation de la sécurité fonctionnelle,
- Le chapitre A de l'IEC 61508-6, qui fournit en 8 pages une vision globale des exigences de l'IEC 61508-2 et de l'IEC 61508-3,
- La figure 2 et le tableau 1 de l'IEC 61508-2 et la figure 3 et le tableau 1 de l'IEC 61508-3, qui permettent de comprendre les exigences du cycle de vie de la sécurité de l''IEC 61508-2 et de l'IEC 61508-3.

Toutes les exigences de l'IEC 61508 doivent être prises en compte dans le contexte de la phase du cycle de vie associée et des objectifs établis pour cette phase. Nous nous sommes basés sur ces 5 parties de la norme pour documenter le chapitre 6.8.

5.2 POSITION OFFICIELLE DE L'UNION EUROPEENNE

Relations entre l'IEC 61508 et les normes sectorielles associées avec les directives européennes "Nouvelle Approche" : S J Brown HSE, RU

5.2.1 IEC 61508 – Sécurité Fonctionnelle des systèmes électriques / électroniques / électroniques programmables concernés par la sécurité

L'IEC 61508 a été approuvée par le CENELEC en tant que norme européenne (EN). Ceci signifie qu'elle doit être publiée en tant que norme nationale par chaque organisation de normalisation nationale. C'est chose faite en France par l'AFNOR depuis 1999 (NF 61508). Cela signifie également que tous les textes nationaux incompatibles avec l'IEC 61508 doivent être abrogés. Mais il n'y a pas d'obligation légale de se conformer aux normes européennes. Ceci signifie que le fait que la norme soit une norme européenne n'implique pas en soit qu'il existe une obligation légale de conformité à l'IEC 61508.

Il faut bien noter que l'EN 61508 n'a pas le statut de norme harmonisée européenne et que donc, aucune directive européenne de la commission n'y fait référence. Ceci est dû partiellement au fait que le périmètre de l'IEC 61508 inclut la totalité du cycle de vie et dépasse de loin le périmètre d'une norme associée à une directive produit. (Le concept de norme européenne "harmonisée" s'applique aux directives européennes pour des produits. Ceci signifie que la conformité à la norme vaut présomption de conformité aux "exigences essentielles" de la directive). Cependant, cela n'empêche pas d'utiliser la conformité à certaines parties de la norme pour supporter la déclaration de conformité avec une directive européenne produit si cela est approprié. Mais puisque l'EN 61508 n'est pas une norme harmonisée, il n'y a pas de présomption de conformité avec quelque directive que ce soit. Il serait donc nécessaire d'expliquer dans le dossier technique d'un produit en quoi la conformité à l'EN 61508 supporte la conformité avec des exigences essentielles d'une directive particulière.

5.2.2 IEC 61511 –Sécurité Fonctionnelle des systèmes instrumentés de sécurité pour le secteur de l'industrie des procédés continus

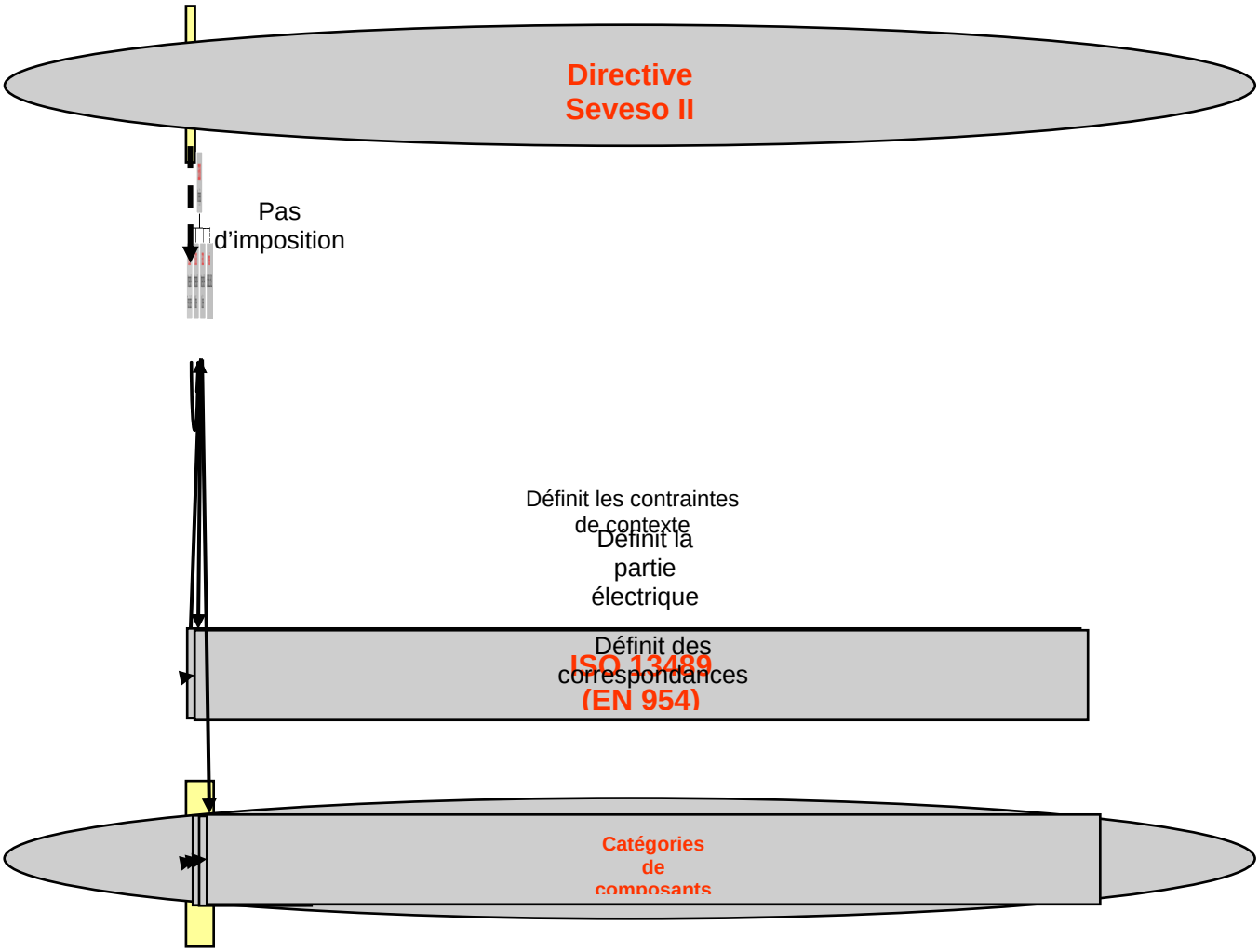
L'IEC 61511 a été approuvée par le CENELEC en tant que norme européenne (EN). Les remarques faites ci-dessus pour l'IEC 61508 s'appliquent également à l'IEC 61511. Il s'en suit que l'IEC 61511 n'a pas le statut de norme européenne harmonisée sous quelque directive européenne que ce soit et qu'il n'y a pas d'obligation légale de conformité à l'IEC 61511.

5.2.3 IEC 62061 – Sécurité Fonctionnelle des systèmes de contrôle électriques / électroniques / électroniques programmables pour les machines

L'IEC 62061 a été rédigée dans l'objectif de devenir une norme européenne harmonisée pour la Directive Machine. Ceci a été rendu possible en réduisant le périmètre de l'IEC 61508 pour n'inclure que des exigences concernant des produits. Il faut toutefois noter que bien que cela fournira une présomption de conformité à certaines exigences essentielles de la Directive Machine, cela n'empêchera pas d'utiliser d'autres moyens (d'autres normes) pour remplir ces exigences.

