République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université El-Hadj Lakhdar - Batna
Institut d'Hygiène et Sécurité Industrielle
Laboratoire de Recherche en Prévention Industrielle (LRPI)

MÉMOIRE

Présenté pour l'obtention du diplôme de

MAGISTÈRE

EN HYGIÈNE ET SÉCURITÉ INDUSTRIELLE

Option : Gestion du Risque

Par

Bilal RABAH

Ingénieur en Hygiène et Sécurité Industrielle

Thème :

Etude de l'implémentation des Systèmes Instrumentés de Sécurité par des méthodes semi-quantitatives dans un environnement de connaissances imparfaites

Soutenu le 26 Décembre 2013 devant le jury d'examen :

M.	Fares INNAL	Maître de Conférences A à l'Univ. de Batna	Président
M.	Rachid NAIT-SAID	Professeur à l'Univ. de Batna	Rapporteur
Mme	Nouara OUAZRAOUI	Maître Assisstante A à l'Univ. de Batna	Co-Rapporteur
M.	Mourad KORICHI	Maître de Conférences A à l'Univ. de Ouargla	Examinateur

2013

Remerciement

Le travail présenté dans ce mémoire a été effectuée au sein de l'équipe de sureté de fonctionnement du laboratoire de recherche en Prévention, Industrielle (LRPI) de l'institut d'Hygiène et Sécurité industrielle.

Je remercie vivement Monsieur Nait-Said Rachid Professeur à l'institut d'hygiène et sécurité industrielle d'avoir accepter la lourde tache de rapporteur et d'avoir consacrer un temps précieux à l'examen de ce manuscrit, sa compétence, sa grande rigueur scientifique, la qualité et la précision de ses remarques m'ont permis d'améliorer ce manuscrit.

Je remercie tout particulièrement Madame Ouzraoui Nouara, Maitre assistante A à l'institut d'hygiène et sécurité industrielle pour son aide inestimable et son soutien morale afin de finaliser ce mémoire.

Je dédie ce mémoire à mes parents et à toute la famille…

Table des matières

Chapitre 2 Approche flou du graphe du graphe de risque

Liste des figures

Liste des tableaux

Acronymes

BPCS	Basic Process Control System
CPF	Central Processing Facilities
DCS	Distributed Control System
E	Exchanger
FAL	Flow Alarm Low
FALL	Flow Alarm Low Low
FT	Flow Transmitter
FV	Flow Valve
H	Heater
HAZOP	Hazard and Operability Study
IEC	International Electrotechnical Commission
OHSAS	Occupational Health and Safety Assessment Series
PAH	Pressure Alarm High
PAHH	Pressure Alarm High High
PAL	Pressure Alarm Low
PALL	Pressure Alarm Low Low
PCV	Pressure Controller Valve
P&ID	Piping and Instrumentation Diagram
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PLC	Programmable Logic Controller
PT	Pressure Transmitter

RRF	Risk Reduction Factor
SDV	Shutdown Valve
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
TAH	Temperature Alarm High
TAHH	Temperature Alarm High High
TI	Temperature Indicator
TV	Temperature Valve
UKOOA	United Kingdom Offshore Operators Association

Introduction générale

Problématique

Les exigences sociétales actuelles imposent que les installations industrielles présentent le moins de risques possibles durant leur utilisation. C'est dans la phase de conception que l'on doit intégrer les éléments nécessaires à la sûreté de fonctionnement de ces installations. Deux approches permettent cette diminution du risque, la prévention en minimisant la probabilité d'apparition d'un risque, la protection en limitant les conséquences d'un dysfonctionnement.

Les moyens à mettre en œuvre pour réduire les risques sont nombreux et variés. Parmi les équipements utilisés pour réduire le risque, le système de contrôle de procédé connu sous le nom BPCS (Basic Process Controller System). Ce système est conçu pour surveiller, contrôler et maintenir le process dans un état de fonctionnement normale et sur. Cependant, la défaillance du BPCS peut être à l'origine d'un scénario d'un accident (événement initiateur).

Des systèmes d'arrêt d'urgence appelés Systèmes Instrumentés de Sécurité (SIS) interviennent dans le cas ou le process se trouve dans des conditions dangereuses de fonctionnement. Les SIS sont utilisés dans l'industrie de transformation pour réaliser une ou plusieurs fonctions instrumentées de sécurité SIF. Les normes IEC 61508 [IEC61508 98] et IEC 61511 [IEC61511 00] ont établi les prescriptions relatives à la spécification, l'exploitation et la maintenance de ces systèmes.

La réduction du risque apportée par la fonction instrumentée de sécurité est appelée réduction nécessaire du risque. Les normes IEC 61508 et IEC 61511 définissent quatre niveaux d'intégrité de sécurité (Safety integrity Level) pour une fonction de sécurité, quatre niveaux possibles de SIL. L'implémentation des SIS dans un système nécessite la détermination préalable du SIL qui devrait être atteint par la fonction instrumentée. L'évaluation du niveau d'intégrité de sécurité est déterminée par des méthodes qualitatives et quantitatives [SAL 06b], [SAL 08].

Parmi les méthodes qualitatives les plus utilisées pour déterminer le niveau de SIL d'une SIF la méthode graphe de risque décrit dans la partie 5 de la norme IEC 61508 [IEC 61508 98]. Quand cette méthode est adoptée, un certain nombre de paramètres de simplification sont introduits pour décrire la nature de la situation dangereuse lorsque les systèmes relatifs à la sécurité sont défaillants ou non disponibles. Un paramètre est choisi parmi quatre groupes caractéristiques du risque et les paramètres sélectionnés sont alors associés pour décider du niveau de SIL des systèmes relatifs à la sécurité.

Bien que le graphe de risque est une méthode relativement facile à appliquer et permettant une évaluation rapide des SIL, il présente tout de même, des insuffisances quant à l'interprétation des termes linguistiques utilisés pour caractériser les paramètres C, F, P et W, laquelle peut différer d'un jugement à l'autre et d'un secteur industriel à l'autre en raison de la subjectivité liée à la définition qualitative des paramètres suscités. A ceci s'ajoute les déclarations fermes en termes de probabilités et taux exprimant les paramètres C, F, P, W et le SIL ; le problème de rigidité des intervalles utilisés pour la représentation quantitative des paramètres leur est imputable.

La logique floue due à L.A Zadah [ZAD 65] semble offrir un cadre très adéquat pour le traitement de l'incertitude liée aux différents paramètres du graphe de risque [NAI 09], [SIM 07]. Dans ce travail, une approche du graphe de risque à base de règles floues est proposée afin d'ajouter des caractéristiques plus puissants au graphe de risque classique.

Objectif du mémoire

Le but essentiel de ce travail est d'étudier l'apport de la logique floue [ZAD 65] à la détermination des SIL par graphe de risque en présence d'informations incomplètes et/ou incertaines, lequel s'articule autour des concepts d'ensemble flou et de variable linguistique.

L'approche développée dans le cadre de ce travail s'appuie sur un système d'inférence à base de règles floues, le SIL étant la sortie de ce système. En utilisant les opérations de la logique floue, les données des paramètres du graphe de risque sont introduites dans le système d'inférence floue pour déterminer le niveau du SIL requis.

L'approche est validée expérimentalement sur un système industriel opérationnel qu'est un four rebouilleur

Organisation du mémoire

Le présent mémoire comporte principalement trois chapitres traitant les aspects théoriques du graphe de risque flou ainsi que la partie expérimentale et la validation de ce modèle par une étude expérimentale.

Le premier chapitre concerne les principales normes de sécurité fonctionnelles utilisées pour la conception des systèmes de sécurité. Ainsi que au développement des méthodes d'évaluation de SIL en s'intéressant particulièrement à la méthode graphe du risque conventionnel.

Dans le deuxième chapitre, nous présenterons d'abord les concepts fondamentaux de la logique flou puis les étapes du modèle graphe de risque flou

Afin de valider le modèle proposé, le troisième chapitre est consacré à l'application du modèle graphe de risque flou à l'évaluation du SIL d'un SIS sur un système industriel opérationnel.

1

Détermination du niveau d'intégrité de sécurité SIL

1.1 Introduction

Généralement les systèmes industriels peuvent présenter des risques pour les personnes et l'environnement, diverses sécurités doivent être mises en œuvre. Ces types de sécurité utilisent des moyens contribuant soit à la prévention soit à la protection pour réduire les risques de dysfonctionnement. Les Systèmes Instrumentés de Sécurité (SIS) sont utilisés comme moyens de sécurité pour réaliser des Fonctions Instrumentées de Sécurité (SIF) afin de mettre le processus dans un état de repli de sécurité si le processus se trouve dans des conditions dangereuses de fonctionnement. La Commission Internationale d'Electronique (CEI), ou "International Electrotechnical Commission" (IEC), a normalisé les systèmes de sécurité; Norme IEC 61508 en 1998 [IEC61508 98] et IEC 61511 en 2000 [IEC61511 00]. [MEC 11].

L'objet de ce chapitre est de donner dans un premier temps une définition de certains termes et concepts utilisés dans le cadre de la sécurité fonctionnelle des systèmes de sécurité. Par la suite, un aperçu sur les principales normes de sécurité utilisées pour concevoir les SIS est donné. La définition des SIS est détaillée. La dernière partie est consacrée à la description des différentes méthodes utilisées pour déterminer les niveaux SIL.

1.2 Concepts et définitions

Les industries déploient beaucoup d'efforts pour éviter les accidents. Malgré ces efforts, de nombreux accidents se produisent dans le monde et causent des dégâts sur les plans ; humains et matériels. La fréquence de ces accidents conduit à des études de sécurité afin de mieux maîtriser les risques.

Dans les études de sécurité, l'utilisation d'une des méthodes conventionnelles est recommandée afin d'identifier les sources ou les situations dangereuses. Une analyse préliminaire des dangers (APD) permet de déterminer les risques qu'un système peut entraîner.

Elle conduit à une série de mesures d'analyse de risques mises en œuvre peut mener l'installation à un niveau de sécurité jugé acceptable par l'exploitant [MKH 08].

1.2.1 Notion de sécurité

La sécurité est généralement définie par l'absence de phénomènes dangereux, de risque inacceptable, d'accident ou de situations catastrophiques [EXI].

Selon Villemeur [VIL 87], " *la sécurité est l'aptitude d'une entité éviter de faire apparaitre, dans des conditions données, des l'évènement critiques ou catastrophiques* ".

D'après Desroches [DES 03], *la sécurité concerne la non occurrence d'événements pouvant diminuer ou porter atteinte à l'intégrité du système, pendant toute la durée de l'activité du système, que celle-ci soit réussie, dégradée ou ait échouée*.

Dans le cadre des systèmes industriels, la sécurité consiste à mettre en œuvre des moyens évitant l'apparition de dangers. Elle s'énonce alors par l'absence de risque inacceptable, selon la norme IEC 61508 [IEC61508 98].

1.2.2 Notion de danger

La norme IEC 61508 [IEC61508 98] définit le danger comme une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction), à l'environnement, ou aux personnes.

Et selon le référentiel OHSAS 18001 [OHS18001 99]: "un danger est une source ou une situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments ". Les dangers liés à

un système sont inhérents au fonctionnement ou au dysfonctionnement du système, soit extérieur au système.

Selon Mazouni [MAZ 08], le danger se définit comme une propriété intrinsèque inhérente à un type d'entité ou un type d'évènement qui a la potentialité de provoquer un dommage.

Soulignons que de nombreux termes sont employés, selon les normes ou les auteurs, autour de la notion de danger et la rendent ambiguë. De plus, les dictionnaires associent souvent le terme danger au terme risque. En effet, plusieurs dictionnaires proposent le terme risque comme synonyme du terme danger, ce qui explique le fait qu'un grand nombre de personnes utilisent indifféremment ces termes. Même les documents et les textes officiels confondent danger et risque.

1.2.3 Risque

Le risque donne une mesure de la combinaison de deux facteurs qui sont la gravité d'un danger (ou sa conséquence) et la fréquence d'occurrence. Sa réduction peut être obtenue par la prévention (réduction de la fréquence d'occurrence) ou la protection (réduction de la gravité).

Selon [VIL 98], le risque est une mesure d'un danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences.

Et selon le référentiel OHSAS 18001 [OHS18001 99], un risque est la combinaison de la probabilité et de la (des) conséquence(s)de la survenue.

De manière plus formelle, un risque peut être mesuré par sa criticité, qui est fonction de sa probabilité et de sa gravité :

$$C = P \times G$$

Le critère de Farmer [FAR 67] permet de définir les notions de risque acceptables et inacceptables (figure 1.1).

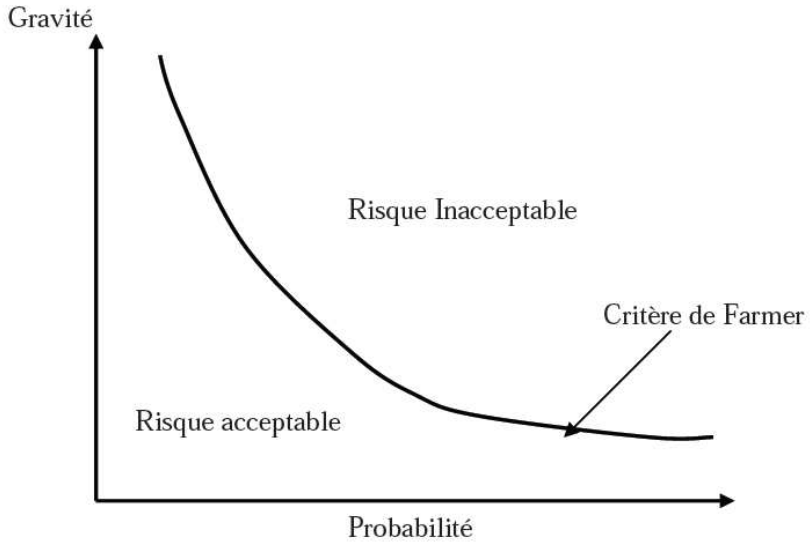


Figure 1.1 Courbe de Farmer [FAR 67]

La courbe de Farmer permet une classification du risque en deux sous-ensembles disjoints, correspondants au domaine du risque acceptable et à celui du risque inacceptable.

1.2.4 Sécurité fonctionnelle

La sécurité fonctionnelle a pour objet de contrôler les risques inacceptables qui pourraient provoquer des accidents dangereux. Elle couvre les systèmes mettant en œuvre des solutions de protection appliquées dans plusieurs domaines : mécanique, électrique, électronique, électronique programmable, hydraulique, optique, . . . [MEC 11]

Selon la norme IEC 61508 [IEC61508 98], *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.*

Selon la norme IEC 61511 [IEC61508 00], *la sécurité fonctionnelle est un sous-ensemble de la sécurité globale qui se rapporte à un système de commande de processus de base (BPCS, Base Process Control System) et qui dépend du fonctionnement correct du système instrumenté de sécurité et d'autres couches de protection* [MKH 08].

1.2.5 Système E/E/EP relatifs aux applications de sécurité

Les systèmes de 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.

[INN 08]

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.

Un système E/E/EP (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité, c'est-à-dire, depuis le capteur, en passant par l'unité logique de traitement, jusqu'à l'élément final (la partie actionneur), tout en tenant compte des actions de l'opérateur du système.

La norme IEC 61508 [IEC61508 98] peut être utilisée pour développer n'importe quel système E/E/EP comportant des fonctions critiques, telles que la protection des équipements, des biens ou de l'environnement.

1.3 Normes relatives aux systèmes instrumentes de sécurité

La norme internationale de sécurité IEC 61508 est une des dernières normes dédiées à la sécurité fonctionnelle. Elle est devenue avec ses normes filles les plus récentes et les plus connues des acteurs de la sécurité dans les secteurs industriels.

1.3.1 Norme IEC 61508 et ses normes filles

En 1984, le comité technique 65 de la CEI a commencé une tâche de définition d'une nouvelle norme internationale relative à la sécurité. Cette norme CEI 61508 [IEC61508 02] est la seule norme multisectorielle traitant de l'ensemble de la problématique des systèmes électriques, électroniques et programmables E/E/EP ; relies à la sécurité elle traite à la fois le matériel et le logiciel. C'est également la seule norme très technique qui apporte des clés, auxquelles il suffit de se conformer pour atteindre un objectif. Cette norme est orientée performances en laissant à l'utilisateur le soin de réaliser son analyse de risque et elle lui propose des moyens pour réduire ce risque. Elle ne concerne pas les systèmes simples, pour lesquels le mode de défaillance de chaque élément est clairement défini et pour lesquels le comportement du système peut être totalement déterminé dans le cas d'une défaillance. Par exemple, un système comportant des fins de course et des relais électromécaniques reliés à un disjoncteur peut être étudié sans avoir recours à la CEI 61508. La norme CEI 61508 repose

sur deux concepts qui sont fondamentaux vis-à-vis de son application : le cycle de vie en sécurité et les niveaux d'intégrité de sécurité.

Cette norme s'applique aux systèmes relatifs à la sécurité lorsque l'un ou plus de ces systèmes comporte des dispositifs électriques/électroniques/électroniques programmables. Elle comprend 7 parties (figure 2.1), afin de couvrir les multiples aspects des systèmes E/E/PE :

– 61508-1 : Prescriptions générales.

– 61508-2 : Prescriptions propres aux systèmes E/E/PE.

– 61508-3 : Prescriptions relatives au logiciel.

– 61508-4 : Définitions et abréviations.

– 61508-5 : Exemples de méthodes pour déterminer le niveau d'intégrité de la sécurité.