La commission européenne reconnaît implicitement que l'EN 954-1 (ISO 13489) est notoirement insuffisante dès que les chaînes de sécurité des machines contiennent des automatismes programmés. Elle recommande (sans encore l'imposer) d'appliquer l'IEC 62061.

5.3 POSITIONS RESPECTIVES DES NORMES



La norme IEC 61508 est générique. Les normes sectorielles qui en sont issues sont totalement compatibles. Ceci signifie qu'il ne faut pas penser trouver une réduction du périmètre fonctionnel ou des entorses aux principes de bases de l'IEC 61508 dans ses normes filles. Les normes sectorielles ne font que préciser les modalités d'application.

Par exemple, l'IEC 61511 précise à partir de quel niveau SIL il faut appliquer des techniques de preuve semi-formelle en fonction du type de langage de programmation utilisé, mais n'élimine en aucun cas la recommandation d'utilisation de ce type de technique.

Autre exemple, l'IEC 62061 réduit son périmètre aux aspects « produit ». Ceci signifie que la norme ne permet pas **seule** de remplir toutes les obligations liées par exemple à l'intégralité du cycle de vie défini dans l'IEC 61508.

D'autre part, les normes étant sectorielles et ne contenant aucune contradiction entre-elles, il peut parfois y avoir ambiguité sur le choix de celle à appliquer. Par exemple, une enrouleuse dans une usine de papier est une machine, une ensacheuse dans une usine d'incinération d'ordures ménagères est également une machine. A ce titre, l'IEC 62061 leur sont applicables. Mais cette dernière ayant un périmètre réduit aux aspects « produit », c'est l'IEC 61511 qui permettra de définira toutes les exigences de contexte. Dans ce type de cas, les deux normes s'appliquent et les aspects « manufacturiers » sont « subordonnés » aux aspects « process ».

L'IEC 62061 est rédigée en cohérence avec l'ISO 12100 et l'ISO 13489 qui sont harmonisées en tant que normes EN de classe A dans le but de remplacer les EN 292 et EN 954.

5.4 VARIATEURS DE VITESSE

Le groupe de travail SC22 WG6 de l'IEC prépare actuellement une nouvelle norme sur la sécurité fonctionnelle des variateurs de vitesse concernés par la sécurité. Cette nouvelle norme IEC 61800-5-2 "Systèmes de variateurs de vitesse électriques - exigences de sécurité - aspects fonctionnels" concernera les composants, prenant en compte le fait que dans de nombreux cas le variateur de vitesse est un composant d'une installation concernée par la sécurité.

Son objectif est de "faciliter l'incorporation de variateurs de vitesse concernés par la sécurité dans un système de contrôle en utilisant les principes de l'IEC 61508, ou des normes sectorielles (par exemple : IEC 61511, IEC 61513, et IEC 62061) et ISO 13849."

Cette norme a les particularités suivantes :

- Les analyses de risques ne font pas partie de son périmètre. Certaines fonctions typiques des variateurs de vitesse concernés par la sécurité sont spécifiées pour être utilisées dans un contexte concerné par la sécurité. Ces fonctions sont appelées "Fonctions de Sécurité de Base".
- Les fonctions de sécurité des variateurs de vitesse concernés par la sécurité se voient attribuer des exigences "capacité SIL", pas des SIL. Un certificat fourni par un organisme tiers (du type TÜV etc.) pourrait donc par exemple déclarer quelque chose tel que "ce variateur de vitesse est apte à être utilisé dans une fonction SIL3".
- Une aptitude SIL n'impose pas une valeur de PFH/PFD particulière. L'IEC 61800-5-2 exige uniquement qu'une valeur de PFH/PFD soit spécifiée pour chaque fonction de sécurité. Bien entendu, un constructeur de variateurs de vitesse concernés par la sécurité ne voudra être tenu responsable que d'une fraction de la valeur globale du PFH/PFD de la fonction de sécurité pour laquelle un variateur est prévu.
- Une aptitude SIL impose une exigence sur le taux de pannes sûres et sur l'évitement des pannes systématiques, en conformité avec l'IEC 61508.

6 IEC 61508 – APPROCHE GENERALE

6.1 GENERALITES

La stratégie générale d'obtention de la sécurité fonctionnelle repose sur :

1. **L'application:**

- De la gestion de la sécurité fonctionnelle

Et

- D'exigences techniques

Et

- De la compétence des personnes

2. **A un cycle de vie global de la sécurité intégrant :**

- La spécification,
- La conception et l'implémentation,
- L'installation et la mise en service,
- L'exploitation et la maintenance,
- Les modifications après réception, y compris le démantèlement.

La stratégie de conception pour atteindre le niveau d'intégrité de la sécurité (SIL) voulu repose sur un double série de mesues :

- Mesures destinées à combattre les pannes aléatoires des matériels,
- Mesures destinées à éviter les pannes systématiques des matériels et des logiciels.

6.2 STRUCTURE DE L' IEC 61508

L'IEC 61508 est constituée de 7 parties :

- IEC 61508-1, Exigences générales,
- IEC 61508-2, Exigences pour les systèmes électriques / électroniques / électroniques programmables concernés par la sécurité,
- IEC 61508-3, Exigences pour le logiciel,
- IEC 61508-4, Définitions et abréviations,
- IEC 61508-5, Exemples de méthodes pour la détermination des niveaux d'intégrité de la sécurité,
- IEC 61508-6, Directives pour l'application de l'IEC 61508-2 et de l'IEC 61508-3,
- IEC 61508-7, Vue d'ensemble de mesures et de techniques.

6.3 OBJECTIFS

Extraits repris de : Sécurité fonctionnelle et IEC 61508 : Guide simplifié Novembre 2002 : BSI

La norme internationale IEC 61508, Sécurité Fonctionnelle des systèmes électriques, électroniques, électroniques, programmables concernés par la sécurité a pour but de :

- fournir le potentiel de technologie E/E/PE pour améliorer à la fois les performances économiques et en termes de sécurité,
- permettre des développements technologiques dans un cadre global de sécurité,
- fournir une approche système, techniquement saine, suffisamment flexible pour le futur,
- fournir une approche basée sur le risque pour déterminer les performances des systèmes concernés par la sécurité,
- fournir une norme générique pouvant être utilisée par l'industrie, mais qui peut également servir à développer des normes sectorielles (par exemple : machines, usine chimiques, ferroviaire ou médical) ou des normes produit (par exemple : variateurs de vitesse),
- fournir les moyens aux utilisateurs et aux autorités de réglementation d'acquérir la confiance dans les technologies basées sur l'informatique,
- fournir des exigences basées sur des principes communs pour faciliter :
    - une compétence améliorée de la chaîne d'approvisionnement des fournisseurs de sous-systèmes et de composants à des secteurs variés,
    - des améliorations de la communication et des exigences (c'est-à-dire de clarifier ce qui doit être spécifié),
    - le développement de techniques et de mesures pouvant être utilisées par tous les secteurs, augmentant de ce fait la disponibilité des ressources,
    - le développement des services d'évaluation de la conformité si nécessaire,

L'IEC 61508 ne couvre pas les précautions qui peuvent se révéler nécessaires pour empêcher des personnes sans autorisation d'endommager et/ou d'affecter la sécurité fonctionnelle réalisée par les systèmes E/E/PE concernés par la sécurité, notamment les intrusions dans les réseaux. Le comité S99 de l'ISA propose un texte sur ce sujet.

6.4 SYSTEMES E/E/PE RELATIFS A LA SECURITE

L'IEC 61508 couvre la sécurité fonctionnelle, réalisée par des systèmes concernés par la sécurité qui sont principalement implémenté dans des technologies E/E/PE, c'est à dire des systèmes E/E/PE concernés par la sécurité. Cette norme est générique dans le sens où elle s'applique à ces systèmes indépendamment de leur application.

Certaines exigences de la norme concernent des activités de développement pour lesquelles les technologies d'implémentation n'ont éventuellement pas encore été décidées. Ceci comprend le développement des exigences de sécurité (conception, périmètre, analyse et évaluation du risque). S'il existe une possibilité que des technologies E/E/PE soient utilisées, la norme doit être appliquée de manière à ce que les exigences de sécurité pour un système concerné par la sécurité soient déterminées de manière méthodique et sans risques.

D'autres exigences de la norme ne sont pas spécifiques aux technologies E/E/PE et incluent la documentation, la gestion de la sécurité fonctionnelle, l'évaluation de la sécurité fonctionnelle et les compétences. Toutes les exigences qui ne sont pas spécifiques à la technologie peuvent être utilement

appliquées à des systèmes concernés par la sécurité même si ces systèmes ne tombent pas dans le périmètre de la norme.

Un système E/E/PE concerné par la sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité (c'est-à-dire, depuis le capteur, en passant par la logique de contrôle et les systèmes de communication, jusqu'à l'actionneur final, tout en incluant les actions critiques de l'opérateur).

Les systèmes de sécurité et les systèmes concernés par la sécurité sont définis en termes d'absence de risque inacceptable de blessure ou de préjudice à la santé des personnes. Les dommages aux personnes peuvent être directs ou indirects, comme des dommages aux biens ou à l'environnement par exemple. Certains systèmes peuvent être principalement conçus pour se prémunir contre des pannes ayant des implications économiques majeures. Ceci signifie que dans l'esprit, à objectifs techniques comparables ou identiques, il n'y a pas de différence entre un système de sécurité et un système de contrôle.

L'IEC 61508 peut donc être utilisée pour développer n'importe quel système E/E/PE comportant des fonctions critiques, telles que la protection des équipements, des biens ou de la productivité.

6.5 APPROCHE TECHNIQUE

L'IEC 61508 est une norme orientée « performances ». Ceci signifie que par opposition aux normes dites déterministes et prescriptives, c'est l'utilisateur qui, à travers son analyse et son évaluation du risque détermine les performances à atteindre par son système E/E/PE concerné par la sécurité. La norme spécifie les performances correspondant au risque déterminé et les moyens (techniques et mesures) à mettre en œuvre pour garantir l'obtention des performances du système E/E/PE concerné par la sécurité. L'ingénierie du système reste donc toujours prépondérante sur le choix des composants. Cette approche est particulièrement inhabituelle pour les utilisateurs français, généralement confrontés à des normes déterministes laissant peu de place à l'ingénierie au sein d'architectures prédéfinies.

En résumé, l'IEC 61508 :

- utilise une approche basée sur le risque pour déterminer les exigences d'intégrité de la sécurité des systèmes E/E/PE concernés par la sécurité, et fournit des exemples de manières d'y parvenir.
- utilise un modèle global de cycle de vie de la sécurité comme cadre technique pour les activités nécessaires pour garantir que la sécurité fonctionnelle est atteinte par les systèmes E/E/PE concernés par la sécurité.
- couvre toutes les activités du cycle de vie de la sécurité depuis la conception initiale, en passant par l'analyse et l'évaluation des risques, le développement des exigences de sécurité, la spécification, la conception, l'implémentation, l'exploitation et la maintenance, la modification, jusqu'au démantèlement final et à la mise au rebut.
- prend en compte les aspects système (y compris tous les sous-systèmes réalisant des fonctions de sécurité, matériel et logiciel) ainsi que les mécanismes de pannes (matérielles aléatoires et systématiques).
- contient des exigences pour se prémunir des pannes (évitant l'introduction de défauts) et pour contrôler les pannes (garantissant la sécurité en présence de pannes).
- spécifie les techniques et mesures nécessaires pour atteindre le niveau d'intégrité de la sécurité nécessaire.

6.6 NIVEAUX D'INTEGRITE DE SECURITE (SIL)

L'IEC 61508 spécifie 4 niveaux possibles de performance de la sécurité pour une fonction de sécurité. Ils sont appelés niveaux d'intégrité de la sécurité (SIL). Le niveau d'intégrité de sécurité 1 (SIL1) est le plus bas niveau d'intégrité de la sécurité et le niveau d'intégrité de sécurité 4 (SIL4) est le niveau d'intégrité de la sécurité le plus élevé. La norme détaille les exigences nécessaires pour atteindre chaque niveau d'intégrité de la sécurité. Ces exigences sont plus sévères aux niveaux d'intégrité de la sécurité les plus élevés de manière à garantir une probabilité de défaillance dangereuse plus basse.

Un système E/E/PE concerné par la sécurité contient habituellement plusieurs fonctions de sécurité. Si les exigences d'intégrité de la sécurité pour ces fonctions de sécurité diffèrent, alors les exigences applicables au niveau d'intégrité de la sécurité le plus s'élevé s'appliquent à l'intégralité du système E/E/PE concerné par la sécurité, sauf si l'implémentation garantit une indépendance suffisante entre les fonctions de sécurité (ce qui doit être démontré).

Si un système E/E/PE unique est capable de contenir toutes les fonctions de sécurité nécessaires, et si le niveau d'intégrité de la sécurité exigé est inférieur à SIL1, alors l'IEC 61508 ne s'applique pas.

6.7 OBTENTION DES NIVEAUX SIL DE L' IEC 61508

L'obtention du niveau d'intégrité de la sécurité (SIL) se fait en :

- Garantissant l'intégrité du cycle de développement du système dans les domaines de la spécification, de la conception et des essais dans le but d'éliminer et d'éviter les pannes systématiques en se référant à la Partie 2 tableaux B1 à B6,

Et en :

- Garantissant la robustesse de la conception par des mesures permettant la tolérance aux pannes systématiques (diagnostics, contrôle d'accès, environnement, etc…) en se référant à la Partie 2 tableaux A16 à A19, et Partie 3 tableau A2,

Et en :

- Respectant des contraintes sur l'architecture du matériel en tant que partie prenante du taux de couverture permettant de déterminer le taux de panne sûre (SFF) en se référant à la Partie 2 tableaux 2 et 3,

Et en :

- En garantissant un PFD, en tant que fonction du taux de panne sur sollicitation et de l'intervalle de test, ou en tant que taux de panne par heure, en se référant à la Partie 1 tableaux 2 et 3,

Et :

- Si un logiciel est concerné,en garantissant l'intégrité et robustesse de la conception concernant uniquement les pannes systématiques en se référant à la Partie 3 tableaux A1 à A10.