– 61508-6 : Guides pour l'application des parties 2 et 3 de la norme.

– 61508-7 : Tour d'horizon des techniques et des mesures.

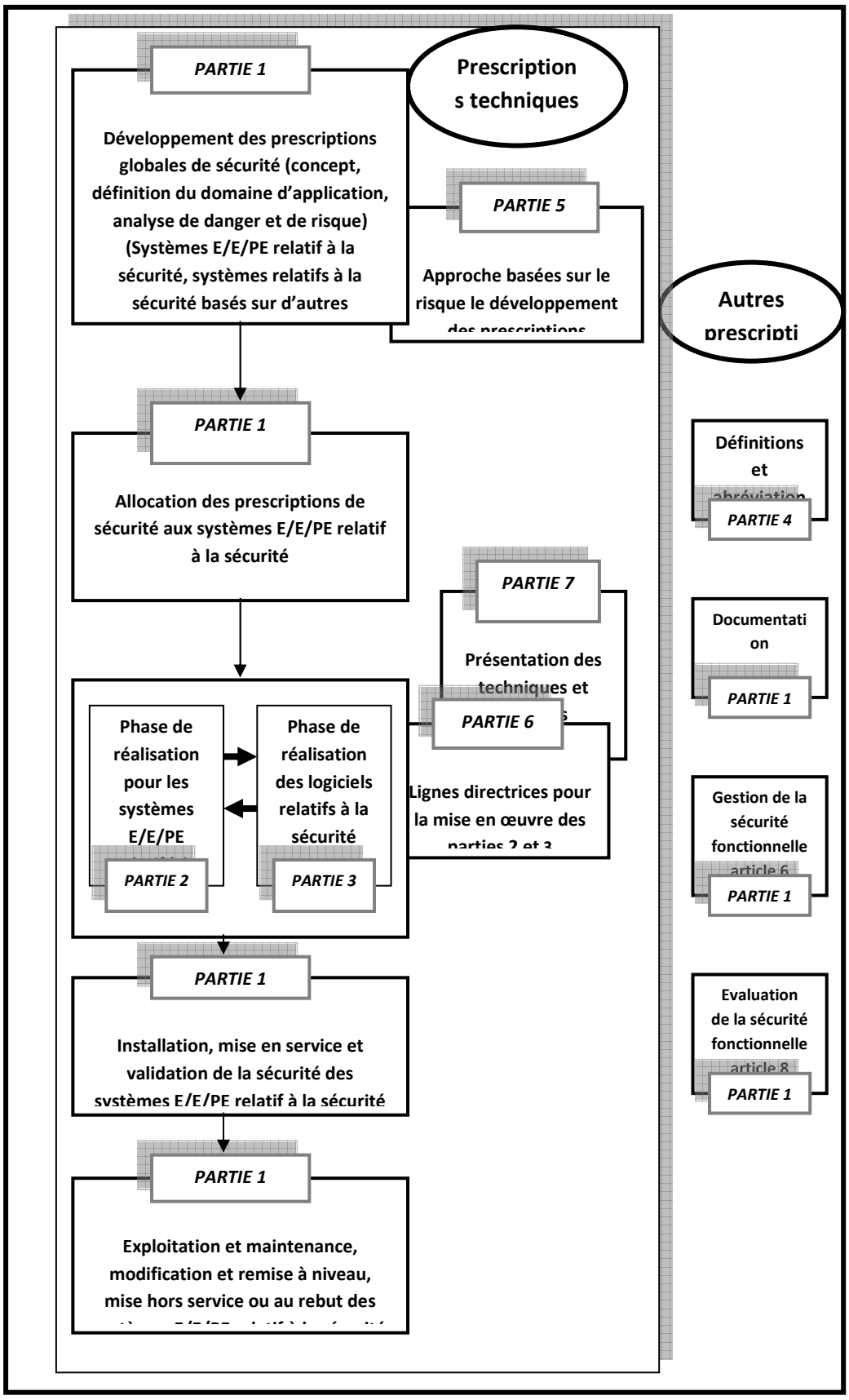


Figure 1.2 Structure générale de la norme IEC 61508 [IEC 61508 02]

La norme CEI 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 figure (figure 1.3) [RAU 06] montre la norme CEI 61508 générique et ses normes filles par secteur d'activité.

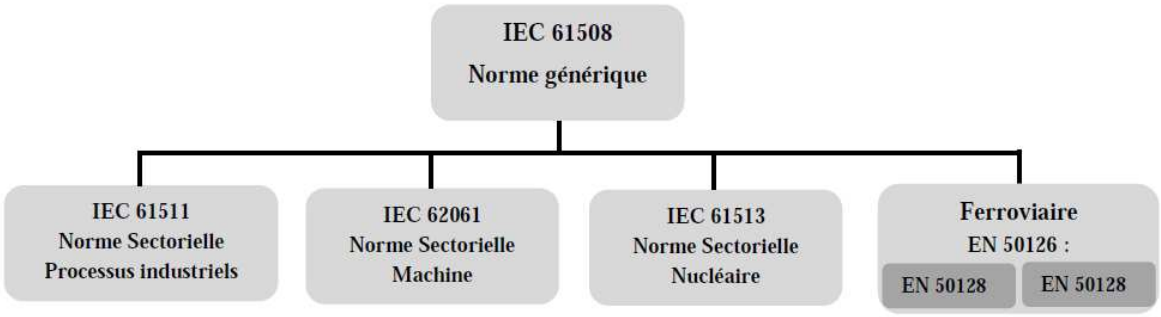


Figure 1.3 Norme CEI 61508 et normes dérivées [RAU 06]

1.3.2 La norme IEC 61511

La norme sectorielle CEI 61511 concerne les systèmes instrumentés de sécurité pour le secteur les processus industriels. Cette norme présente une approche relative aux activités liées au cycle de vie de sécurité, pour satisfaire à ces normes minimales. Cette approche a été adoptée afin de développer une politique technique rationnelle et cohérente. Dans la plupart des cas, la meilleure sécurité est obtenue par une conception de processus de sécurité intrinsèques, chaque fois que cela est possible, combinée, au besoin, avec d'autres systèmes de protection, fondés sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable) et qui couvrent tous les risques résiduels identifiés. Elle comprend trois parties :

1. Cadre, définitions, exigences pour le système, le matériel et le logiciel,

2. Lignes directrices pour l'application de la CEI 61511-1,

3. Conseils pour la détermination des niveaux exigés d'intégrité de sécurité.

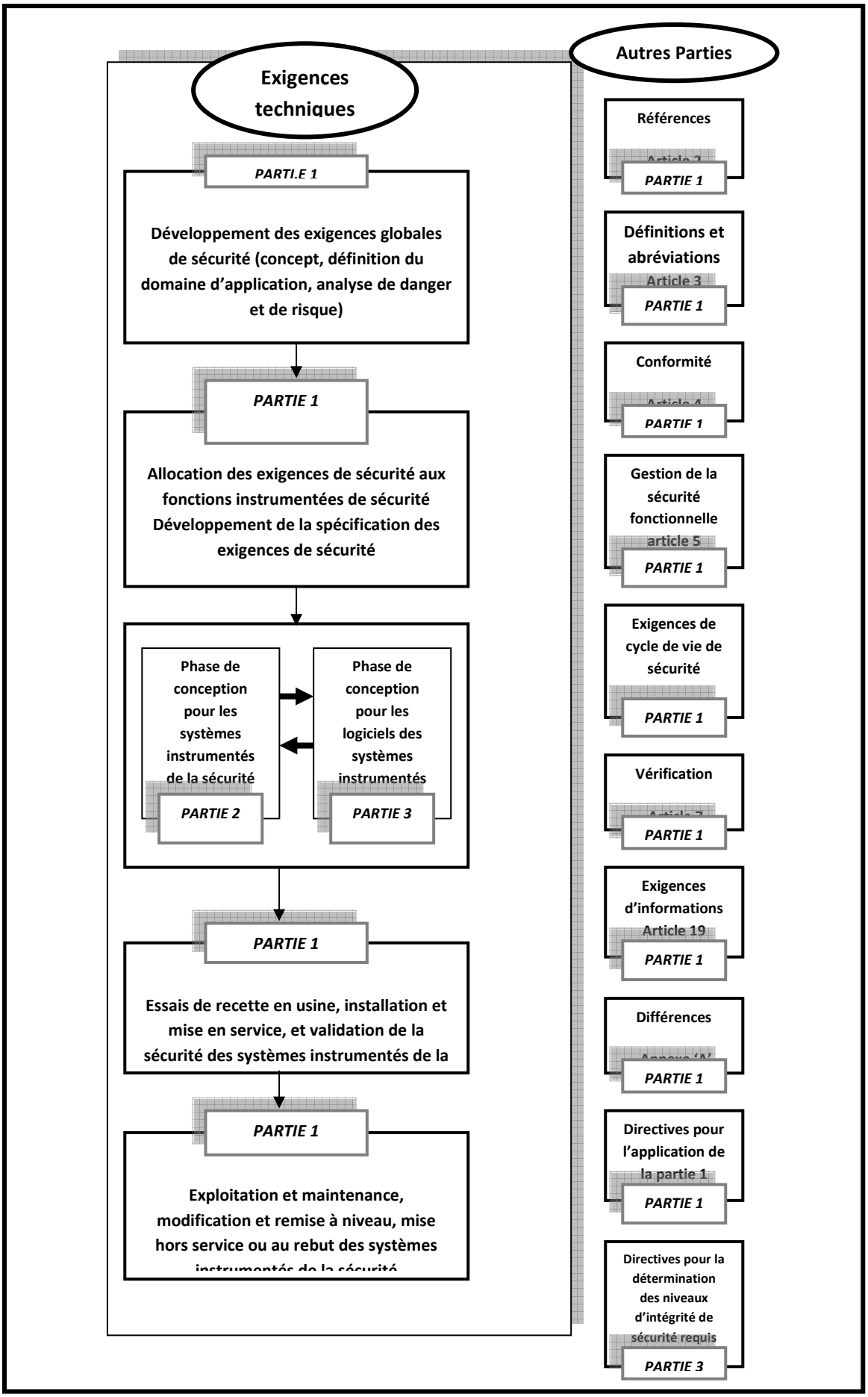


Figure 1.4 Structure générale de la norme IEC61511 [IEC61511 00]

Cette norme permet de définir des exigences relatives aux spécifications, à la conception, à l'installation, à l'exploitation et à l'entretien d'un SIS, afin d'avoir toute confiance dans sa capacité à amener le procédé dans un état de sécurité.

La norme CEI 61511 restreint le périmètre aux systèmes pour des applications SIL 1 à 3 (les applications SIL 4 ne pouvant être traitées par un SIS seul). Les applications qui nécessitent l'utilisation d'une fonction instrumentée de sécurité de niveau d'intégrité de sécurité SIL 4 sont rares dans l'industrie de processus. Ces applications doivent être évitées en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie de sécurité [IEC61511 03].

1.3.3 La norme IEC 62061

L'IEC 62061 [IEC62061 05] repose sur les mêmes concepts que ceux de l'IEC 61508 [IEC61508 98] . Elle est destinée à être utilisée par les concepteurs de machines et les fabricants de systèmes de commande électroniques relatifs à la sécurité de machines [IEC61513 01]. Elle concerne la spécification des prescriptions et fait des recommandations pour la conception, l'intégration et la validation de ces systèmes [SAL 07].

1.3.4 La norme IEC 61513

L'IEC 61513 [IEC61513 01] concerne le secteur de la sûreté des centrales nucléaires. Elle présente les prescriptions relatives aux systèmes de contrôle commande utilisés pour accomplir les fonctions de sécurité des centrales nucléaires. La conception des systèmes de contrôle commande peuvent être réalisés à l'aide d'une combinaison de composants traditionnels câblés à des composants informatiques. La conformité à l'IEC 61513 facilite la compatibilité avec les exigences de l'IEC 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire.

1.3.5 La norme EN 50126

La norme EN 50126 [EN50126 99] s'intéresse essentiellement aux applications ferroviaires. Elle permet de spécifier les principaux concepts de la sûreté de fonctionnement des systèmes tels que : la fiabilité, la disponibilité et la sécurité,. . . Cette norme est constituée de deux normes filles. L'EN 50128 [EN50128 01] est destinée à la partie logicielle des

systèmes de protection ferroviaire. L'EN 50129 [EN50129 98] concerne les systèmes électroniques de sécurité pour la signalisation [SAL 07].

1.4 Systèmes instrumentés de sécurité

1.4.1 Définition d'un SIS

La norme CEI 61511 [IEC61511 00] définit les systèmes instrumentés de sécurité de la façon suivante : système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal (aux).

La norme CEI 61508[IEC61508 98] définit quant à elle les systèmes relatifs aux applications de sécurité par : un système E/E/PE (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité.

Les systèmes instrumentés de sécurité sont donc utilisés comme moyens de prévention et comportent une proportion grandissante de systèmes électriques, électroniques ou encore électroniques programmables (E/E/EP). Ces systèmes sont complexes ce qui rend difficile dans la pratique la connaissance de chaque mode de défaillance par l'examen des comportements possibles et la prévision des performances en terme de sécurité.

Un système instrumenté de sécurité est un système visant à mettre le procédé en état stable ne présentant pas de risque pour l'environnement et les personnes lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu…) [SAL 07].

1.4.2 Constitution d'un SIS

Les SIS sont constitués de différents éléments unitaires reliés entre eux par des moyens de transmissions. Au minimum, on retrouve en série un capteur, une unité de traitement et un actionneur [AYA 05].

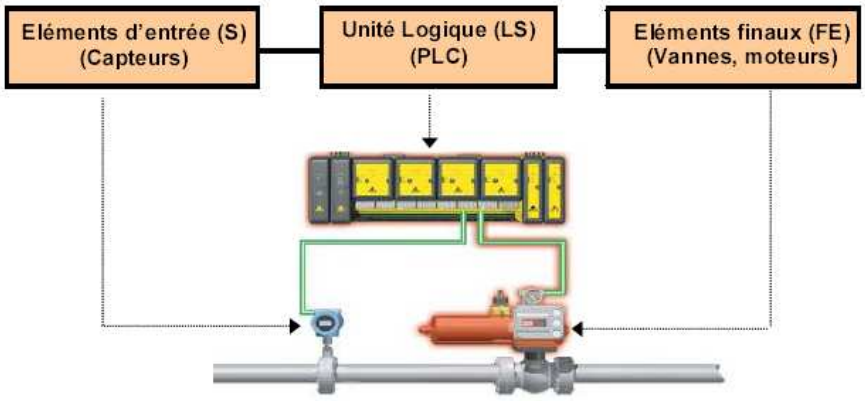


Figure 1.5 Schéma d'un SIS

A. Capteur :

Est un équipement qui délivre, à partir d'une grandeur physique, une autre grandeur, souvent électrique (tension, courant, résistance), fonction de la première et directement utilisable pour la mesure ou la commande [AYA05].

Cette grandeur physique peut être la température, la pression, le niveau, le débit, la concentration d'un gaz.

B. Unité de traitement :

La fonction "traitement" peut être plus ou moins complexe [AYA05]. Elle peut se résumer à acquérir une grandeur mesurée par un capteur et à l'indiquer. Elle peut également consister à activer la commande d'un ou plusieurs actionneurs à partir d'une fonction combinatoire des informations délivrées par différents capteurs. Les unités de traitement peuvent être classées en deux catégories selon leur technologie :

- Les technologies câblées, à base de composants logiques élémentaires (relais), liés entre eux électriquement (ou de manière pneumatique).
- Les technologies programmées, à base de centrales d'acquisition ou d'alarmes, d'automates programmables (API), de systèmes numériques de contrôle commande (SNCC), de calculateurs industriels ou de cartes électroniques à microprocesseurs.

C. Actionneurs :

Un actionneur peut être (vanne, moteur, servo-moteur…) transforment un signal (électrique ou pneumatique) en phénomène physique qui permet de commander le démarrage d'une pompe, la fermeture ou l'ouverture d'une vanne… Selon l'énergie motrice, on parle d'actionneur pneumatique, hydraulique ou électrique [AYA05].

Enfin, l'unité de traitement est reliée aux capteurs et aux actionneurs par des moyens de transmission. Il peut s'agir de câbles électriques, de lignes téléphoniques, d'ondes hertziennes (transmission par talkie-walkie…), ou de tuyauteries (transmission pneumatique ou hydraulique).

Les capteurs, l'automate et les actionneurs sont des équipements de sécurité. Un équipement de sécurité est un élément d'un SIS qui remplit une sous-fonction de sécurité.

Exemples :

- un capteur remplit la sous-fonction "détecter du gaz",
- une vanne motorisée la sous-fonction "juguler une fuite".

Associées au traitement, l'ensemble de ces sous-fonctions permet la réalisation de la fonction instrumentée de sécurité "maîtriser une fuite".

1.4.3 Fonction instrumentée de sécurité SIF

Les principales étapes de la norme IEC 61508 [IEC61508 98] et ses normes filles sont déclinées dans ce qu'on appelle le cycle de vie, c'est-à-dire que ces normes traitent depuis l'analyse des risques jusqu'à l'exploitation des fonctions de sécurité instrumentées SIF (Safety Instrumented Functions).

Une SIF est définie pour obtenir un facteur de réduction du risque mise en œuvre pour un SIS. Lorsque le SIS est considéré comme un système réalisant une barrière de protection fonctionnelle, cette barrière est considérée comme une fonction de sécurité [MKH 08], [CHA 02].

Une fonction instrumentée de sécurité est spécifiée pour s'assurer que les risques sont maintenus à un niveau acceptable par rapport à un événement dangereux spécifique.