6.8 MISE EN ŒUVRE

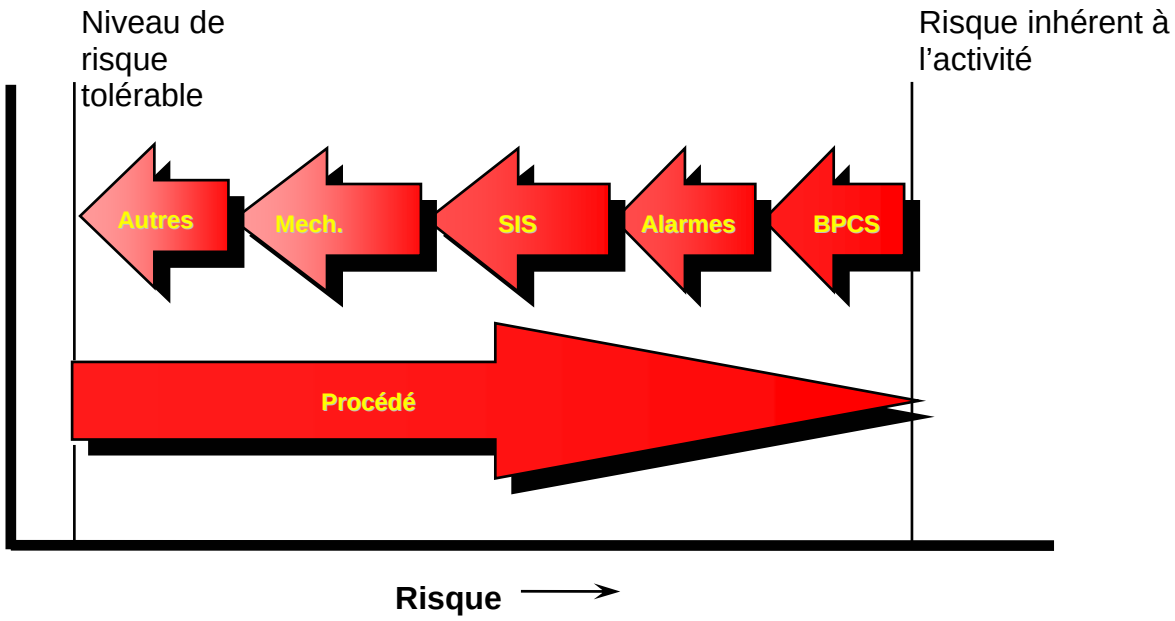
6.8.1 CONCEPTS DE RISQUE ET D'INTEGRITE DE LA SECURITE

La **démarche repose sur une analyse et une classification du risque**. Cette activité peut être réalisée par diverses méthodes quantitatives et/ou qualitatives mais doit aboutir à une liste de risques dont l'évaluation est quantifiée et que l'on va mettre en regard des objectifs quantifiés ou au moins classés de risques tolérables.

On touche ici à la première difficulté de la norme. **Quelqu'un doit s'engager sur le risque tolérable**. Normalement, il s'agit de l'utilisateur final, qui se tourne naturellement vers les textes réglementaires pour tenter de décharger sa responsabilité. Peine perdue, les textes sont soit non prescriptifs (directive Seveso II pour le process), soit déterministes (directive machine = il n'y a plus de risque).

Or sans cette valeur de risque tolérable, il n'y a pas d'ingénierie de la sécurité possible.

Le schéma ci-dessous décrit le principe général de la réduction du risque :



Dans ce contexte le **rôle du SIS** est de **contribuer**, avec les autres systèmes de sécurité, à **atteindre le niveau de risque résiduel tolérable**.

L'**intégrité de la sécurité** est la probabilité de bon fonctionnement du SIS dans un contexte donné, pendant une période de temps donnée et dans tous ses modes de fonctionnement prévus. L'intégrité de la sécurité est composée de 2 éléments :

- L'intégrité de la sécurité du matériel, liée à ses pannes aléatoires dangereuses, qui peut être calculée avec un degré de précision raisonnable. Ceci permet de dimensionner les exigences techniques associées aux niveaux voulus (en particulier en jouant sur les architectures),

- L'intégrité de la sécurité vis-à-vis des pannes systématiques dangereuses du matériel et des logiciels. Ce type de panne est très difficile à quantifier. La norme propose donc d'appliquer des techniques de conception plutôt que de se lancer dans des calculs.

Il est important de bien distinguer le risque en tant que combinaison quantifiée de la gravité et de la fréquence d'un événement, du risque tolérable qui est une notion sociétale. L'intégrité de la sécurité ne s'applique que aux SIS.

Les exigences en termes d'intégrité de la sécurité se traduisent par des niveaux SIL. Les normalisateurs sont passés d'un spectre d'exigences continu (PFD ou PFH) à des « tranches » SIL de 1 à 4 dans un rapport logarithmique. En pratique l'utilisateur doit être prudent et conserver des ordres de grandeur raisonnables. Par exemple, un PFD exigé de 9.10^{-1} correspond à un niveau SIL 1. En prenant en compte, les erreurs d'appréciation, de validité des données de base, l'influence des erreurs systématiques, il est clair que la spécification devra exiger SIL 2 pour garantir la réduction de risque recherchée. Ce type d'approche est au cœur même de la démarche IEC 61508.

6.8.2 CONCEPT DE CYCLE DE VIE

Le tableau ci-dessous décrit les **objectifs de chaque phase du cycle de vie** global de la sécurité.

Phase du cycle de vie de sécurité	Objectifs	Périmètre
Concept	Développer un niveau de compréhension de l'équipement sous contrôle (EUC) et son environnement (physique, réglementaire, etc.) suffisant pour permettre de réaliser de manière satisfaisante les autres activités du cycle de vie de la sécurité.	Equipement sous contrôle (EUC) et son environnement (physique, réglementaire, etc.).
Définition du périmètre général	Déterminer les limites de l'équipement sous contrôle (EUC) et de son système de contrôle, Spécifier le périmètre de l'analyse de dangers et de risques (par exemple dangers procédés, dangers environnementaux, etc.).	Equipement sous contrôle (EUC) et son environnement.
Analyse de dangers et de risques	Déterminer les dangers et les événements dangereux de l'équipement sous contrôle (EUC) et du système de contrôle de l'EUC (dans tous ses modes d'exploitation), dans toutes les circonstances raisonnablement prévisibles, y compris les mauvais emplois et les pannes, Déterminer les séquences d'événements conduisant aux événements déterminés, Déterminer les risques de l'EUC associés avec les événements dangereux déterminés.	Le périmètre dépend, dans le cadre d'une démarche itérative, de la phase atteinte dans le cycle de vie global. Pour une analyse de dangers et de risques préliminaire, le périmètre comprend l'EUC, le système de contrôle de l'EUC et les facteurs humains.
Exigences globales de sécurité	Développer les spécifications pour les exigences globales de sécurité, en termes d'exigences de fonctions de sécurité et d'exigences d'intégrité de la sécurité pour les systèmes E/E/PE concernés par la sécurité, pour des systèmes de sécurité basés sur d'autres technologies et pour les équipements externes de réduction du risque, de façon à réaliser la sécurité fonctionnelle.	L'EUC, le système de contrôle de l'EUC et les facteurs humains.
Allocation des exigences de sécurité	Affecter les fonctions de sécurité, contenues dans les exigences globales de sécurité, (exigences de fonctions de sécurité et exigences d'intégrité de la sécurité) aux systèmes E/E/PE concernés par la sécurité, aux systèmes de sécurité basés sur d'autres technologies et aux équipements externes de réduction du risque, Affecter un niveau d'intégrité de la sécurité (SIL) à chaque fonction de sécurité.	L'EUC, le système de contrôle de l'EUC et les facteurs humains.
Planification générale de l'exploitation et de la maintenance	Développer un plan pour l'exploitation et la maintenance des systèmes E/E/PE concernés par la sécurité , pour garantir que la sécurité fonctionnelle requise est conservée pendant l'exploitation et la maintenance.	L'EUC, le système de contrôle de l'EUC et les facteurs humains, Systèmes E/E/PE concernés par la sécurité.
Planification générale de la validation de la sécurité	Développer un plan pour faciliter la validation de la sécurité globale des systèmes E/E/PE concernés par la sécurité.	L'EUC, le système de contrôle de l'EUC et les facteurs humains, Systèmes E/E/PE concernés par la sécurité.