Une fonction instrumentée de sécurité est à réaliser par un système instrumenté de sécurité (ou par une combinaison des composantes de ce système), par un système relatif à la

sécurité basé sur une autre technologie ou par un dispositif externe de réduction de risque. [MKH 08]

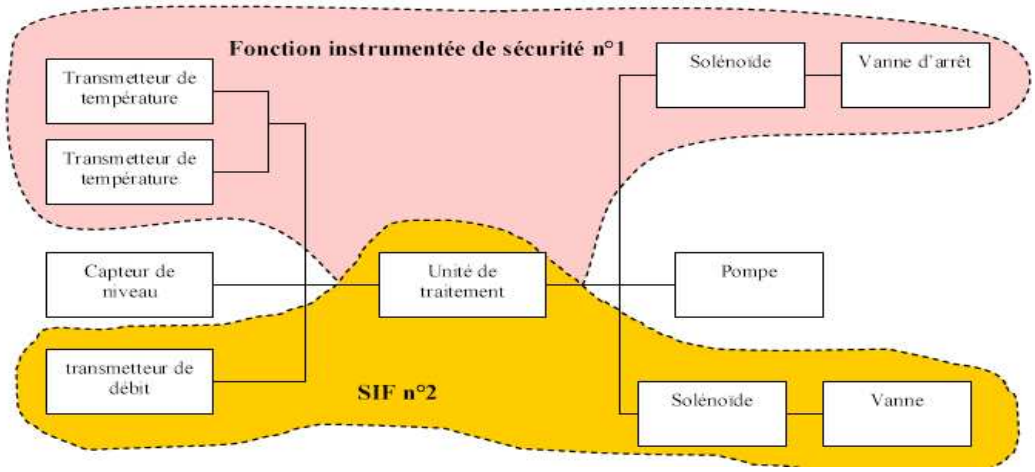


Figure 1.6 Fonction instrumentée de sécurité [MKH 08]

Pour illustrer et rendre plus claire cette définition, nous proposons l'exemple d'un équipement utilisé dans la fonction instrumentée de sécurité (Figure 1.7).

Cette dernière est conçue pour protéger un réservoir sous pression contenant un liquide inflammable lorsqu'une haute pression a lieu à l'intérieur du réservoir, cette fonction de sécurité agira selon deux procédures :

- Fermeture de la vanne pour arrêter l'alimentation du liquide.
- Arrêt de la pompe qui injecte le liquide dans le réservoir.

Il est indispensable de lister tous les composants intervenant à la réalisation de cette fonction instrumentée de sécurité, ces composants sont : Transmetteur de pression, solver, vanne, pompe.

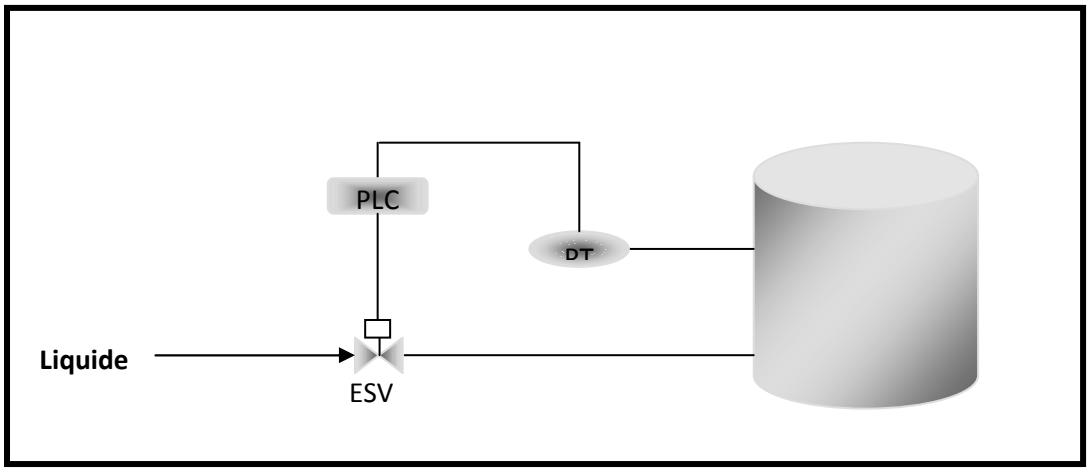


Figure 1.7 Exemple de fonction instrumentée de sécurité

1.4.4 Propriétés d'un SIS

Un certain nombre de propriétés caractérisent les systèmes instrumentés de sécurité :

- Les systèmes instrumentés de sécurité nécessitent une source d'énergie extérieure pour remplir leur fonction de sécurité.
- On retrouve tout ou partie de ces différents éléments pour constituer des chaînes de sécurité.
- Plusieurs capteurs ou actionneurs peuvent être reliés à une même unité de traitement.
- Toutes les combinaisons de capteurs, d'unité de traitement et d'actionneurs qui sont exigées pour accomplir des fonctions de sécurité sont considérées comme une partie de systèmes instrumentés de sécurité.
- Les capteurs, l'unité de traitement, les éléments finaux sont des équipements de sécurité et réalisent des sous-fonctions de sécurité. L'ensemble des sous-fonctions réalise la fonction de sécurité.

1.4.5 Niveau d'intégrité de sécurité (SIL)

Les normes de sécurité fonctionnelle IEC 61508 et IEC 61511 définissent une démarche d'analyse du niveau d'intégrité de sécurité (SIL) d'un système. Elles permettent de définir le niveau SIL qui doit être atteint par un SIS qui réalise la fonction de sécurité suite à une analyse de risque, [SAL 06a] [SCH 10]. Plus le SIL à une valeur élevée plus la réduction du risque est importante.

Les SIS sont classés en quatre niveaux SIL qui se caractérisent par des indicateurs discrets positionnés sur une échelle de un à quatre niveaux (Tableau 1.1). Les SILs sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisées par des systèmes E/E/EP relatifs à la sécurité selon la norme IEC 61508 [IEC61508 98]. Le SIL "quatre" désigne le degré de sécurité le plus élevée du fait de l'exigence forte de sécurité imposée et le niveau SIL "un" désigne l'exigence la plus faible [SCH 10].

Sollicitation	**Demande faible**	**Demande élevée**
SIL	**PFD_{avg}**	**PFH**
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$10^{-6} \leq PFH < 10^{-5}$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$10^{-7} \leq PFH < 10^{-6}$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$10^{-8} \leq PFH < 10^{-7}$
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$10^{-9} \leq PFH < 10^{-8}$

Tableau 1.1 Les différents niveaux de SIL définis par la norme IEC 61508 [IEC61508 98]

L'utilisation des niveaux SILs permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel menant aux évènements dangereux identifiés pendant l'analyse de risque [IEC61508 98] [SCH 10]. Les SILs sont attribués aux fonctions de sécurité sur la base de l'étude des défaillances.

Un SIS est en mode de fonctionnement à faible demande lorsque la fréquence de sollicitation est inférieure à une fois par an (1/an) ou inférieure au double de la fréquence des tests périodiques auxquels il est soumis. A partir de l'architecture du SIS réalisant la SIF faiblement sollicitée, la PFDavg est évaluée sur un intervalle [0, t].

Un SIS en mode de fonctionnement continu ou à forte demande implique une forte sollicitation du SIS. Il est considéré lorsque la fréquence de sollicitation est élevée ou continue, c'est-à-dire qu'elle est supérieure à une fois par an (1/an) ou supérieure à deux fois la fréquence des tests périodiques [IEC61508 98]. A partir de l'architecture du système instrumenté de sécurité réalisant la fonction instrumentée de sécurité fortement sollicitée, la PFH est évaluée sur un intervalle de temps [0, t] [IEC61508 98].

La norme IEC 61508 relative à l'évaluation de performance des SIS établit la classification des systèmes étudiés selon des niveaux de sécurité à partir du calcul de la PFDavg pour les SIS faiblement sollicités (moins d'une sollicitation par an) ou de la PFH dans le cas des SIS fortement sollicitées) [IEC61508 98], [MKH 08].

1.5 Détermination des niveaux de SIL requis

Un élément majeur développé dans les normes en question est l'évaluation quantitative de la performance du système de sécurité mis en œuvre et la qualification de cette performance par des niveaux référencés (Tableau 1.1) [SAL 07], [SAL 06a], [INN 08], [SIG 04], [SIG 06], [SIM 07].

L'évaluation du niveau d'intégrité de sécurité d'un SIS est déterminée par des méthodes qualitatives et quantitatives [SAL 06a], [SAL 08]. Elles permettent ; d'examiner les différents dangers provenant du système opérationnel et de déterminer le SIL de la SIF pour réduire la criticité du danger analysé. L'objectif global de ces méthodes est de décrire une procédure d'identification des SIF, d'établir les niveaux de sécurité correspondant et de les mettre en œuvre dans un SIS afin de ramener le procédé dans l'état de sécurité attendue [SAL 06a].

1.5.1 Les méthodes quantitatives

Les normes de sécurité fonctionnelle, l'IEC 61508 [IEC61508 98] et l'IEC 61511 [IEC61511 00], introduisent une approche probabiliste pour l'évaluation quantitative de la performance du SIS et la qualification de cette performance par des niveaux de sécurité référencés [SIG 06]. L'introduction de probabilité dans la mesure du niveau d'intégrité a entrainé la mise en place de concepts tels que les notions de calcul de probabilité de défaillance µa la sollicitation ou de défaillance par unité de temps [SIG 07].

L'évaluation de la performance des SIS doit être réalisée par l'utilisation de modèles adaptés. Différentes techniques sont néanmoins préconisées dans les annexes de la norme IEC 61508 [54]. Parmi les méthodes quantitatives citées, on trouve les équations simplifiées, les arbres de défaillances [SIG 06], les blocs diagramme fiabilité, les réseaux de Petri ainsi que les chaines de Markov [INN 08], [ZHA 03] ; [SAL 07]. La performance ainsi calculée permet de qualifier le niveau SIL du SIS selon les niveaux définis dans la norme (Tableau1.1).

1.5.1.1 Les équations simplifiées

Les normes de sécurité fonctionnelle n'imposent cependant pas l'utilisation de modèles particuliers mais fournissent des formules approchées pour les architectures courantes. En effet, la communauté des fiabilistes s'est rendue compte que certaines équations citées dans la norme IEC 61508-6 [IEC61508 98] ne sont valables que sous plusieurs hypothèses qui ne sont pas citées dans la norme [SIG 06]. En outre, ces formules ne sont valables que pour certains types d'architecture *k* parmi *n*. D'aprés Innal [IEC61508 98], les équations simplifiées sont utilisées pour l'étude d'architectures de SIS dont les canaux sont mutuellement indépendants et homogènes [IEC61508 98], [SIG 06].

Les équations simplifiées donnent la *PFDavg* du SIS en fonction de l'architecture des composants (1*oo*1 : un parmi un, 1*oo*2 : au moins un parmi deux, . . .) et des paramètres de fiabilité utilisés (taux de défaillances des composants ¸, taux de couverture de diagnostic *DC* et le facteur qui caractérise les défaillances des causes communes) [INN 08].

Comme mentionné par plusieurs chercheurs dans le domaine de la fiabilité des systèmes [SAL 06], [INN 08], il est nécessaire d'utiliser des méthodes de sureté de fonctionnement classiques telles que les diagrammes de fiabilité [RAU 04], les arbres de défaillances , ou les approches markoviennes pour évaluer les performances des SIS (la *PFDavg* et le SIL), plutôt que d'utiliser les équations simplifiées données dans la partie six de la norme IEC 61508 [IEC61508 98].

1.5.1.2 Blocs diagramme de fiabilité

La méthode de diagramme de fiabilité est une représentation de la logique de fonctionnement des systèmes. Cette méthode est basée sur l'utilisation de blocs pour représenter les composants, les sous-systèmes ou les fonctions. La modélisation consiste à rechercher les liens existants entre ces blocs [RAU 04]. Elle permet une analyse quantitative qui a pour objectif en particulier de définir la probabilité de bon fonctionnement d'un système. Les calculs reposent sur les probabilités de réussite des missions des éléments constituants le système. Cette méthode est utilisée dans l'évaluation des performances des SIS par le calcul de la *PFDavg* résultante et la détermination du son niveau SIL [GUO 06].

La méthode de bloc diagramme de fiabilité a ses limites d'application : il faut s'assurer de l'indépendance entre les différents états de fonctionnement, elle ne permet pas de modéliser des systèmes dynamiques, sauf sous certaines conditions.

1.5.1.3 Arbres de défaillance

La méthode des arbres de défaillance est l'une des méthodes les plus utilisées dans les analyses des performances des SIS [RAU 06], [SIG 07]. Elle a pour objectif le recensement des causes entrainant l'apparition de l'événement indésirable d'un système et le calcul de sa *PFDavg*. Elle constitue un moyen de représentation de la logique des défaillances, cette méthode est adaptée aussi pour l'étude des systèmes élémentaires présentant des défaillances de mode commun [VIL 98].

L'arbre de défaillances est une méthode déductive, qui commence par l'événement indésirable et détermine ses causes. L'analyse par l'arbre de défaillances nécessite deux phases ; une qualitative, où on détermine la fonction logique du système en terme de l'ensemble de ses coupes minimales, et l'autre est dite quantitative, où on calcule la probabilité d'occurrence de l'événement indésirable (sommet).

L'évaluation quantitative de la probabilité de l'événement sommet qui représente la défiabilité du système lorsque cet évènement est la défaillance d'un système non réparable [RAU 93], [SIG 04]. La méthode de l'arbre de défaillances consiste µa rechercher toutes les combinaisons possibles d'événements entraînant la réalisation de l'évènement indésirable.

On représente graphiquement ces combinaisons au moyen d'une structure arborescente dont l'évènement non désiré est le sommet (ou racine).

Pour décrire la relation entre les événements et la logique d'un système, l'arbre de défaillances utilise des portes logiques. Ces portes indiquent les types des évènements et les types de relation qui sont impliquées.

L'arbre de défaillances peut mener à des évaluations quantitatives de la probabilité d'occurrence de l'évènement indésirable qui représente la défiabilité lorsque cet évènement est la défaillance d'un SIS non réparable [VIL 98], [RAU 93].

1.5.1.4 Chaines de Markov

Les chaines de Markov apportent une bonne formalisation de tous les états que peuvent prendre les systèmes en fonction des événements rencontrés (défaillance, réparation,. . .) et des paramètres étudiés (taux de défaillance, défaillance de cause commune,. . .) [ZHA 03].

Les chaines de Markov apportent une finesse de modélisation pertinente au regard du comportement des SIS étudiés notamment les SIS faiblement sollicités et périodiquement

testés [SIG 07]. Compte tenu de la relative complexité des SIS, l'explosion combinatoire du nombre des états est l'inconvénient majeur des chaines de Markov. Cet inconvénient est généralement surmontable.

L'évaluation de la performance du SIS est obtenue grâce à une chaine de Markov synthétique représentant les différents états du SIS tout en tenant compte des différents types de défaillance. Elle permet de déterminer la probabilité de défaillance à la demande du SIS et de calculer sa valeur moyenne par intégration dans le temps. La détermination du niveau de sécurité du SIS est obtenue par référence aux données du tableau 1.1, [INN 08], [SAL 07], [SIG 07].

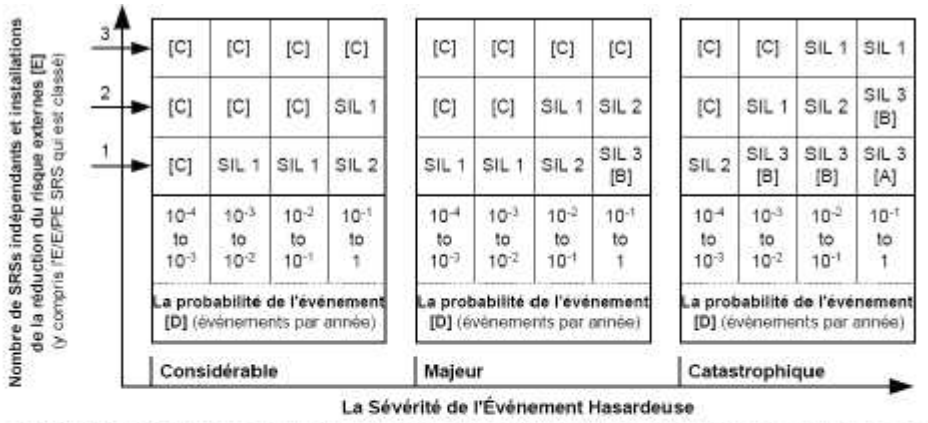
La méthode des chaines de Markov est souvent utilisée pour analyser et évaluer les per- formances des systèmes réparables et avec des composants à taux de défaillance constant. La construction d'un graphe de Markov consiste à identifier les différents états du système (défaillants ou non défaillants) et à chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une action de réparation. Elle permet ainsi de faire une analyse dynamique du système.

Dans l'évaluation des performances des systèmes par les chaines de Markov on utilise le processus d'analyse constitué de trois parties. La première partie est consacrée au classement de tous les états du système en états de fonctionnement, états dégradés ou états de panne. La deuxième partie concerne la détermination de toutes les transitions possibles entre ces différents états, tout en tenant compte des actions de réparations. Enfin on calcule les probabilités de se trouver dans les différents états du système étudié.

1.5.2 Les méthodes qualitatives

La norme IEC 61508 introduit des méthodes qualitatives qui permettent d'allouer le SIL à partir de la connaissance des risques associés au procédé. Les méthodes les plus utilisées sont la méthode du graphe de risque [BEU 07] [SAL 07], [SIM 07] et la méthode de la matrice de gravité des évènements dangereux [SAL 06a].