Phase du cycle de vie de sécurité	Objectifs	Périmètre
Planification générale de l'installation et de la mise en service	Développer un plan pour installer de manière maîtrisée les systèmes E/E/PE concernés par la sécurité, pour garantir la sécurité fonctionelle requise; Développer un plan pour mettre en service de manière maîtrisée les systèmes E/E/PE concernés par la sécurité, pour garantir la sécurité fonctionelle requise.	L'EUC, le système de contrôle de l'EUC et les facteurs humains, Systèmes E/E/PE concernés par la sécurité.
Réalisation des systèmes E/E/PE concernés par la sécurité	Réaliser des systèmes E/E/PE concernés par la sécurité conformes aux exigences de sécurité des spécifications E/E/PES (comprenant les spécifications pour les exigences des fonctions de sécurité des systèmes E/E/PE et les spécifications pour les exigences d'intégrité pour les ssytèmes E/E/PE).	Systèmes E/E/PE concernés par la sécurité.
Réalisation des systèmes concernés par la sécurité à base d'autres technologies	Réaliser les systèmes de sécurité basés sur d'autres technologies de manière à remplir les exigences des fonctions de sécurité et d'intégrité de la sécurité de ces systèmes (hors du périmètre de la norme).	Systèmes de sécurité basés sur d'autres technologies.
Réduction externe du risque **Réalisation des installations**	Réaliser les équipements/installations externes de manière à remplir les exigences des fonctions de sécurité et d'intégrité de la sécurité de ces installations (hors du périmètre de la norme).	Equipements/installations de réduction du risque externes.
Installation et mise en service	Installer les systèmes E/E/PE concernés par la sécurité, Mettre en service les systèmes E/E/PE concernés par la sécurité.	L'EUC et le système de contrôle de l'EUC, Systèmes E/E/PE concernés par la sécurité.
Validation de la sécurité	Valider que les systèmes E/E/PE concernés par la sécurité remplissent les spécifications des exigences globales de sécurité en termes d'exigences des fonctions de sécurité et d'exigences globales d'intégrité de la sécurité, en prenant en compte l'affectation des exigences de sécuritéaux systèmes E/E/PE concernés par la sécurité.	L'EUC et le système de contrôle de l'EUC, Systèmes E/E/PE concernés par la sécurité.
Exploitation maintenance et réparations	Exploiter, maintenir et réparer les systèmes E/E/PE concernés par la sécurité de manière à conserver la sécurité fonctionnelle requise.	L'EUC et le système de contrôle de l'EUC, Systèmes E/E/PE concernés par la sécurité.
Modifications et rénovations	Garantir que la sécurité fonctionnelle des systèmes E/E/PE concernés par la sécurité est appropriée, pendant et après les phases de modification et/ou de rénovation.	L'EUC et le système de contrôle de l'EUC, Systèmes E/E/PE concernés par la sécurité.
Démantèlement ou mise au rebut	Garantir que la sécurité fonctionnelle des systèmes E/E/PE concernés par la sécurité est appropriée pendant et après les activités de démantèlement ou de mise au rebut de l'EUC.	L'EUC et le système de contrôle de l'EUC, Systèmes E/E/PE concernés par la sécurité.

6.8.3 GESTION DE LA SECURITE ET EVALUATION DE LA SECURITE

La norme exige que le management des activités soit encadré par des procédures techniques. Les responsabilités individuelles et organisationnelles doivent être clairement établies et documentées. Le maintien de la compétence et les boucles de retour d'expérience prévues par la norme sont directement inspirés de l'ISO 9000.

L'évaluation de la sécurité fonctionnelle est définie comme une activité permanente le long du cycle de vie de la sécurité. L'évaluation est basée sur un plan d'évaluation.

Cette activité est effectuée par des personnes spécialisées et s'applique à tous les domaines couverts par le cycle de vie de la sécurité. Il en résulte les exigences d'indépendance suivantes :

Niveaux minimums d'indépendance des personnes en charge de l'évaluation de la sécurité fonctionnelle hors phase de réalisation des systèmes E/E/PE concernés par la sécurité

Niveau minimum D'indépendance	Conséquence (voir note)			
	A	B	C	D
Personne indépendante	HR	HR	NR	NR
Département indépendant	–	HR	HR	NR
Organisation indépendante	–	–	HR	HR
NOTE – A – blessure mineure temporaire; B – blessure permanente d'une ou plusieurs personnes, décès; C – décès multiples; D – catastrophe.				

Niveaux minimums d'indépendance des personnes en charge de l'évaluation de la sécurité fonctionnelle de la phase de réalisation des systèmes E/E/PE concernés par la sécurité

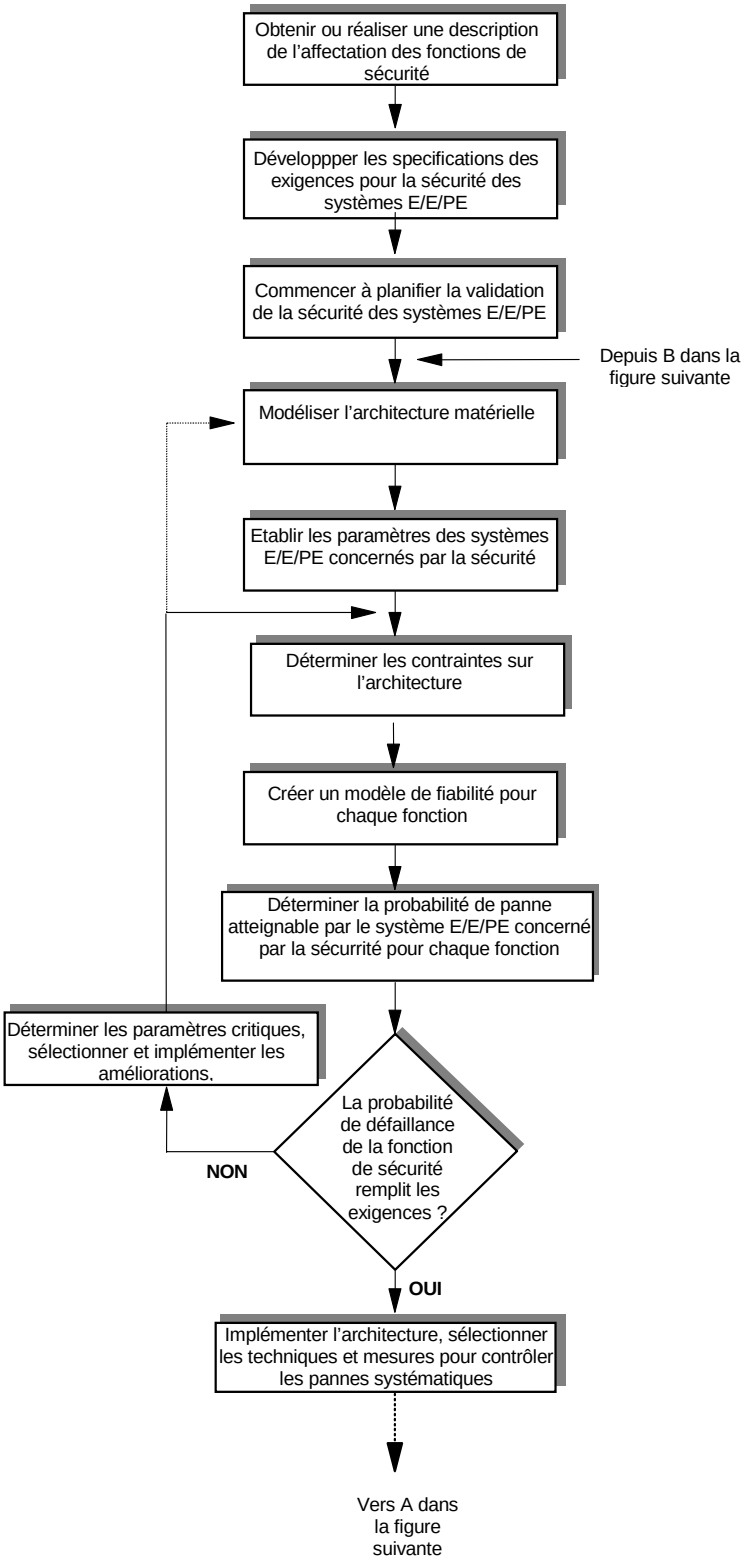
Niveau minimum D'indépendance	Niveaux d'intégrité de la sécurité			
	1	2	3	4
Personne indépendante	HR	HR	NR	NR
Département indépendant	–	HR	HR	NR
Organisation indépendante	–	–	HR	HR