La matrice de risque intègre plusieurs fonctions de sécurité sous réserve de leur indépendance [IEC61508 98]. La matrice possède trois dimensions : la gravité, la probabilité d'occurrence de l'accident potentiel et le nombre de dispositifs de sécurité qui sont déjà mis en place pour empêcher le développement du danger en un accident [BEU 06]. La structure de la matrice de risque dépend du domaine spécifique d'activité [BEU 07].



[A] Un SIL 3 E/E/PE le système sécurité-apparenté ne fournit pas réduction du risque suffisante à ce niveau du risque. Les mesures de la réduction du risque supplémentaires sont exigées.

[B] Un SIL 3 E/E/PE le système sécurité-apparenté ne peut pas fournir réduction du risque suffisante à ce niveau du risque. Le hasard et risque l'analyse est exigée pour déterminer si les mesures de la réduction du risque supplémentaires sont nécessaires.

[C] Un E/E/PE indépendant que le système sécurité-apparenté n'est pas exigé probablement.

[D] La probabilité de l'événement est la probabilité que l'événement hasardeux se produit sans toute sécurité systèmes apparentés ou installations de la réduction du risque externes.

[E] SRS = système sécurité-apparenté. Probabilité de l'événement et le nombre total de couches de la protection indépendantes sont définis par rapport à la candidature spécifique.

Figure 1.8 Matrice de risque [IEC61508 98]

1.6 Méthode du graphe de risque

La méthode qualitative la plus utilisée pour déterminer le niveau de SIL est la méthode dite du « graphe de risque » [IEC 61508 00]. Quand cette méthode est adoptée, un certain nombre de paramètres de simplification sont introduits pour décrire la nature de la situation dangereuse lorsque les systèmes relatifs à la sécurité sont défaillants ou non disponibles. Un paramètre est choisi parmi quatre groupes caractéristiques du risque et les paramètres sélectionnés sont alors associés pour décider du niveau de SIL des systèmes relatifs à la sécurité. Ces quatre paramètres permettent de faire une gradation significative des risques et contiennent les facteurs clés d'appréciation du risque.

1.6.1 Synthèse du graphe de risque

La procédure simplifiée s'appuie sur l'équation suivante: R = f x C

Où: R est le risque en l'absence de systèmes relatifs à la sécurité, f est la fréquence de l'événement dangereux en l'absence de systèmes relatifs à la sécurité et C est la conséquence de l'événement dangereux.

La fréquence de l'événement dangereux f est supposée être le résultat de trois facteurs exerçant une influence :

· Fréquence et durée d'exposition dans une zone dangereuse ;

· La possibilité d'éviter l'événement dangereux ;

· La probabilité que l'événement dangereux se produise en l'absence de systèmes relatifs à la sécurité. C'est ce qu'on appelle la probabilité d'occurrence non souhaitée.

On obtient les quatre paramètres de risque suivants :

· Conséquence de l'événement dangereux (C) ;

· Fréquence et durée d'exposition au danger (F) ;

· Possibilité d'éviter l'événement dangereux (P) ;

· Probabilité de l'occurrence non souhaitée (W).

Paramètre		Description
Conséquence	**C**	Nombre d'accidents mortels et/ou de blessures graves pouvant résulter de l'occurrence de l'événement dangereux. Déterminé en calculant les nombres d'accidents dans la zone exposée lorsque celle-ci est occupée en tenant compte de la vulnérabilité à l'événement dangereux.
Occupation	**F**	Probabilité que la zone exposée soit occupée. Déterminée en calculant la fraction de temps d'occupation de la zone. Il convient de prendre en compte la possibilité d'une probabilité accrue de personnes se trouvant dans la zone exposée afin de rechercher les situations anormales pouvant exister lors de la progression vers l'événement dangereux.
Probabilité d'éviter le phénomène dangereux	**P**	Probabilité que des personnes exposées peuvent éviter la situation de phénomène dangereux qui existe si la fonction instrumentée de sécurité échoue à la sollicitation. Dépend s'il existe des méthodes indépendantes d'alerte des personnes exposées au phénomène dangereux et s'il existe des moyens pour y échapper.
Taux de demande	**W**	Nombre de fois par an que l'événement dangereux se produit si aucun système instrumenté de sécurité n'a été adapté. Peut être déterminé en considérant toutes les défaillances pouvant générer l'événement dangereux et en estimant le taux global d'occurrence.

Tableau 1.2 Descriptions des paramètres du graphe de risque [IEC61511 00]

1.6.2 Mise en œuvre du graphe de risque

En combinant les paramètres de risque décrits ci-dessus, on peut développer une courbe du risque comparable à celle présentée à la Figure 1.9.

Un exemple de classification des paramètres du graphe de risques est montré au tableau 1.3.

Paramètre		Classification
Gravité des Conséquences	C_A	Blessure mineure
	C_B	Blessure sérieuse ou victime
	C_C	Plusieurs victimes
	C_D	Grand nombre de victimes
Temps d'exposition (Occupation)	F_A	Rare
	F_B	Fréquent
Probabilité d'éviter le phénomène dangereux	P_A	Possible
	P_B	invraisemblable
Probabilité d'apparition d'un accident (Taux de demande)	W_1	Très faible probabilité
	W_2	Faible probabilité
	W_3	Forte probabilité

Tableau 1.3 Légende de la classification des paramètres du graphe de risque [IEC6108 98]

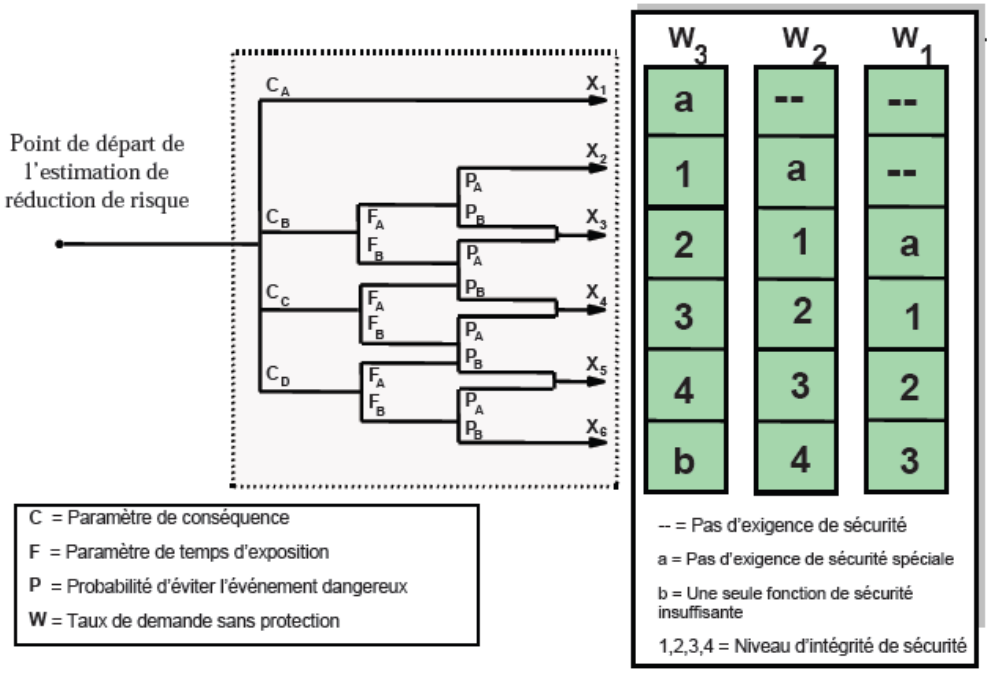


Figure1.9 Schéma général de graphe de risque [IEC6108 98]

Le graphe de risque s'explique de la manière suivante. L'utilisation des paramètres de risque C, F et P aboutit à un certain nombre de sorties, à savoir X1, X2, X3…Xn. La Figure 2 prend pour exemple une situation dans laquelle aucune pondération n'est appliquée aux pires conséquences. Chaque sortie est consignée dans une des trois échelles (W1, W2 et W3).

Chaque échelon indique le niveau de SIL nécessaire auquel doit satisfaire le système relatif à la sécurité pris en considération.

La mise en correspondance avec W1, W2 ou W3 permet de réaliser la contribution d'autres mesures de réduction du risque. Le décalage dans les échelles W1, W2 et W3 est nécessaire pour avoir trois niveaux différents de réduction des risques à partir d'autres mesures. Cette échelle est composée de l'échelle W1, qui fournit la réduction minimale du risque grâce à d'autres mesures (c'est-à-dire la plus forte probabilité de l'apparition d'un événement non désiré), l'échelle W2 une contribution moyenne et l'échelle W3 une contribution maximale. Pour une sortie spécifique du graphe de risque (c'est-à-dire X1, X2…ou X6) et, pour une échelle W spécifique (c'est-à-dire W1, W2 et W3) [SIM 06], la sortie finale du graphe de risque donne le niveau de SIL du SIS (c'est-à-dire 1, 2, 3 ou 4) et correspond à une mesure de la réduction nécessaire du risque pour le système.

A l'aide de ce graphe de risque, la fonction de sécurité à implanter pour prévenir un danger de faible probabilité sera réalisée en tenant compte des exigences relatives au SIL1.

Dans cet exemple les conséquences portent uniquement sur l'atteinte à la vie de personnes. La prise en compte des dégâts matériels et de dommages causés à l'environnement nécessite l'utilisation de graphes additionnels.

1.6.3 Etalonnage du graphe de risque

Les objectifs de la procédure d'étalonnage sont les suivants: [IEC61511 00]

a) Décrire tous les paramètres afin de permettre à l'équipe chargée d'établir le niveau d'intégrité de sécurité (SIL) de porter des jugements objectifs fondés sur les caractéristiques de l'application.

b) Garantir que le SIL choisi pour une application répond aux critères de risque définis par la société et qu'il tient compte de risques provenant d'autres sources.

c) Permettre de vérifier la procédure de sélection des paramètres.

L'étalonnage du graphe de risque est une procédure qui consiste à attribuer des valeurs numériques aux paramètres du graphe de risque. Ceci constitue la base pour l'évaluation du

risque lié au procédé et permet de déterminer l'intégrité requise de la fonction instrumentée de sécurité faisant l'objet de l'étude. A chacun des paramètres est attribuée une plage de valeurs de sorte que, lorsque ces paramètres sont combinés, ils permettent d'effectuer une évaluation nuancée du risque qui existe en l'absence de la fonction particulière de sécurité.

De ce fait, on détermine une mesure du degré de confiance à attribuer à la fonction instrumentée de sécurité. Le graphe de risque se rapporte à des combinaisons particulières de paramètres de risque et de niveaux d'intégrité de sécurité. La relation entre les combinaisons de paramètres de risque et de niveaux d'intégrité de sécurité est établie en considérant le risque tolérable associé aux dangers spécifiques.

1.6.4 Exemple d'étalonnage fondé sur des critères types

Le Tableau 1.4, qui fournit des descriptions et des plages de paramètres pour chaque paramètre, a été élaboré dans le but de répondre à des critères types pour les procédés chimiques tels que décrits plus haut. Avant de pouvoir utiliser cela dans le cadre d'un projet, il est important de confirmer qu'il répond bien aux besoins des personnes responsables de la sécurité. [IEC61511 00]

Paramètre de risque		Classification	Commentaires
Conséquence (C) Nombre d'accidents mortels Ce paramètre peut être calculé en déterminant le nombre de personnes présentes lorsque la zone exposée au danger est occupée et en multipliant par la vulnérabilité au danger identifié. La vulnérabilité est déterminée par la nature du danger contre lequel la protection est assurée. Les facteurs suivants peuvent être utilisés: V=0,01 Faible déversement ou dégagement de matériau inflammable ou toxique V=0,1 Important déversement ou dégagement de matériau inflammable ou toxique V=0,5 Comme ci-dessus, mais aussi une haute probabilité d'incendie ou matériau très toxique V=1 Rupture ou explosion	C_A C_B C_C C_D	Lésion mineure Plage de 0,01 à 0,1 Plage de >0,1 à 1,0 Plage > 1,0	1 Le système de classification a été établi pour traiter les blessures infligées aux personnes ou les décès. 2 Pour l'interprétation de C_A, C_B, C_C et C_D, il convient de tenir compte des conséquences de l'accident et du rétablissement normal
Occupation (F) Ce paramètre est calculé en déterminant la durée proportionnelle pendant laquelle la zone exposée au danger est occupée pendant les périodes normales de travail. NOTE 1 Si le temps de séjour dans la zone dangereuse est différent selon l'équipe d'exploitation, il convient alors de choisir le temps maximal. NOTE 2 L'utilisation du paramètre F_A n'est appropriée que s'il est possible de démontrer que le taux de sollicitation est aléatoire et qu'il n'est pas lié à la période durant laquelle l'occupation est supérieure à la normale. C'est habituellement le cas avec des sollicitations qui se produisent au moment du démarrage des équipements ou pendant la recherche d'anomalies.	F_A F_B	Exposition rare à plus fréquente dans la zone dangereuse. L'occupation est inférieure à 0,1 Exposition fréquente à permanente dans la zone dangereuse	3 Voir commentaire 1 ci-dessus.
Probabilité (P) pour que l'événement dangereux soit évité en cas de défaillance du système de protection.	P_A P_B	Adoptée si toutes les conditions de la colonne 4 sont remplies Adoptée si toutes les conditions ne sont pas remplies	4 Il convient de choisir P_A uniquement si toutes les conditions suivantes sont vraies: – des moyens sont prévus pour avertir l'opérateur de la défaillance du SIS ; – des moyens indépendants sont prévus pour arrêter le procédé afin d'éviter le danger ou pour permettre aux personnes d'être évacuées vers une zone sûre ; – le temps, entre le moment où l'opérateur est averti et le moment où un événement dangereux se produit, dépasse 1 h ou est finalement suffisant pour entreprendre les actions nécessaires.
Taux de sollicitation (W). Le nombre de fois par an où l'événement dangereux est susceptible de se produire en l'absence d'un SIS. Pour déterminer le taux de sollicitation, il est nécessaire de considérer toutes les sources de défaillance susceptibles de provoquer un événement dangereux. Lors de la détermination du taux de sollicitation, il faut accorder une confiance limitée aux performances et à l'intervention du système de commande. Les performances, qui peuvent être revendiquées si le système de commande n'est pas conçu et entretenu conformément à la CEI 61511, sont limitées à des valeurs inférieures aux plages de performances associées au niveau d'intégrité de sécurité SIL1	W_1 W_2 W_3	Taux de sollicitation inférieur à 0,1D par an Taux de sollicitation entre 0,1D et D par an Taux de sollicitation entre D et 10D par an Pour des taux de sollicitation supérieurs à 10D par an, une intégrité plus élevée est nécessaire	5 Le but du facteur W est d'estimer la fréquence du danger qui apparaît sans l'ajout du SIS. Si le taux de sollicitation est très élevé, le SIL doit être déterminé par une autre méthode ou le graphe de risque doit être étalonné une nouvelle fois. Il convient de noter qu'il est possible que les méthodes utilisant des graphes de risques ne constituent pas la meilleure approche dans le cas d'applications fonctionnant en mode continu, se reporter au paragraphe 3.2.43.2 de la CEI 61511–1. 6. Il convient de déterminer la valeur de C à partir de critères propres à la société concernant le risque tolérable en tenant compte d'autres risques auxquels des personnes peuvent être exposées.

Tableau 1.4 Exemple d'étalonnage du graphe de risque général [IEC61511 00]

1.7 Conclusion

Dans ce chapitre nous avons d'abord rappelé la définition de certains concepts utilisés dans le cadre de la sécurité fonctionnelle des systèmes de sécurité. Une brève description des normes relatives aux systèmes de sécurité est donnée, suivie d'une description des différentes méthodes utilisées pour déterminer le SIL d'un SIS.

Rappelons dans le cadre de ce travail la méthode du graphe de risque est choisi comme approche d'évaluation du SIL. Cependant le graphe de risque présente certaines difficultés dans la définition et l'interprétation des paramètres du graphe, ce qui peut conduire à des résultats incohérents qui peuvent entrainer du conservatisme quant aux valeurs du niveau du SIL [NAI 09]. Pour surmonter cette difficulté, un modèle du graphe de risque est développé qui est l'objet du prochain chapitre.

2

Approche floue du graphe de risque

2.1 Introduction

Le graphe de risque est parmi les méthodes les plus utilisées pour déterminer le niveau de SIL, les paramètres de ce dernier sont associés pour décider du niveau de SIL du système. Les quatre paramètres permettent de faire une gradation significative du risque. Cependant, les connaissances dont nous disposons concernant les paramètres sont généralement imparfaites.

Cela exige des méthodes qui permettent la modélisation et la manipulation de ces imperfections. À cet égard, plusieurs théories de représentation des connaissances imparfaites ont été développées : la théorie des probabilités, la théorie des ensembles flous, la théorie des possibilités et la théorie de l'évidence. [ZAD 97] [MAS 92]

Nous nous sommes fixé comme objectif dans le cadre du présent chapitre, de montrer l'intérêt de la théorie des ensembles flous dans l'évaluation de SIL en présence d'informations incertaines en proposant un modèle du graphe de risque flou.

2.2 Représentation des connaissances imparfaites

2.2.1 Formes d'imperfection des connaissances

Les connaissances dont nous disposons sur un système quelconque, pris au sens d'un ensemble d'éléments en relation les uns avec le autres et interférant avec leur environnement, sont en général imparfaites [BOU 95].

Dans la littérature, nous distinguons principalement deux sortes d'imperfection de connaissances [DUB 94] : *l'incertitude* et *l'imprécision*. Les connaissances sont incertaines quand nous avons un doute sur leur validité. Si nous éprouvons une difficulté à les exprimer clairement, elles sont alors imprécises. Bouchon-Meunier [BOU 95] considère que l'imperfection dans les connaissances peut être divisée en trois formes principales :

- Les incertitudes qui représentent un doute sur la validité d'une connaissance ;
- Les imprécisions qui correspondent à une difficulté dans l'énoncé ou dans l'obtention de la connaissance. Ces imprécisions sont aussi appelées « incertitudes du type épistémique » [HEL 04] ;
- Les incomplétudes qui sont des absences totales ou partielles de connaissances sur certaines caractéristiques du système.

En anglais, nous employons souvent le terme "Uncertainty" pour désigner les connaissances imparfaites en général, alors que le terme "Imprecision" utilisé pour désigner les connaissances imprécises est rarement cité. Ces deux formes d'imperfection sont souvent intimement mêlées, mais n'ont cependant pas présenté la même importance dans les préoccupations scientifiques.

2.2.2 Esquisse des théories de représentation des connaissances imparfaites

En ce qui concerne l'incertain, il a d'abord été abordé par la notion de probabilité dès le XVII^{me} siècle par Pascal et Fermat [KOL 60]. La théorie des probabilités fournit une structure mathématique pour l'étude des phénomènes qui présentent des incertitudes aléatoires. Le problème de l'imprécision a été traité par le calcul d'erreurs, restreint aux imprécisions de caractère numérique. En 1965, Lotfi Zadeh [ZAD 65], professeur à l'université de Berkley en Californie, a introduit la notion de sous-ensemble flou (en anglais "Fuzzy set") dans une généralisation de la théorie classique des ensembles. Il a ensuite introduit, à partir de 1978 [ZAD 78], la théorie des possibilités qui a été développée par

Dubois et Prade [DUB 88]; elle permet de traiter les incertitudes sur les connaissances. L'association de la théorie des possibilités à la théorie des ensembles flous permet le traitement des connaissances à la fois imprécises et incertaines. La théorie des fonctions de croyances permet aussi de traiter ces deux types d'imperfections [DEM 67], elle est basée sur la modélisation et la quantification de la crédibilité attribuée à des faits. Elle définit le degré avec lequel un événement est crédible ou plausible.

La théorie des probabilités qu'a bénéficié de quatre siècles de travaux et reposant donc sur des fondements mathématiques et une expérience solides, constitue le plus ancien formalisme permettant de traiter les incertitudes dans les connaissances imparfaites. C'est un outil efficace pour le traitement des incertitudes aléatoires et les cas où nous disposons d'une bonne connaissance des événements et de leurs événements contraires. Elle ne peut cependant pas traiter les imprécisions qui sont une autre forme d'imperfection des connaissances [BAU 05].

Nous allons introduire dans ce qui suit, la notion des ensembles flous qui permet de traiter, de façon souple, l'aspect imprécis et vague des connaissances imparfaites.

2.3 Théorie des ensembles flous

Dans cette section, nous présentons succinctement les concepts fondamentaux de la logique floue qui sont en relation avec les travaux du présent mémoire. Pour plus de détails, on pourra consulter, avec profit, entre autres, les références [BOU 95], [DUB 80], [KAU 77], [ZAD 65], [ZAD 75], [ZAD 78], [ZAD 92].

2.3.1 Notion d'ensemble flou

Le concept d'ensemble flou [ZAD 65] a été introduit pour éviter les passages brusques d'une classe à une autre (de la classe blanche à la classe noir, par exemple) et permettre l'appartenance partielle à chacune d'elles (avec un fort degré à la classe blanche et un faible degré à la classe noir dans le cas du gris clair, par exemple). La définition de l'ensemble flou répond au besoin de représenter des connaissances imprécises telles que celles exprimées en langage naturel (i.e., linguistique) par un voyageur (ex., le trajet est long, le train est rapide, …). Le caractère graduel des ensembles flous est basé sur l'idée que, plus en se rapproche de la caractérisation typique d'une classe, plus l'appartenance à cette classe est forte (ex., 20 ans caractérise bien la jeunesse, 60 ans ne caractérise plus cette classe d'age).

Le concept d'ensemble flou permet de traiter :

- des classes aux limites mal définies (catégories d'appréciation perçue par un observateur) ;
- des classes intermédiaires entre le tout et le rien (ex., "presque certain") ;
- le passage progressif d'une classe à une autre (ex., du "petit" au "grand", du "faible" au "fort") ;
- des valeurs approximatives (ex., "autour de 13 de moyenne", "environ 5m de distance").

■ *Définition*

Soit U un ensemble référentiel et soit x un élément de U. Un ensemble A de U est défini par une fonction d'appartenance $\mu_A(x)$ qui prend ses valeurs dans l'intervalle [0, 1]. Cette fonction donne le degré d'appartenance de x dans A. Un ensemble ordinaire est un cas particulier de l'ensemble flou ($\mu_A(x)$ ne prend que 0 et 1). Formellement, l'ensemble flou A peut s'écrire comme :

$$A = \{(x, \mu_A(x)) / x \in U\} \tag{2.1}$$

■ *Exemple*

Soit à apprécier le confort lié à la conduite d'une voiture qui circule sur une autoroute. Ce confort est vu sous l'angle de la vitesse variant entre 30 et 130 km/h. En termes de la théorie des ensembles flous, la caractérisation « conduite confortable » peut être décrite par un ensemble flou défini sur un univers de vitesses. À ces dernières seront affectés des scores selon la compatibilité avec cette caractérisation. Supposons qu'un conducteur cote la conduite confortable (CC) comme suit :

Vitesse (km/h)	30	40	50	60	70	80	90	100	110	120	130
Degré de confort	0	0.2	0.4	0.5	0.8	1	0.9	0.4	0.3	0.2	0

Ces résultats montrent que les vitesses faibles (≤ 60 km/h) et les vitesses élevées (≥ 80 km/h) sont désagréables et confèrent une conduite inconfortable ; la conduite 80 km/h correspond à une conduite hautement confortable. Les valeurs des différents degrés de confort sont en fait les valeurs de la fonction d'appartenance $\mu_{cc}(v)$ de l'ensemble flou CC (Figure 2.1)

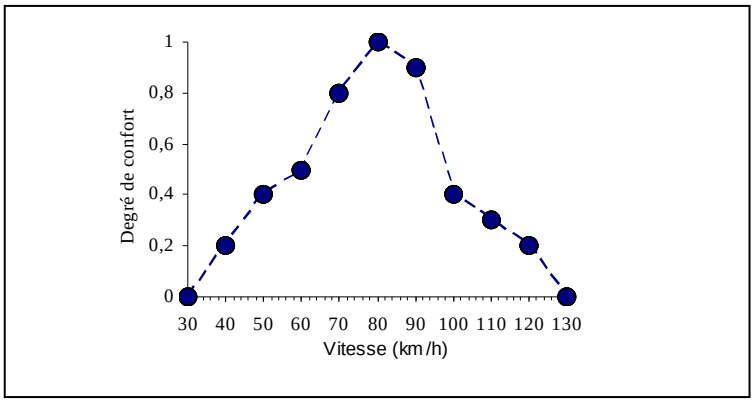


Figure 2.1 L'ensemble flou « conduite confortable »

2.3.2 Propriétés d'un ensemble flou

Les caractéristiques de l'ensemble flou de *U* les plus utiles pour le décrire sont celles qui montrent à quel point il diffère d'un ensemble classique de *U*. Citons les caractéristiques suivantes :

- *Support* d'un ensemble flou : le support d'un ensemble flou, noté *supp*(*A*), est l'ensemble des éléments de *U* qui appartiennent, au moins un peu, à *A*. C'est la partie de *U* sur laquelle la fonction d'appartenance de *A* n'est pas nulle :

$$\sup p(A) = \{x \in U \,/\, f_A(x) \neq 0\}. \tag{2.2}$$

- *Hauteur* d'un ensemble flou : la hauteur, notée *h* (*A*), d'un ensemble flou est le plus fort degré avec lequel un élément de *U* appartient à *A*, c'est-à-dire la plus grande valeur prise par sa fonction d'appartenance.

$$h(A) = \sup_{x \in X} f_A(x). \tag{2.3}$$

- Ensemble flou *normalisé* :
  l'ensemble flou *A* de *U* est dit normalisé si sa hauteur *h*(*A*) est égale à 1.

- *Noyau* d'un ensemble flou : le noyau de l'ensemble flou normalisé *A*, noté *noy*(*A*), est l'ensemble des éléments de *U* pour lesquels la fonction d'appartenance de *A* vaut 1.

$$noy(A) = \{x \in U \,/\, f_A(x) = 1\}. \tag{2.4}$$

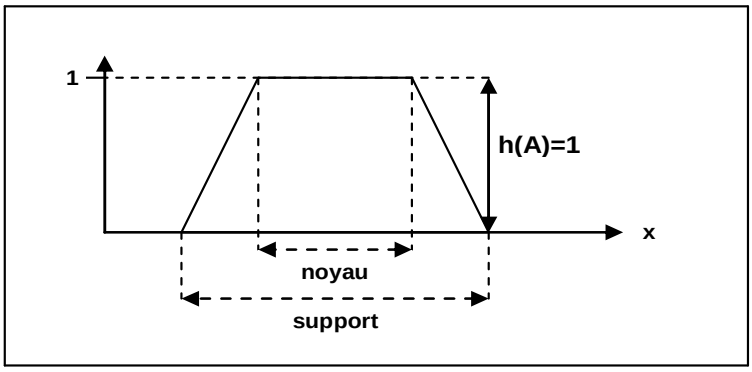


Figure 2.2 Support, Hauteur et Noyau d'un ensemble flou

2.3.3 Fonctions d'appartenance

Les ensembles flous peuvent être définis en leur affectant une fonction continue pour décrire analytiquement ou graphiquement l'appartenance. De ce fait, la représentation des ensembles flous dépend du type de la fonction d'appartenance retenu. Zadeh a proposé une série de fonctions d'appartenance scindée en deux groupes : les fonctions d'appartenance «linéaires» et les fonctions d'appartenance « courbées » ou de forme « gaussienne ».

- La fonction d'appartenance Triangulaire (générale et symétrique) ;
- La fonction d'appartenance Singleton (gauche et droite) ;
- La fonction d'appartenance Gamma (générale et linéaire) ;
- La fonction d'appartenance Trapézoïdale (gauche et droite) ;
- La fonction d'appartenance Gaussienne (gauche et droite ou pseudo exponentielle).

Les fonctions d'appartenance les plus répandues sont illustrées par la figure 2.3.

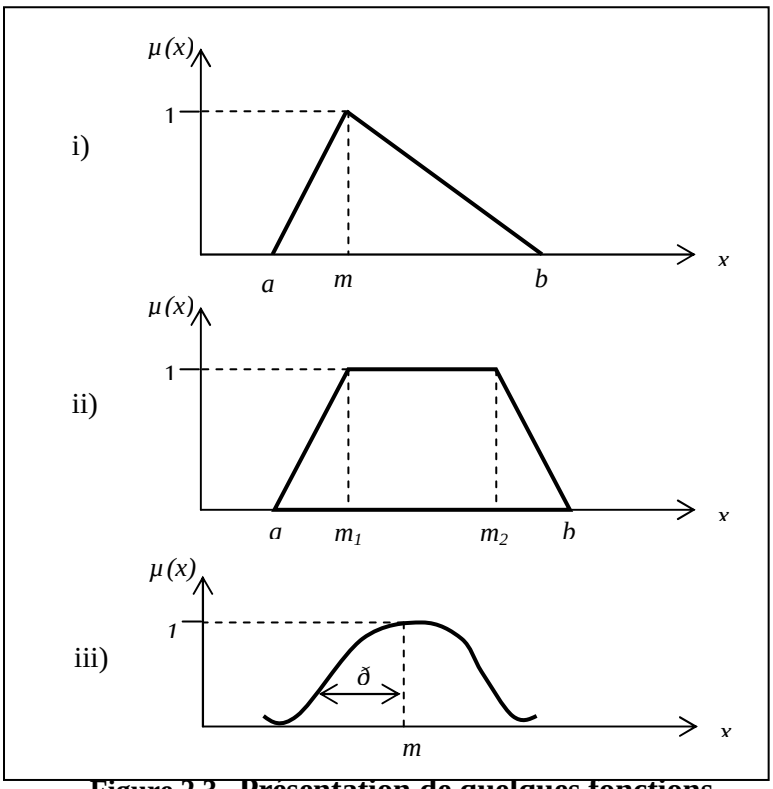


Figure 2.3 Présentation de quelques fonctions d'appartenance :
i) Triangulaire ;
ii) Trapézoïdale ;
iii) Gaussienne.

- La fonction d'appartenance Triangulaire de la figure (2.3.i) est exprimée comme suit:

$$\begin{aligned}\mu(x) &= \frac{(x-a)}{(m-a)}; a \le x \le m,\\ &= 1;\ x = m,\\ &= \frac{b-x}{b-m};\ m < x \le b.\end{aligned} \tag{2.5}$$

- La fonction d'appartenance Trapézoïdale de la figure (2.3.ii) est exprimée comme suit :

$$\begin{aligned}\mu(x) &= \frac{(x-a)}{(m_1-a)}; a \le x < m_1,\\ &= 1;\ m_1 \le x \le m_2,\\ &= \frac{b-x}{b-m_2};\ m_2 < x \le b.\end{aligned} \tag{2.6}$$

- La fonction d'appartenance Gaussienne de la figure (II.3.iii) est exprimée comme suit :

$$\mu(x) = \exp\left(\frac{(-x-m)^2}{2\sigma^2}\right). \tag{2.7}$$

2.3.4 Opérations sur les ensembles flous

La théorie des ensembles flous propose plusieurs opérateurs ensemblistes. Les principaux opérateurs et relations flous sont présentés ci-dessous [ZAD 65].

i. Inclusion : On dit que *A* est inclus dans *B*, et on note $A \subseteq B$, si et seulement si :

$$\forall x \in U \qquad \mu_A(x) \leq \mu_B(x) \tag{2.8}$$

ii. Egalité : On dit que *A* et *B* sont égaux, et on note *A* = *B*, si et seulement si :

$$\forall x \in U \qquad \mu_A(x) = \mu_B(x) \tag{2.9}$$

iii. Complémentation : On dit que *A* et *B* sont complémentaires, et on note $A = \overline{B}$ ou $\overline{A} = B$, si et seulement si :

$$\forall x \in U \qquad \mu_B(x) = 1 - \mu_A(x) \tag{2.10}$$

iv. Intersection : On définit l'intersection de *A* et *B*, et on note *A* ∩ *B*, par le plus grand ensemble flou de contenu à la fois dans *A* et *B*, c'est-à-dire :

$$\forall x \in U \qquad \mu_{A \cap B}(x) = \min\left(\mu_A(x), \mu_B(x)\right) \tag{2.11}$$

v. Réunion : On définit l'union ou la réunion de *A* et *B*, et on note *A* U *B*, par le plus petit ensemble flou de *U* qui contient à la fois *A* et *B*, c'est-à-dire :

$$\forall x \in U \qquad \mu_{A \cup B}(x) = \max\left(\mu_A(x), \mu_B(x)\right) \tag{2.12}$$

Toutes ces opérations sont des extensions des opérations ensemblistes usuelles avec lesquelles elles coïncident si les ensembles considérés sont des ensembles usuels. Les extensions de ces opérations aux ensembles flous ne sont pas uniques [KAU 77].

La figure 2.4 illustre les opérations d'intersection, de réunion et de complémentation.

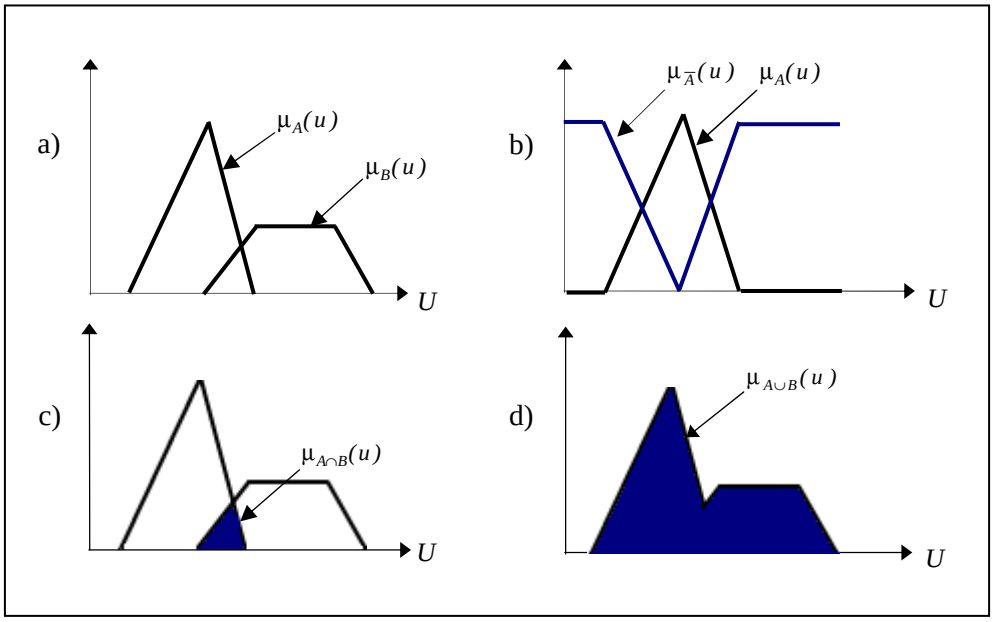


Figure 2.4 Illustration de quelques opérations sur les ensembles flous:

a) Ensembles flous A et B
b) $\overline{A}$
c) $A \cap B$
d) $A \cup B$.