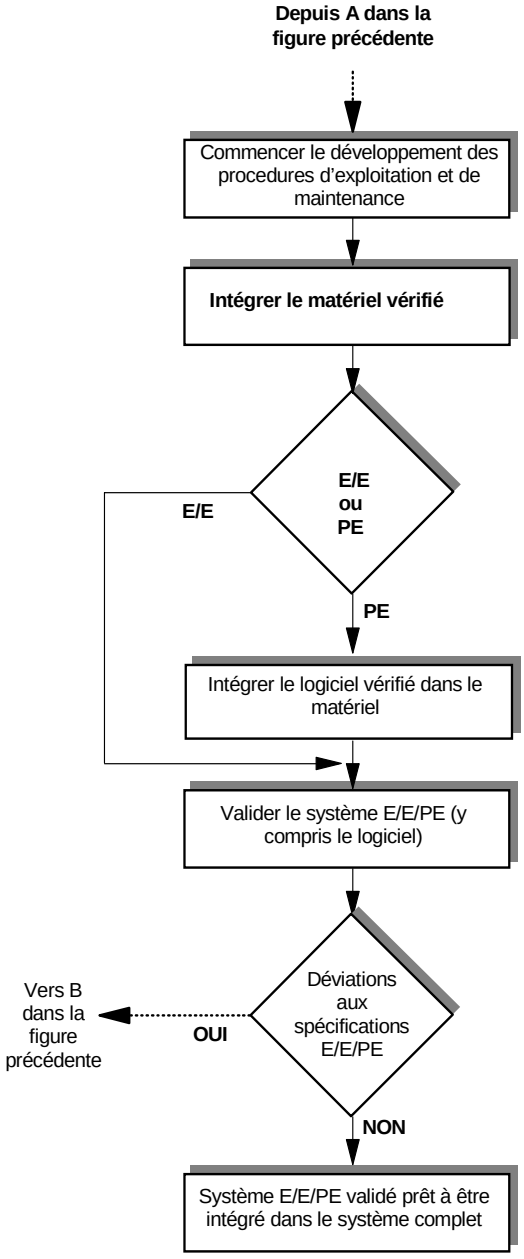
HR = Hautement Recommandé

NR = Non Recommandé

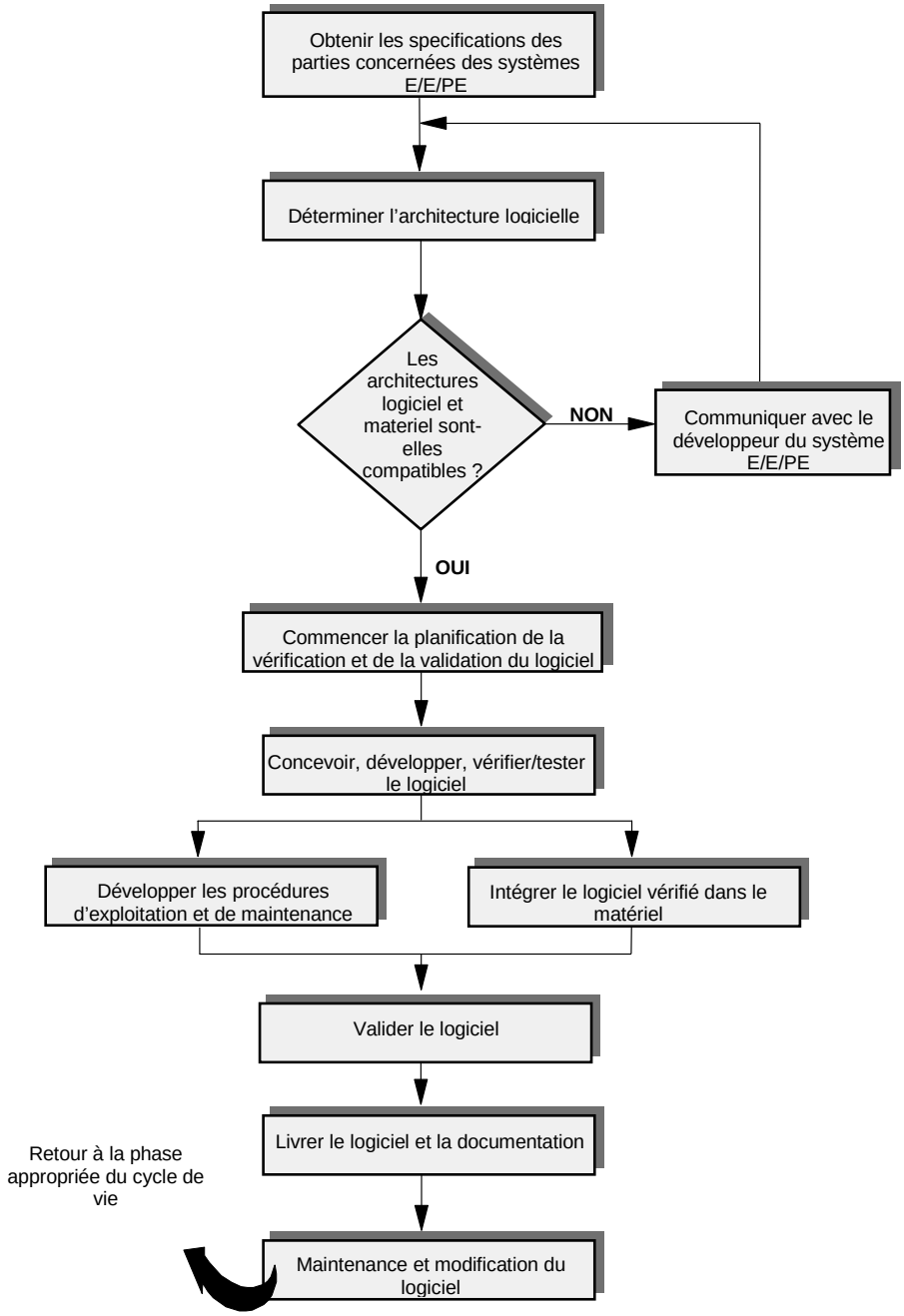
6.8.4 MISE EN ŒUVRE DE L'IEC 61508-2 (MATERIEL)