L'algèbre des ensembles flous est la même que celle des ensembles ordinaires, sauf que le tiers-exclu n'est plus vérifié. En effet, on y retrouve les opérations suivantes :

a) Commutativité :

$$A \cap B = B \cap A$$
$$A \cup B = B \cup A \tag{2.13}$$

b) Associativité :

$$A \cap (B \cap C) = (A \cap B) \cap C$$
$$A \cup (B \cup C) = (A \cup B) \cup C \tag{2.14}$$

c) Distributivité :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{2.15}$$

d) Involution :

$$\overline{\overline{A}} = A \tag{2.16}$$

e) Lois de De Morgan :

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$
$$\overline{A \cup B} = \overline{A} \cap \overline{B} \tag{2.17}$$

Le tiers-exclu n'étant pas vérifié par les ensembles flous (Fig. II.5) :

$$A \cap \overline{A} \neq \phi$$
$$A \cup \overline{A} \neq 1_U \tag{2.18}$$

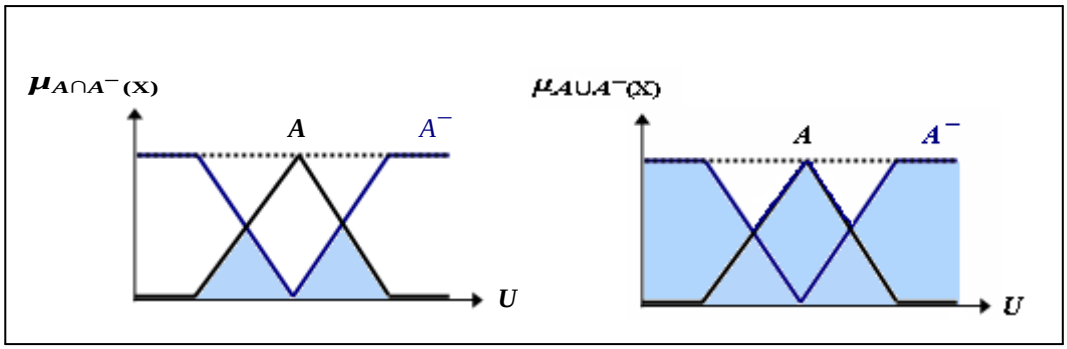


Figure 2.5 Illustration de la propriété du tiers-exclu:

2.3.5 Notion de variable linguistique

Le concept de variable linguistique [ZAD 75] est utilisé dans la caractérisation des phénomènes qui sont si complexes ou si mal définis qu'ils ne peuvent pas être décrits par des termes quantitatifs conventionnels. Ainsi, les valeurs de la variable linguistique sont des termes linguistiques du langage naturel, lesquelles sont modélisées par des ensembles flous.

Plus spécifiquement, ces derniers représentent des restrictions sur les valeurs de la variable linguistique et peuvent être vus comme résumant les différentes catégories d'éléments d'un univers de discours (i.e., l'ensemble référentiel). D'une manière générale, une variable linguistique est caractérisée par un 5-uplet (L, $T(L)$, Gr, Mr) où :

- L est le nom de la variable linguistique ;
- $T(L)$ est l'ensemble des termes, i.e., les noms des variables linguistiques de L, dont chacune d'elles représente un ensemble flou défini sur un univers U ;
- Gr est une règle syntaxique, généralement de la forme d'une grammaire, utilisée pour générer les noms des valeurs de L ;
- Mr est une règle sémantique qui associe à chaque nom un sens $Mr(X)$ qui est un ensemble flou de U.

■ *Exemple*

Reprenons l'exemple de la sous-section 2.3.1 et supposons que le « confort » est une variable linguistique L. Il en ressort que

- l'ensemble des termes est $T(L)$ = {inconfortable$_-$, confortable, inconfortable$_+$}. Chacun des qualificatifs représente une valeur linguistique de L décrite par un ensemble flou dans un référentiel de vitesses U = [30, 130] (km/h) ;
- la règle sémantique *Mr* associe la valeur « inconfortable » aux vitesses inférieures à 60 km/h et supérieures à 100 km/h et la valeur « confortable » aux vitesses comprises entre 70 et 90 km/h, selon des ensembles flous trapézoïdaux (un choix issu d'une expertise). La représentation de la variable « confort » est visualisée sur la figure suivante :

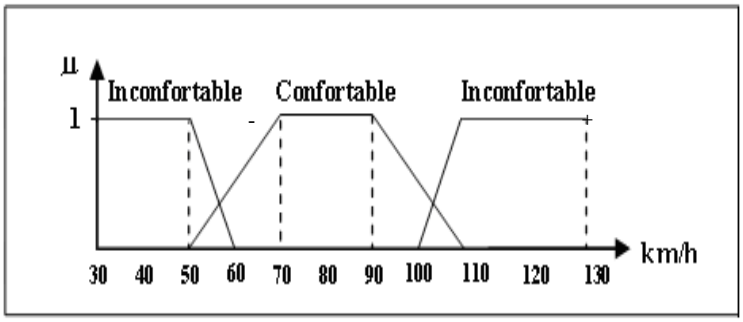


Figure 2.6 Représentation de la variable linguistique « confort »

2.3.6 Système d'inférence de Mamdani

2.3.6.1 A propos des systèmes d'inférence

A l'opposé des méthodes quantitatives qui requièrent des équations pour modéliser les comportements des systèmes réels, la logique floue, elle, peut caractériser ces comportements moyennant le concept de variable linguistique et les règles floues grâce au concept d'ensemble flou et aux techniques d'inférence floue.

Les systèmes d'inférence floue ont fait preuve de nombreuses applications et dans plusieurs domaines tels que le contrôle automatique, le traitement de données, l'analyse de décision, les systèmes experts, et les études de sécurité [NAI 09].

Parmi ces systèmes d'inférence, celui proposé par Mamdani et Assilian [MAM 75] est le plus rencontré dans la résolution des problèmes à base de règles floues. Basée sur une technique simple utilisant l'inférence max-min, la méthode de Mamdani a été introduite avec succès dans plusieurs champs d'application allant des processus de contrôle jusqu'au diagnostic médical.

La méthodologie générale des Systèmes d'Inférence Floue est donnée par la figure 2.7.

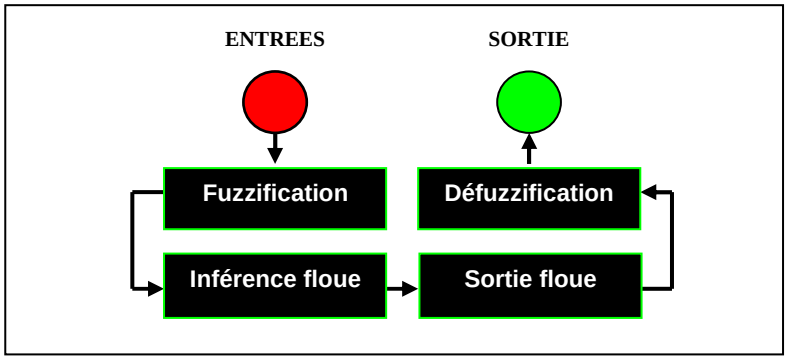


Figure 2.7 Organigramme du Système d'Inférence Floue

2.3.6.2 Méthodologie du système d'inférence de Mamdani

Le système d'inférence de Mamdani peut être décrit comme suit [MAM 75]:

Supposons une base de règles constituée de n Si/Alors règles floues avec des entrées multiples et une sortie unique (Multiple Inputs and Single Output : MISO). Chaque règle R_i (i =1, …, n) est donc de la forme :

$$R_i : \text{si } X_1 \text{ est } A_{i1} \text{ et } \ldots \text{ et } X_m \text{ est } A_{im} \text{ alors } Y \text{ est } B_i; \qquad (2.19)$$

Où les X_j , (j=1, …,m) et Y sont des variables linguistiques définies respectivement sur les univers $U = U_1 \text{x} \ldots \text{x} U_m$ et V. Les ensembles flous A_{ij} sont des éléments de la partition linguistique T_j de U_j (univers de la variable X_j).

Pour un vecteur ordinaire d'entrée $u^0 = (u_1^0, \ldots, u_m^0)$, la valeur de la sortie est déterminée suivant les trois étapes suivantes :

- *Fuzzification*

La fuzzification est l'opération qui consiste à convertir une donnée d'entrée ordinaire u_j^0 en sa représentation symbolique, c'est-à-dire l'ensemble flou A_{ij}^* utilisant la partition floue T_j de U_j, par calcul du degré d'appartenance $\mu_{Aij}(u_j^0)$ de u_j^0 pour chaque A_{ij}. Ensuite le degré $\alpha_i = \min \mu_{Aij}(u_j^0)$ est calculé pour chaque règle R_i.

- *Inférence floue*

Le moteur d'inférence transforme les ensembles flous d'entrée (issus de l'opération de fuzzification) en des ensembles flous de sortie en utilisant la base de règles linguistiques et les opérations d'implication floue.

La sortie floue est obtenue par la méthode d'inférence max-min selon les sous-étapes suivantes :

(i) Repérage du niveau d'activation de chaque règle : La valeur de vérité attribuée à l'"antécédent" (prémisse) de chaque règle R_i est calculée puis appliquée à la partie "conclusion" de cette règle. Le calcul se fait comme suit :

$$\alpha_i = \min_j \mu_{A_{ij}}\left(u_j^0\right) \tag{2.20}$$

(ii) Inférencement : Dans l'étape d'inférence, la sortie B_i de chaque règle R_i est calculée à l'aide de l'opérateur de conjonction (min) (voir équation II.24), d'où $B_I' = \alpha_i \wedge B_i$ est donné par :

$$u_{B_i'}(v) = \min\left(\alpha_i, \mu_{B_i}(v)\right) \tag{2.21}$$

(iii) Agrégation : Pour obtenir la sortie globale du système, les sorties propres à chaque règle sont combinées à l'aide de l'opérateur union. Ainsi, $B' = \bigcup_i B_i' = \bigcup \alpha_i \wedge B_i$, avec la fonction d'appartenance :

$$u_{B'}(v) = \max_{i=1,\ldots,n} \mu_{B_I'}(v) \tag{2.22}$$

- *Défuzzification*

L'étape de défuzzification permet de transformer la sortie floue en une valeur numérique v^o représentative de Y dans B'. Différents algorithmes de défuzzification ont été développés et il n'y a pas un algorithme meilleur pour toutes les applications, cependant, la méthode de « la moyenne des maximums » et la méthode du « centre de gravité » sont le plus fréquemment utilisées. Selon cette dernière, la valeur représentative est donnée par :

$$v^0 = \frac{\int_{v \in V} \mu_{B'}(v) \cdot v \cdot dv}{\int_{v \in V} \mu_{B'}(v) \cdot dv}. \tag{2.23}$$

2.4 Graphe de risque flou proposé

Comme mentionné précédemment, malgré que la méthode graphe de risque est facile à mettre en œuvre, elle présente des difficultés d'interprétation des paramètres du graphe. En effet, l'utilisation des termes linguistiques tels que « rare », « possible » peut conduire à des interprétations qui défèrent d'un évaluateur à un autre. Ceci peut conduire à des décisions subjectives.

Pour remédier à ce problème plusieurs alternatives ont été proposés telles qu'elle proposé par Ormos et Ajtonyi [ORM 04] concerne l'utilisation d'un système à base de règles floues pour déterminer la valeur de SIL. De la même façon, Simon et al [SIM 07] proposent une approche à base de règles floues du graphe de risque aussi bien qu'une évaluation subjective des paramètres du graphe par agrégation de jugements d'experts. .

Dans notre travail, nous avons tenté d'améliorer le graphe de risque conventionnel en le décrivant par un système d'inférence flou.

2.4.1 Structure du graphe de risque flou

Le modèle flou développé est un graphe de risque flou qui sera exploité dans le cadre d'une approche d'analyse des risques à base de scénarios (Scenario-based risk analysis approach).

La structure globale du modèle du graphe de risqué flou proposé est illustré dans la figure 2.8

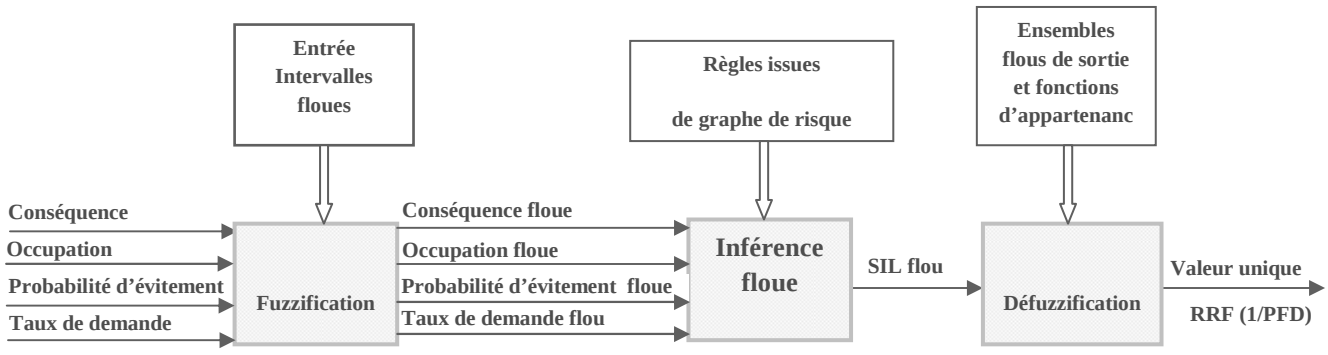


Figure 2.8 Procédure globale d'évaluation de SIL à base de règles floues

La mise en oeuvre de la GRF fait apparaître trois grands modules:

- Le premier module traite les entrées du système (valeurs de *C, F, P* et de *W*). On définit tout d'abord un univers de discours, un partitionnement de cet univers en classes pour

chaque entrée, et des fonctions d'appartenance pour chacune de ces entrées. La première étape, appelée fuzzification, consiste à attribuer à la valeur réelle (donnée du scénario) de chaque entrée sa fonction d'appartenance à chacune des classes préalablement définies, donc à transformer l'entrée réelle en un ensemble flou.

- Le deuxième module est constitué d'une base de règles et d'un moteur d'inférence permettant le calcul; il consiste en l'application de règles.
- Le troisième module décrit l'étape de défuzzification qui permet de passer d'un degré d'appartenance de SIL du scénario à la détermination de la valeur précise à donner à cet SIL.

Nous reviendrons plus en détail, dans les sections qui suivent, sur les étapes de la démarche proposée.

2.4.2 Variables d'entrée et de sortie

Comme pour le graphe de risque conventionnel [CEI 61511], la base de règles floues prend en considération les quatre paramètres *C, F, P* et *W* comme des variables d'entée, et le facteur de reduction de risque (RRF) comme variable unique de sortie.

Les paramètres *C, F, P* et de *W* permettent d'obtenir une graduation signifiante du graphe et constituent les facteurs-clés de l'évaluation du SIL. Leurs niveaux sont définis, à partir de l'analyse du système et de jugements d'experts, par des catégories dont le nombre répond à la fois, à la capacité des individus à pouvoir distinguer ces catégories (problème de perception), et à la capacité des échelles à couvrir une large gamme de risque (problème de résolution) [NAI 09].

La sortie du modèle est un facteur de réduction de risque flou dont la défuzzification permet d'obtenir une valeur unique qui représentera son niveau de SIL.

Le nombre de valeurs attribuées à chacune des variables d'entrée et de sortie correspond à l'univers de discours de cette variable.

2.4.3 Partition floue des variables d'entrée et de sortie

En se basant sur le concept de variable linguistique [ZAD 75], permettant de caractériser les situations considérées comme complexes ou mal définies par rapport à l'application des techniques quantitatives conventionnelles, l'amplitude des variables *C, F, P , W et SIL* dites *variables linguistiques,* est représentée sur des échelles continues moyennant

des fonctions d'appartenance μ à valeurs dans [0,1]. Les ensembles flous utilisés, avec leurs frontières définies de manière non exclusive, représentent les valeurs des variables linguistiques et peuvent être vus comme résumant diverses sous-classes dans l'univers de discours.

2.4 .4 Développement des échelles floues

Dans notre travail, il était question de passer des échelles d'intervalles ordinaires vers des échelles floues. Pour se faire, nous nous sommes référés à un travail récent [NAI 09] lequel propose les équations (2.24) et (2.25) qui ont pu être déduites en considérant la transformation d'un intervalle ordinaire (des bornes E_* et E^*) en un intervalle flou « Q » comme étant le problème inverse de la détermination de la valeur moyenne d'un intervalle flou.

$$E(Q) = [E_*(Q), E^*(Q)], \tag{2.24}$$

Où

$$\begin{aligned} E_*(Q) &= \inf E(Q) = \int_{-\infty}^{+\infty} u dF^*(u), \\ E^*(Q) &= \sup E(Q) = \int_{-\infty}^{+\infty} u dF_*(u). \end{aligned} \tag{2.25}$$

F_* et F^* étant respectivement, les fonctions de distribution inférieure et supérieure de P qui appartient à l'ensemble des mesures de probabilité $P(Q)$ définies sur le support de Q.