La mise en œuvre de la partie 2 de la norme est résumée dans les 2 schémas suivants :


Obtenir ou réaliser une description de l'affectation des fonctions de sécurité
Développper les specifications des exigences pour la sécurité des systèmes E/E/PE
Commencer à planifier la validation de la sécurité des systèmes E/E/PE
Depuis B dans la figure suivante
Modéliser l'architecture matérielle
Etablir les paramètres des systèmes E/E/PE concernés par la sécurité
Déterminer les contraintes sur l'architecture
Créer un modèle de fiabilité pour chaque fonction
Déterminer la probabilité de panne atteignable par le système E/E/PE concerné par la sécurrité pour chaque fonction
Déterminer les paramètres critiques, sélectionner et implémenter les améliorations.
La probabilité de défaillance de la fonction de sécurité remplit les exigences ?
NON
OUI
Implémenter l'architecture, sélectionner les techniques et mesures pour contrôler les pannes systématiques
Vers A dans la figure suivante


Depuis A dans la figure précédente
Commencer le développement des procedures d'exploitation et de maintenance
Intégrer le matériel vérifié
E/E ou PE
E/E
PE
Intégrer le logiciel vérifié dans le matériel
Valider le système E/E/PE (y compris le logiciel)
Déviations aux spécifications E/E/PE
OUI
Vers B dans la figure précédente
NON
Système E/E/PE validé prêt à être intégré dans le système complet

6.8.5 MISE EN ŒUVRE DE L'IEC 61508-3 (LOGICIEL)



7 MISE EN ŒUVRE DE L'IEC 61508 DANS LES PROCEDES CONTINUS ET MANUFACTURIERS

L'IEC 61511 est la norme sectorielle « Procédés continus » issue de l'IEC 61508. A ce titre un certain nombre de précisions s'imposent :

- Il n'y a pas de différences de fond entre IEC 61511 et IEC 61508. L'IEC 61511 apporte des précisions en restreignant le champ d'application initial de l'IEC 61508 au contexte traditionnel des procédés continus. Par exemple, en ce qui concerne les langages de programmation, l'IEC 61511 ne s'intéresse que aux langages de programmation usuels du métier (IEC 1131-3). Cela n'interdit aucunement de programmer un système E/E/PE en C++. Mais dans ce cas il faut se référer à l'IEC 61508.
- L'approche de la sécurité incluant le concept « pipe to pipe », les méthodes d'évaluation de la sécurité et d'analyse du risque du secteur (HAZOP, etc…) est intégralement reprise.
- Dans l'esprit, l'IEC 61511 n'est pas nécessaire car tout est déjà dit dans l'IEC 61508. L'IEC 61511 contient plus de renvois à l'IEC 61508 que de matière propre.
- L'IEC 61511 apporte surtout dans ses parties non normatives des réponses à des questions fréquentes.
- La norme reflète profondément l'industrie des procédés continus « lourds ». Les utlisateurs des industries intermédiaires (pharmacie, agro-alimentaire,etc…) mélangeant des équipements de type « process » et des machines plus « manufacturières » pourront être déroutés par une approche dont ils n'ont pas l'habitude.
- Du fait de la totale compatibilité entre les normes, les questions / réponses ci-dessous s'appliquent en fait à tous les secteurs. Il n'y a pas de réponses différentes entre secteurs industriels.

Pour ce qui concerne l'IEC 62061, norme pour les machines, l'appréhension du texte est plus délicate car :

- La norme ne cesse de se référer à la norme EN 954-1 pour établir des passerelles entre les niveaux d'exigence et la classification des équipements. Cet exercice est limité en termes de périmètre et d'apport à l'utilisateur.
- Le périmètre de la norme, dans le cycle de vie de la sécurité, est très limité et ne s'étend pas sur le logiciel.
- Le lecteur « reste sur sa faim » et en définitive est renvoyé d'une part à l'IEC 61508 et aux limites des correspondances IEC 62061/EN954-1.

Nous reprenons ci-après un certain nombre de questions fréquemment posées et renvoyons le lecteur aux réponses proposées par les guides d'application de l'ISA S84 (nettement plus complets que ceux de l'IEC 61511). Nous avons choisi ce type d'approche car les réponses nécessitent parfois plusieurs pages pour être rigoureuses. Les réponses sont toutes applicables quelque soit l'industrie concernée.

Les questions sont classées par domaine d'intérêt et peuvent se retrouver dans plusieurs domaines :

1. Ecarts entre IEC 61508, IEC 61511 et IEC 62061,
2. Analyse du risque et évaluation du risque,
3. Organisatoin générale et spécifications,
4. Choix des matériels et architectures matérielles,

5. Méthodes de calcul pour analyse quantitative,
6. Développement des logiciels d'application,
7. Capteurs et actionneurs,
8. Eléments de contexte (alimentations, câblage, etc..),
9. Mise en œuvre dans les procédés manufacturiers.

8 QUESTIONS FREQUENTES

8.1 ECARTS ENTRE IEC 61508, IEC 61511 ET IEC 62061

Q - 1. Quelles sont les correspondances entre l'ancienne norme allemande DIN 19250 et l'IEC 61511 ?

Q - 2. Quelles sont les ajustements faits par l'IEC 61511 sur les exigences d'architecture des systèmes ?

Q - 3. Quelles sont les différences (périmètre, terminologie) entre l'IEC 61508 et l'IEC 61511 ?

Q - 4. Pourquoi le niveau SIL 4 n'est-il pas pris en compte dans l'IEC 61511 ni dans l'IEC 62061 ?

Q - 5. Quelles sont les différences entre l'IEC 61508 et l'IEC 62061 ?

8.2 DOMAINE ANALYSE ET EVALUATION DU RISQUE

Un des grands mérites de l'IEC 61508 et de l'IEC 61511 est de prendre la problématique de la sécurité à sa source, c'est-à-dire au niveau du risque. C'est probablement le domaine le plus important puisqu'il conditionne la suite du cycle de vie de la sécurité.

Q - 6. Qu'est-ce que la « défense en profondeur » ? Qu'est-ce que le LOPA (Layer Of Protection Analysis) ? Quelle est la place des systèmes E/E/PE concernés par la sécurité dans la « défense en profondeur » ?

Q - 7. Existe-t-il un exemple de mise en oeuvre de la méthode LOPA ?

Q - 8. Existe-t-il des valeurs typiques de fiabilité de couches de protection ?

Q - 9. Qu'est-ce que le risque tolérable ? Existe-t-il des valeurs typiques ?

Q - 10. A quoi correspond le concept ALARP (As Low As Reasonably Practical) ?

Q - 11. Qu'est ce que l'intégrité de sécurité ?

Q - 12. Comment classer les risques ?

Q - 13. Quelle est la différence entre des méthodes de classement quantitatives, semi-quantitatives et qualitatives ?

Q - 14. Quelles méthodes de classement sont conformes aux normes ?

Q - 15. Existe-t-il un exemple de méthode semi-quantitative ?

Q - 16. Existe-t-il un exemple de méthode qualitative ?

Q - 17. Qu'est-ce que la méthode de la matrice des couches de protection ?

Q - 18. Ces méthodes sont-elles applicables à la protection de l'environnement ?

Q - 19. Existe-t-il des formations à l'analyse de risque dans le cadre de l'IEC 61508 ?

Q - 20. Comment passer de l'analyse et de l'évaluation des risques aux niveaux SIL ?

Q - 21. Existe-t-il des exemples ?

Q - 22. Qu'est-ce que le graphe des risques ?

Q - 23. Quelles sont les étapes d'une analyse du risque ?

Q - 24. Où puis-je trouver des valeurs typiques de taux de défaillance d'équipements ?

Q - 25. Où puis-je trouver des valeurs typiques pour des défaillances humaines ?

Q - 26. De quels outils doit-on disposer pour réaliser une analyse de risque ?

8.3 ORGANISATION GENERALE ET SPECIFICATIONS

Q - 27. Où puis-je trouver une description des rôles et compétences nécessaires à l'application des normes ?

Q - 28. Existe-t-il une checklist de spécification des exigences de sécurité ?

Q - 29. Qu'est-ce qu'une conception intrinsèquement sûre ?

Q - 30. Quels sont les principes génériques de la tolérance aux pannes ? Comment diversifier les matériels ? Quelles sont les limites de la diversité ?

Q - 31. Existe-t-il des check-lists d'évaluation de la sécurité fonctionnelle ?

Q - 32. Comment doit-on conduire les audits ? A quelle fréquence ? Par qui doivent-ils être menés ?

Q - 33. Existe-t-il des exemples de ce qu'un audit peut habituellement trouver ?

Q - 34. Peut-on utiliser le système de contrôle commande pour exécuter des fonctions E/E/PE concernées par la sécurité (SIF) ? Quelles en sont les conséquences ?

Q - 35. Qu'elle est l'importance de l'intervalle de test du SIS ?

Q - 36. Existe-t-il des recommandations concernant la sécurité de l'accès au système ?

8.4 CHOIX DES MATERIELS ET ARCHITECTURES MATERIELLES

Q - 37. Que signifie conforme à IEC 61508 pour un composant ?

Q - 38. Les normes imposent-elles des composants certifiés ?

Q - 39. Qu'apporte la certification d'un produit à l'utilisateur ?

Q - 40. Quelles sont les limites des composants certifiés dans le cadre de la conception d'un système E/E/PE concerné par la sécurité ?

Q - 41. Doit-on systématiquement utiliser des solveurs logiques conforme à l'IEC 61508 ?

Q - 42. Comment gérer la communication entre le système de contrôle du procédé/machine et le système E/E/PE concerné par la sécurité ?

Q - 43. Existe-t-il des recommandations d'architecture matérielle ?

Q - 44. Existe-t-il des recommandations de technologies ?

8.5 METHODES DE CALCUL POUR ANALYSE QUANTITATIVE

Q - 45. Quels sont les différents types de défaillances et leurs classifications ?

Q - 46. Quelles sont les formules de calcul permettant de quantifier les différents types de défaillances ?

Q - 47. Quelles sont typiquement les origines des défaillances ?

Q - 48. Qu'est-ce qu'une panne de mode commun ?

Q - 49. Quelles sont les stratégies pour répondre aux différents types de défaillances ?

Q - 50. Qu'est-ce que le taux de pannes sûres (SFF) ?

Q - 51. Quelle est la différence entre fonctionnement continu et fonctionnement sur sollicitation ?

Q - 52. Quel est l'impact de la simplification des calculs ? A partir de quand est-ce que l'on se trompe ?

Q - 53. Existe-t-il des tableaux de taux de panne typiques de composants ?

Q - 54. Quelles méthodes et outils de calculs sont nécessaires pour calculer le PFD et le FTR ?

8.6 DEVELOPPEMENT DES LOGICIELS D'APPLICATION

Q - 55. Que doit contenir la spécification du logiciel ?

Q - 56. Quelles sont les techniques de programmation recommandées ?

8.7 CAPTEURS ET ACTIONNEURS

Q - 57. Peut-on utiliser des transmetteurs à la fois pour le contrôle commande et pour les fonctions E/E/PE concernées par la sécurité ? Quelles en sont les conséquences ?

Q - 58. Quelles précautions doit-on prendre avec les capteurs et les actionneurs ?

8.8 ELEMENTS DE CONTEXTE (CABLAGE, ALIMENTATIONS,…)

Q - 59. Existe-t-il des recommandations concernant les sources d'alimentation ?

Q - 60. Existe-t-il des recommandations concernant le câblage ?

Q - 61. Existe-t-il des recommandations concernant l'interface homme-machine et l'opérateur ?

8.9 MISE EN ŒUVRE DANS LES PROCEDES MANUFACTURIERS

Q - 62. Quelle est l'approche de la réduction des risques dans le secteur manufacturier ?

Q - 63. Quelles sont les différences entre l'IEC 62061 et l'EN 954-1 (ISO 13489) ?

Q - 64. Quelles sont les ajustements faits par l'IEC 62061 sur les exigences d'architecture des systèmes ?

Q - 65. Quels sont les points durs actuels dans l'application de l'EN 954-1 (ISO 13489) ?

Q - 66. Quels sont les points durs actuels dans l'application de l'IEC 62061 ?

Q - 67. Quels éléments de la norme sont-ils intéressants pour faire valider une machine ?

9 CONCLUSION

Les normes sectorielles doivent être utilisées avec l'IEC 61508 car elles y font référence et ne sont pas autoportantes.

Nos pratiques accusent un retard certain par rapport à nos connaissances.

Ceci est dû en partie à une grande frilosité française vis-à-vis des sujets en rapport avec les risques industriels.

Le marché n'est par ailleurs pas mûr dans la mesure où les acteurs manquent et où les niveaux de prix n'intègrent pas encore les coûts des compétences et des outils nécessaires au saut qualitatif induit par les exigences des normes de la série IEC 61508.

Le domaine de la sécurité fonctionnelle est probablement appelé à un bel avenir, notamment car la recherche de la fiabilité fait généralement progresser également la disponibilité, et donc la productivité des unités de production automatisées.

L'arrivée de contraintes nouvelles est toujours reçue par des réticences. Nous partageons donc avec le lecteur quelques réflexions simples.

« On s'est mis à appliquer le référentiel et on a toujours autant de bugs. » Est-ce bien une excuse pour ne pas l'appliquer ? Le problème n'est-il pas ailleurs ?

Une analogie pourrait être : « Je respecte les limitations de vitesse et je mets ma ceinture de sécurité. Pouratnt j'ai toujours autant d'accidents ! ». Les limitations de vitesse et la ceinture ne sont cerftainement pas en cause !

La norme est très axée sur les calculs de performance, et cela est normal puisque c'est sa base. Il ne faut toutefois pas oublier le bon sens et l'expérience d'années d'ingénierie. Il ne faut pas non plus trop se focaliser sur les chiffres ou essayer de prouver n'importe quoi à n'importe quel prix : « Les chiffres sont comme les espions, à force de les torturer on leur fait dire ce que l'on veut. »

10 BIBLIOGRAPHIE

- dANSI/MME/ISA-84.00.01-2003 – Part 3 (IEC 61511:Mod 2003) : Functional safety: Safety Instrumented Systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels - informative
- ISA-TR84.00.04 Part 1 : Guideline on the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511 Mod)
- STSARCES Standards for Safety Related Complex Electronic Systems : Final report 29/02/2000
- Relationship of IEC 61508 and associated sector standards with EC 'New Approach' directives : S J Brown HSE, UK
- CNISF : propositions d'action au Ministre de l'Envireonnement et de l'Aménagement du Territoire 23 janvier 2002
- Functional safety and IEC 61508 A basic guide November 2002 : BSI
- EMC –Related Functional Safety EMC –Related Functional Safety Seminar Seminar - 22 March 2001- Ron Bell - Technology Division - Health & Safety Executive, UK
- STSARCES Standards for Safety Related Complex Electronic Systems : Final report 29/02/2000