A partir des expressions (2.24) et (2.25), on a pu démontrer les équations suivantes :

$$E_*(Q) = q_- - \frac{\alpha}{2}, \tag{2.26}$$

$$E^*(Q) = q_+ + \frac{\beta}{2}. \tag{2.27}$$

Sachant que α et β sont, respectivement, l'étalement gauche et l'étalement droit

Ces résultats sont en cohérence avec le fait que la valeur moyenne est une fonction linéaire de α et β [DUB 87]. Ces étalements seront déterminés en utilisant respectivement (2.26) et (2.27).

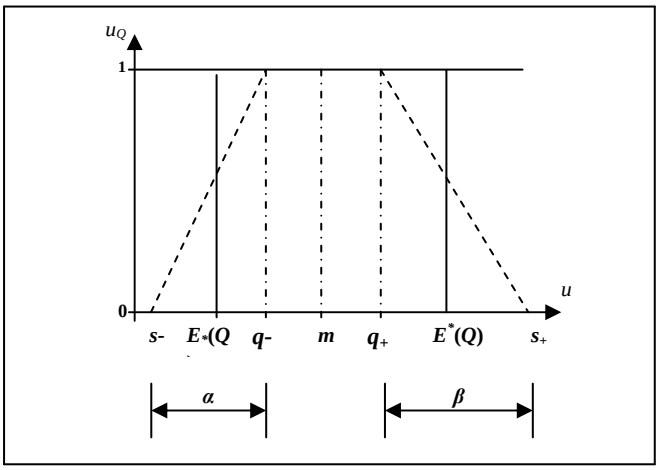


Figure 2.9 Transformation d'un intervalle ordinaire en un intervalle flou

Comme pour les valeurs moyennes, E_* et E^* sont données par les bornes des intervalles ordinaires ; α et β sont calculés selon la méthode suivante : Premièrement, on calcule la valeur moyenne, m, de l'intervalle $[E_*,E^*]$ puis les bornes q_- et q_+ du noyau en utilisant respectivement, la valeur moyenne des subdivisions $[E_*,m]$ et $[m,E^*]$. Selon que l'univers de l'échelle soit, ou non, linéaire, la moyenne arithmétique, comme la moyenne géométrique, sont utilisées à la fois pour obtenir m, q_- et q_+.

La figure 2.9 illustre la transformation d'un intervalle ordinaire en un intervalle flou sur une échelle linéaire. A titre d'exemple, l'étalement α et la borne inférieure s- de Q sont déterminés par :

$$\begin{aligned} \alpha &= 2(q_- - E_*) = 2\left(\frac{E_* + m}{2} - E_*\right) \\ &= m - E_* = \frac{E_* + E^*}{2} - E_* \\ &= \frac{E^* - E_*}{2}, \\ s_- &= q_- - \alpha. \end{aligned} \qquad \textbf{(2.28)}$$

Les ensembles flous extrêmes contenus dans la partition linguistique sont générés de la transformation tout en supposant des étalements infinis, c'est-à-dire en prenant α=-∞, μ_{Qeg} (u)=1 pour $u \leq q_-$ et β=+∞, μ_{Qed} (u)=1 pour $u \geq q_+$ (*eg* et *ed* dénotent respectivement, l'extrême gauche et l'extrême droite).

En outre, transformer une partition ordinaire (discrète) irrégulière en une partition floue, peut entraîner des valeurs non significatives des termes linguistiques (problème de

compatibilité). Dans ce cas, la pente de ces ensembles flous nécessite d'être raisonnablement modifiée.

2.4.5 Construction de la base de règles floues

2.4 .5.1 Intérêt des règles floues dans l'analyse de SIL

La combinaison des valeurs des variables d'entrée *C, F, P* et de *W* selon les objectifs de sécurité donne lieu à une base de règles décrivant de manière flexible les différent niveaux de SIL (1-4) du risque. La base de règles permet de décrire SIL pour chaque combinaison des variables d'entrée. Ces règles sont le plus convenablement exprimées par des termes linguistiques plutôt que numériques, et souvent formulées sous le modèle Si/Alors qui est facilement utilisée pour les déclarations conditionnelles floues; où « Si » se réfère aux variables d'entrée et « Alors » à la variable de sortie, composant ainsi, la prémisse et la conclusion de la règle.

L'importance des règles Si/Alors réside dans le fait que la connaissance et l'expérience humaine peuvent, souvent, être représentées par ce type de règles [SHA 05]. Etant donné que les règles floues sont linguistiques plutôt que numérique, associant les paramètres du graphe de risque (dans la prémisse) avec la valeur du SIL (dans la conclusion), elles fournissent une structure naturelle pour exprimer ce type de connaissances. Ainsi, les experts trouvent souvent, les règles floues comme la manière la plus convenable pour exprimer leurs connaissances sur une situation donnée.

2.4.5.2 Dérivation des règles

Il existe plusieurs techniques pouvant être utilisées pour générer les règles floues. Citons à titre d'exemple [BOW 95] :

- la connaissance d'expert et l'expertise ; et
- la modélisation floue du processus.

La première approche exploite le fait que les analystes qualifiés possèdent souvent une " bonne connaissance intuitive" sur le comportement du système et les risques entraînés, sans avoir aucun modèle quantitatif dans l'esprit.

Dans la deuxième approche, les règles floues peuvent être vues comme une "fonction floue" donnant une évaluation floue de SIL pour les diverses combinaisons de conséquence,

occupation, probabilité d'évitement et de taux de demande. Ces relations forment la base de règles. Comparativement à la seule connaissance d'expert, cette approche (bien qu'elle semble être plus compliquée), elle offre parfois une structure plus étendue pour l'évaluation de la criticité.

Ces deux techniques ne sont pas mutuellement exclusives, leur combinaison est souvent la méthode la plus efficace pour construire la base de règles.

La cohérence de la base de règles peut être appréciée au travers l'examen du tracé de la surface du SIL en matière des combinaisons possibles des variables d'entrée. Les incohérences sont révélées par une variation brusque du niveau SIL pour de petites variations dans les paramètres d'entrée.

Dans notre approche, la base de règles est fournie par le graphe de risqué conventionnel à partir de la règle d'association des paramètres C,F,P et W donnant pour résultat, les niveaux de SIL.

Chaque règle se présente sous la forme de

Si C est *B et* F est *A et P est A et W est 3* Alors SIL est *1*,

2.4.5.3 Exploitation de la base de règles floues

On regroupe dans ce bloc, d'existence virtuelle, l'ensemble de définitions utilisées dans le graphe de risque conventionnel : univers de discours, partitions floues, ainsi que les règles Si/Alors du graphe de risque conventionnel.

Fuzzification des données d'entrée

En utilisant le simulateur Toolbox du Matlab, les données d'entrée des différent paramètres du scénario considéré sont fuzzifiées en leur plaçant sur les échelles floues correspondantes pour déterminer les degrés d'appartenance aux ensembles flous impliqués.

Évaluation de la conclusion floue (Inférence floue)

Les règles floues sollicitées par les variables d'entrée du scénario étudié sont activées. Afin de transformer ces règles qualitatives en un résultat quantitatif interprétable, l'algorithme d'inférence floue de Mamdani (modèle max-min) est exploité. L'applicabilité (la valeur de vérité) de la règle est déterminée à partir de la conjonction et l'implication des prémisses de la

règle en utilisant l'opérateur « min ». L'opérateur « max » est utilisé pour l'agrégation des sorties floues résultantes

Défuzzification de la sortie floue

L'évaluation des données d'entrée dans la base de règles donne un résultat imprécis et flou. Le processus de défuzzification crée un classement discret de la conclusion floue pour exprimer le SIL du scénario étudié. La défuzzification est requise pour [BOW 95] :

1) Déchiffrer le sens des conclusions floues et de leurs valeurs d'appartenance;
2) Résoudre les contradictions qui peuvent surgir entre les différents résultats durant l'évaluation.

Le choix de l'algorithme de défuzzification dépend des critères suivants [SHA 05]:

- l'absence d'ambiguïté (résultat sous forme de valeur numérique) ;
- la plausibilité ;
- la facilité du calcul.

Dans le cas de défuzzification pour obtenir un niveau de SIL, la stratégie de défuzzification doit :

- Résulter en un classement continu du niveau de SIL ;
- Combiner toute les règles activées durant l'évaluation, selon la valeur de vérité de la conclusion.

En utilisant la méthode du centre de gravité (la valeur défuzzifiée correspond à l'abscisse du centre de gravité de la surface sous la courbe résultante de l'agrégation des règles. C'est une valeur numérique de SIL, comparable à celle donnée par le graphe conventionnel.

2.5 Détermination du SIL par graphe de risque flou

Le modèle de graphe de risque que nous allons utiliser pour déterminer le niveau de SIL des fonctions instrumentés en vue de maitriser les scenarios d'accident représenté par la figure 3.3

La figure 3.3 et tableau 3.2 montrent respectivement un exemple d'un graphe de risque tel qu'elle est utilisée dans les lignes directrices d'UKOOA et les définitions quantitatives des paramètres du graphe [SMI 04], [DEA 99], [GUL 04]

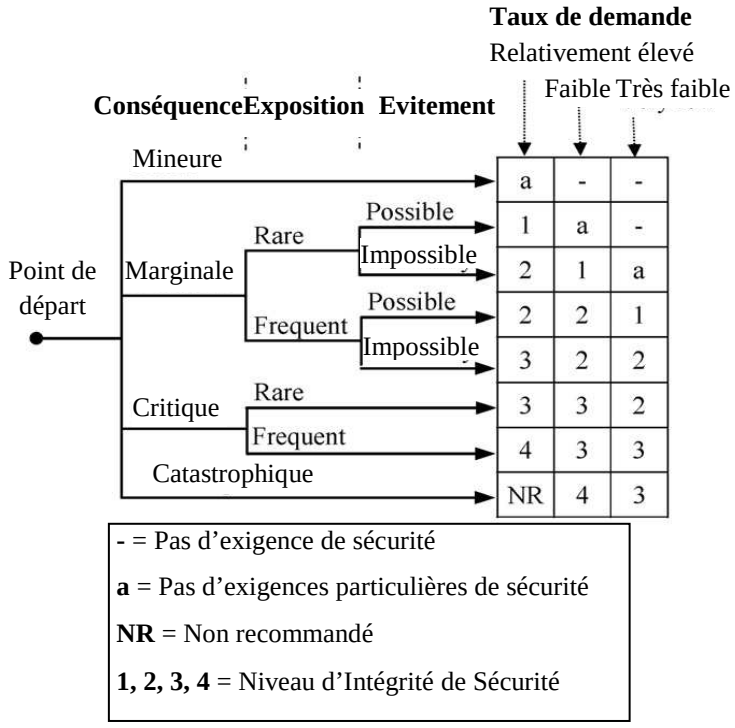


Figure 2.10 Graphe de risque avec description qualitative des paramètres

Les échelles des paramètres C,F,P,W et de SIL auxquelles nous nous référons dans la suite, se présentent de la manière suivante :

Paramètre	**Description qualitative**	**Description quantitative**
Conséquence (C)	Mineur	Pas de mort
	Marginal	$[10^{-2},10^{-1}]$
	Critique	$[10^{-1},1]$
	Catastrophique	> 1
Occupation (F)	Rare	< 10% de temps
	Fréquent	≥10% de temps
Probabilité d'évitement (P)	Possible	90% probabilité d'évitement de danger
	Impossible	≤90% probabilité d'évitement de danger
Taux de demande (W)	Très faible	<1 dans 30 ans≈<0.03/an
	Faible	1 dans [3,30] ans≈ [0.03, 0.3] par an
	Elevé	1 dans [0.3,3] ans≈[0.3,3] par an

Tableau 2.1 Description qualitative et quantitative des paramètres du graphe de risque

2.5.1 Établissement des échelles floues

2.5.1.1 Conséquence : quatre ensembles flous, à savoir Mineur, Marginale, Critique et Catastrophique ont été définis sur l'espace d'entrée de cet variable. Les valeurs variant de 10^{-9} à 10 sont représentés sur un échelle logarithmique. A la valeur linguistique mineure définis dans le graphe de risque comme pas de mort est attribué l'intervalle discret $[10^{-9},10^{-7}]$ qui représente convenablement un événement improbable. Cet intervalle est transformé en un intervalle flou avec l'omission de partie négative.

2.5.1.2 0ccupation : deux ensembles flous à savoir Rare et Fréquente ont été définis sur une échelle linéaire allant de 0% à 100%. Comme le précédent paramètre la partie négative du premier u limite inférieur ensemble Rare est retirée et la borne supérieure de son noyau a servi lde imite du second ensemble Fréquent. La fonction d'appartenance de ce dernier est évidemment ouverte

2.5.1.3 Probabilité d'évitement : comme dans le paramètre d'entrée précédemment, deux ensembles flous nommés respectivement «Impossible » et « Possible » ont été définis sur l'univers [0,100], Pour le premier ensemble la partie négative est enlevée et la limite supérieure de son support prend la valeur limite inférieure du noyau de l'ensemble « Possible ». Les valeurs de ces derniers sont limitées à 100 avec une fonction d'appartenance ouverte à droite.

2.5.1.4 Taux de demande : trois ensembles flous, à savoir « Très faible », « Faible » et « Relativement élevé » ont été définis sur un espace de probabilité allant de 10^{-5} à 1. Les valeurs de taux de demande sont présentées sur un échelle logarithmique

En se référant aux données du tableau 2. l'échelle des différent paramètres sont transformés en ses représentation floue, dérivée de l'intervalle $Q = [s_-,[q_-, q_+],s_+]$, selon la méthode décrite dans§ 2.4.4

Le tableau 2.2 montre les résultats numériques de la transformation pour le paramètre conséquence

Symboles	E_*	E^*	M	q_-	$q+$	S_-	S_-^*	S_+	S_+^*
Conséquence									
Mineur	1,00E-09	1,00E-07	1,00E-08	3,16E-09	3,16E-08	-1,16E-09	1,00E-09	1,68E-07	/
Marginal	0,01	0,1	3,16E-02	1,78E-02	5,62E-02	2,22E-03	/	1,44E-01	/
Critique	0,1	1	3,16E-01	1,78E-01	5,62E-01	2,22E-02	/	1,44E+00	/
Catastrophique	1	10	3,16E+00	1,78E+00	5,62E+00	2,22E-01	/	1,44E+01	1,00E+01

Tableau 2.2 Résultats numériques de la partition floue des intervalles du paramètre conséquence

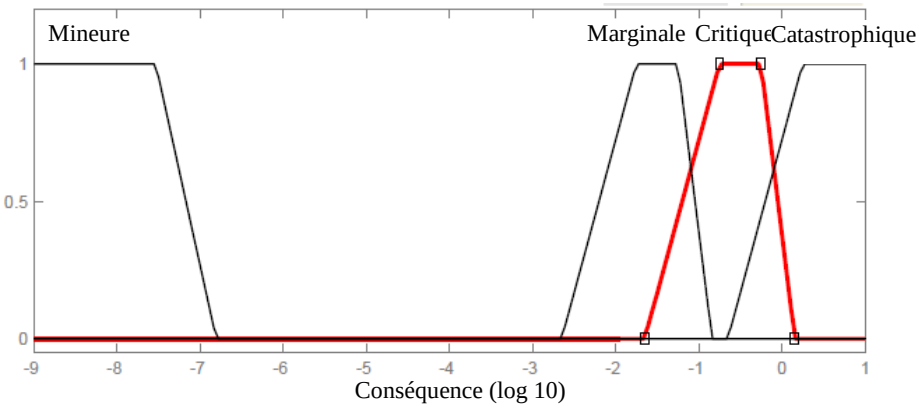


Figure 2.11 Fonction d'appartenance générée pour la conséquence

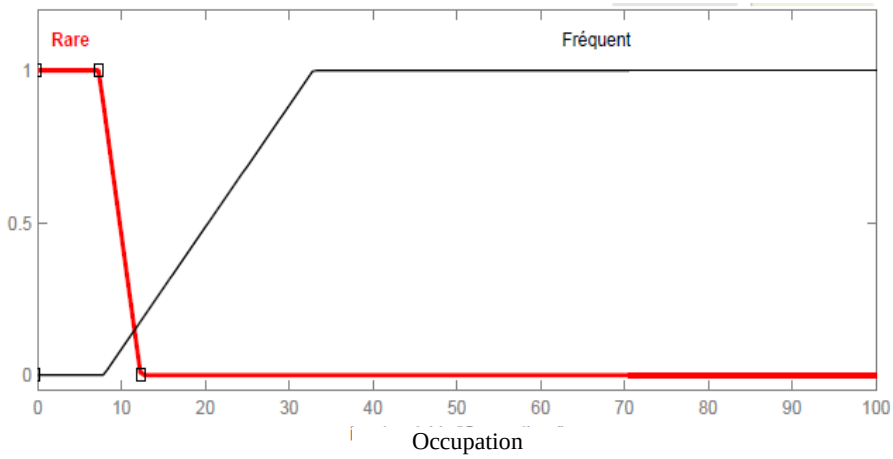


Figure 2.12 Fonction d'appartenance générée pour l'occupation

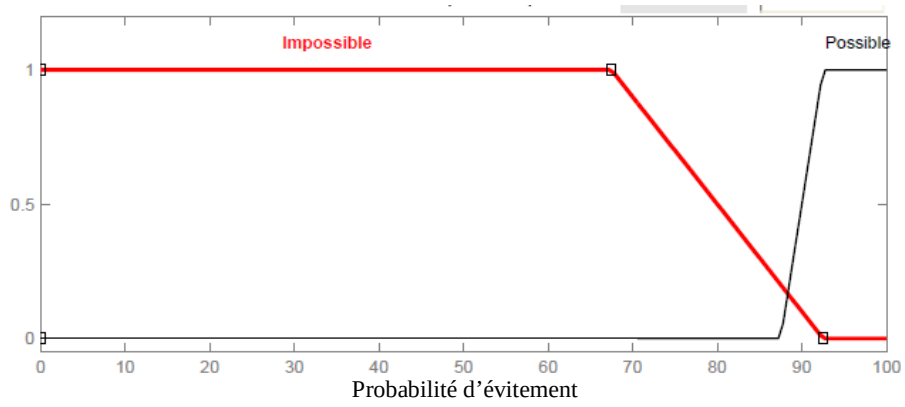


Figure 2.13 Fonction d'appartenance générée pour la probabilité d'évitement

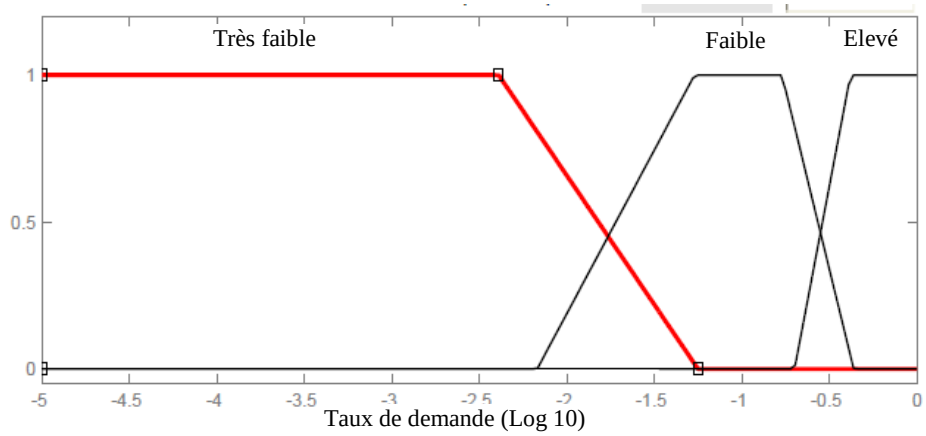


Figure 2.14 Fonction d'appartenance générée pour le taux de demande

Échelle de SIL

Le SIL du comme variable unique de sortie est définie sur un échelle de RRF .L' univers de discours de valeurs entre 1 et 10^{-6} et représentée sur une échelle logarithmique avec une partition régulière. Six ensembles flous sont compris dans l'échelle : *NSSR, SIL1, SIL2, SIL3, SIL4* et *NR*

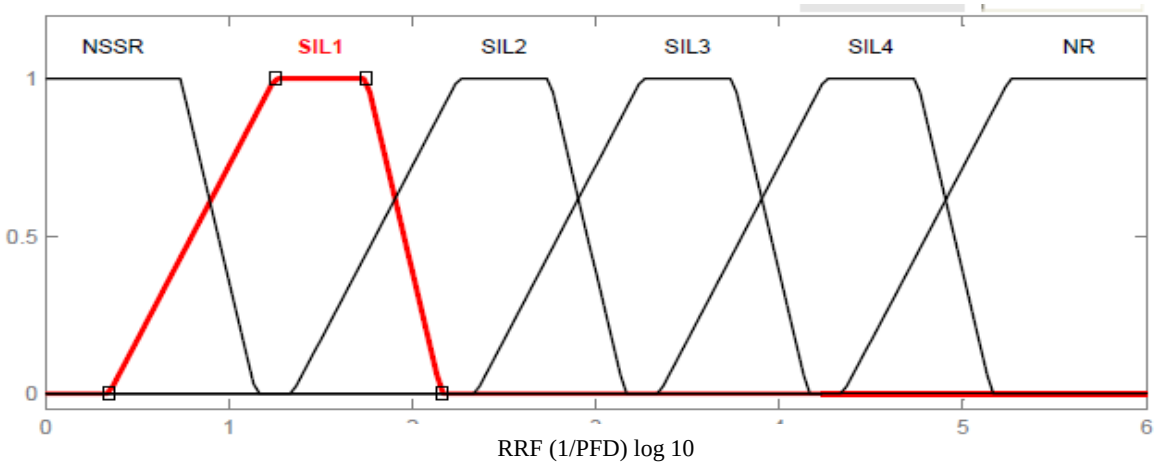


Figure 2.15 Fonction d'appartenance générée pour SIL

2.5.2 Établissement des règles floues

Un certain nombre de règles floues Si-Alors sont extraites en suivant la logique du graphe de risque et en utilisant les descripteurs linguistiques associés aux paramètres de risque et au SIL. Dans ce cas, la base de règle peut être comprise comme une traduction du graphe de risque.

Règle	Conséquence	Occupation	Probabilité d'évitement	Taux de demande	SIL
1	Mineur	Néant	Néant	Elevée	a
2	Mineur	Néant	Néant	Faible	/
3	Mineur	Néant	Néant	Très faible	/
4	Marginale	Rare	Possible	Elevée	1
5	Marginale	Rare	Possible	Faible	a
6	Marginale	Rare	Possible	Très faible	/
7	Marginale	Rare	Impossible	Elevée	2
8	Marginale	Rare	Impossible	Faible	1
9	Marginale	Rare	Impossible	Très faible	a
10	Marginale	Fréquent	Possible	Elevée	2
11	Marginale	Fréquent	Possible	Faible	2
12	Marginale	Fréquent	Possible	Très faible	1
13	Marginale	Fréquent	Impossible	Elevée	3
14	Marginale	Fréquent	Impossible	Faible	2

15	Marginale	Fréquent	Impossible	Très faible	2
16	Critique	Rare	Néant	Elevée	3
17	Critique	Rare	Néant	Faible	3
18	Critique	Rare	Néant	Très faible	2
19	Critique	Fréquent	Néant	Elevée	4
20	Critique	Fréquent	Néant	Faible	3
21	Critique	Fréquent	Néant	Très faible	3
22	Catastrophique	Néant	Néant	Elevée	NR
23	Catastrophique	Néant	Néant	Faible	4
24	Catastrophique	Néant	Néant	Très faible	3

Tableau 2.3 Règles de combinaison des paramètres du risque

Le tableau précédent représente l'ensemble des règles de combinaison des paramètres *C,F,P et W* déduites de graphe de risque. La règle 4, par exemple, doit être lue comme suit :

Si la Conséquence est *marginale* et l'occupation est *rare et la probabilité d'évitement est possible et le taux de demande est élevée* alors le SIL est *1*.

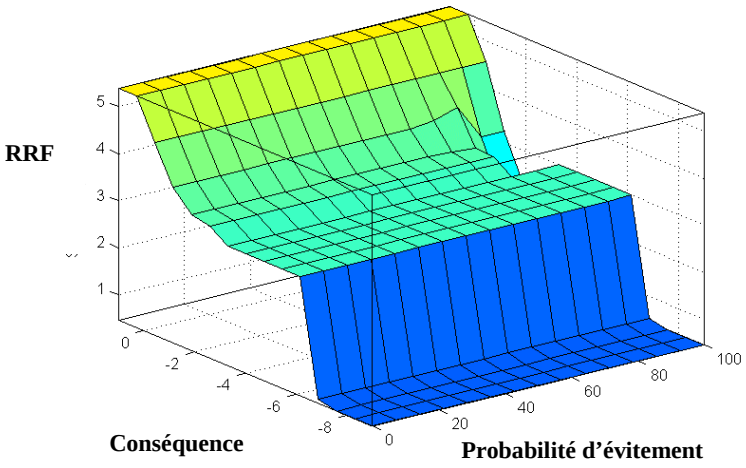


Figure 2.16 Surface floue de SIL

2.6 Conclusion

Dans ce chapitre, nous avons proposé une approche floue d'évaluation de SIL par graphe de risque, en l'occurrence, le graphe de risque flou que nous estimons prometteuse et capable de représenter et traiter, avec souplesse, la connaissance relative à graphe de risque conventionnel.

Afin de tester l'approche proposée, nous consacrerons le prochain chapitre à une étude expérimentale portant sur un procédé industriel pour pouvoir affirmer qu'elle peut constituer une alternative aux pratiques classiques d'évaluation de SIL des fonctions instrumentées.

3

Application à un four rebouilleur

3.1 Introduction

Dans l'industrie pétrolière, le process présente des risques majeurs et nécessitent des moyens de sécurité sophistiqués pour la maitrise de ces risques. Parmi ces moyens BPCS, SIS. Cependant, avant l'implémentation de ces systèmes la détermination de leurs niveaux de SIL est exigée. Dans ce contexte, l'utilisation du graphe de risque conventionnel présente des inconvénients concernant la qualité des échelles des paramètres du graphe. En plus, les données nécessaires à l'évaluation du SIL en fonction des C, F, P et W sont entachées d'imprécision et d'incertitude. Ce qui conduit à l'affectation de la qualité de l'évaluation en donnant des résultats imprécis sur le niveau de SIL requis, ce qui peut ramener l'entreprise à décider des mesures de sécurité non appropriées à la gestion du risque résiduel.

L'objet de ce chapitre est l'application, dans un premier temps du graphe de risque conventionnel sur un système opérationnel, à savoir Four H321 de l'association Sonatrach/BP/Statoil. Le modèle graphe de risque flou proposé sera également appliqué au même système dans le but de comparer les résultats des deux applications et montrer l'intérêt de l'approche floue dans la réduction de l'incertitude.

3.2 Présentation du processus

L'installation prise en référence pour la présente étude étant un four rebouilleur du CPF (Cental Process Facilities) au sein de la raffinerie d'hydrocarbures Sonatrach/BP/Statoil du site industriel In Amenas.

Dans une unité pétrolière, le rôle du four est d'apporter la chaleur nécessaire au réchauffement des fluides en les portant à des niveaux de température élevée. Le four rebouilleur H-101 est destiné au réchauffement du l'huile pour alimenter les échangeurs de chaleur situés dans les trois trains de l'unité de traitement de gaz.

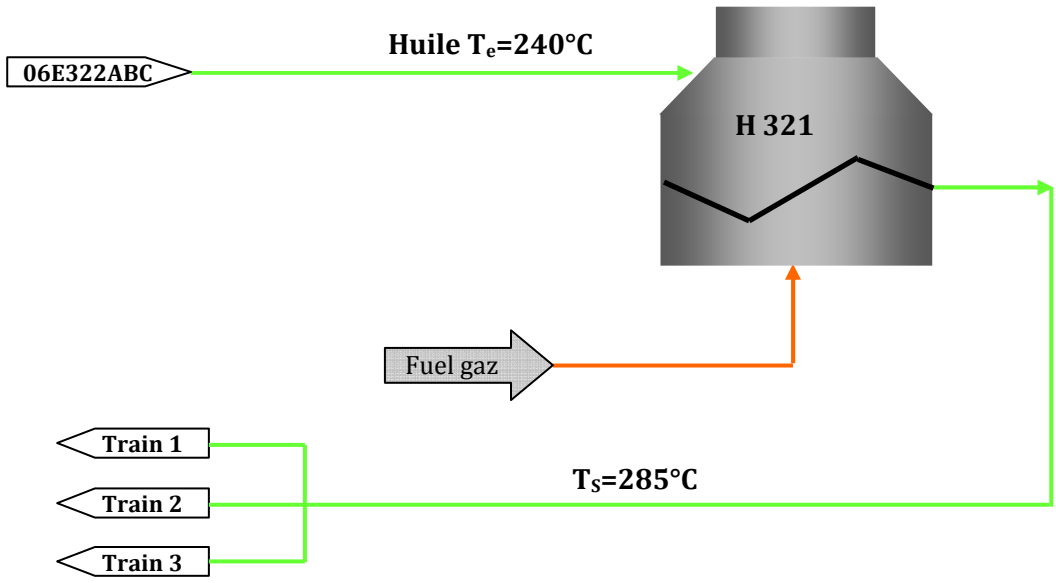


Figure 3.1 Schéma du circuit d'huile chaude

Dans le CPF, l'huile des échangeurs 06E322ABC passe à travers les pompes, dans le four à 240°C. Le fluide sortant porter à 285°C est renvoyé vers les échangeurs 06E322ABC comme reflux chaud pour un échange thermique entre ce fluide (l'huile) et le condensat passant dans la partie tubulaire des échangeurs. (Voir figure 3.1).

Le four H321 est de type cylindrique vertical composé de deux zones :

- D'une zone de radiation (chambre de combustion) intérieurement garnie par un matériau réfractaire isolant. Dans cette chambre se trouvent des tubes exposés à la flamme et recevant par rayonnement la chaleur dégagée des produits en combustion ;

- D'une zone de convection (éventuellement garnie) installée à la sortie des fumées de la chambre de combustion et constituée d'un faisceau tubulaire placé perpendiculairement à la direction des fumées ;
- Une cheminée: d'évacuation des fumées.
- D'accessoires: Portes d'accès, brûleurs, pilotes, thermocouples et diverses connexions nécessaires au fonctionnement du four.

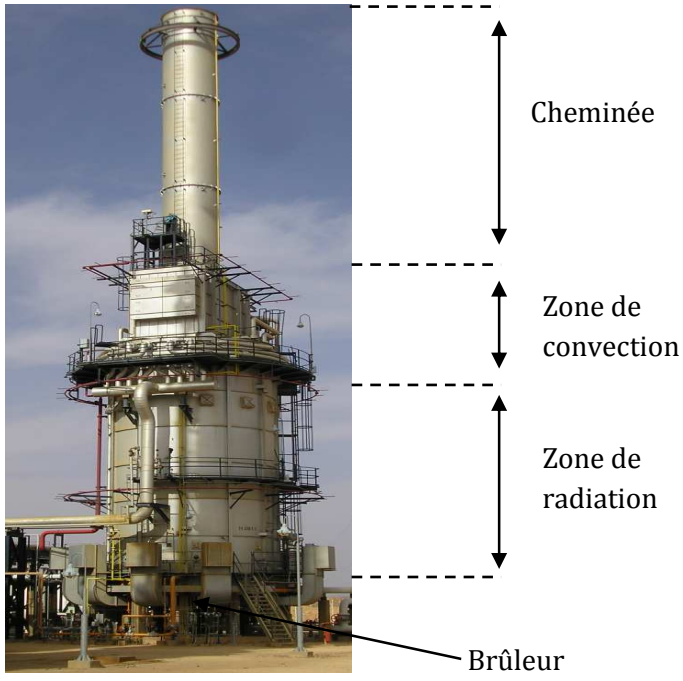


Fig. 3.2 Architecture du four rebouilleur H321

3.3 Analyse structurelle et fonctionnelle du système four rebouilleur

Pour une meilleure description du système étudié une analyse structurelle et fonctionnelle s'avère indispensable. Le but de cette analyse est de décomposer le système et identifier les différentes fonctions de chaque partie de ce système.

Les résultats de cette analyse sont indiqués dans le tableau 3.1 suivant :

Sous-systèmes	Équipements	Composants
SS1 : circuit d'alimentation [Alimentation du four rebouilleur]	**E11 :** circuit comburant (Fuel Gaz) [Assure l'alimentation en combustible]	**C111 :** Vanne FV 3202 [régulation de pression de fuel gaz en fonction de la température de liquide]
		C112 : Les pilotes [Garantir une flamme continue pour l'amorçage du fuel gaz]
		C113 : Les brûleurs [Réaliser la combustion de fuel gaz]
	E12 : circuit Liquide (l'huile) [Assure l'alimentation en huile des échangeurs]	**C121 :** Pompes P301 A/B/C [pomper l'huile à l'entrée du four]
		C122 : Vanne FV 3200 [régulation de débit de liquide]
		C123 : Serpentin [Assure la circulation et l'échauffement du liquide]

Tableau 3.1 Décomposition du four H321

Sous-systèmes	Équipements	Composants
SS2 : de contrôle [contrôle des paramètres du procédé]	**E21 :** contrôle de débit [Contrôle le débit du liquide à l'entrée du four]	**C211 :** DCS (SOLVER) [Adaptation du débit de liquide à l'entrée de four par action sur la vanne FV 3200]
		C212 : Débitmètre FT 3200 [Mesure le débit du liquide à l'entrée de four]
	E22 : contrôle de température [Contrôle la température du liquide à l'intérieur et à la sortie du four]	**C221 :** DCS (SOLVER) [Adaptation de température de liquide à la sortie de four par action sur la vanne TV 3213]
		C222 : Thermocouple TI 3213 [Mesure la température du liquide à la sortie du four]
		C223 : Indicateurs de température locale TI [Indique la température]

Tableau 3.1 Décomposition du four H321 (suite)

Sous-système	Equipement	Composant
SS3 : d'alarmes [Faire alerter l'opérateur par un signal audio-visuel]	**E31 :** TAH/ FAL/ PAL/PAH [alarme de haute température du l'huile à chauffé] [alarme de bas débit du l'huile à l'entrée du four] [alarme de basse/ haute pression de fuel gaz]	**C311 :** Thermocouple TI/ Débitmètre FT/ Transmetteur de pression PT [Mesure la température du liquide à la sortie du four/ Mesure le débit du liquide à l'entrée de four/ mesure la pression de fuel gaz]
		C312 : DCS [Adaptation de la mesure de température, débit et pression à une alarme audio-visuelle]
SS4 : d'arrêt d'urgence [Mettre le four a l'état d'arrêt]	**E41 :** TAHH/ FALL/ PALL/PAHH [alarme de très haute température du l'huile à chauffé] [alarme de très bas débit du l'huile à l'entrée du four] [alarme de très basse et haute pression de fuel gaz]	**C411 :** Thermocouple TI/ Débitmètre FT/ Transmetteur de pression PT
		C412 :SDV3210/ SDV 3211 [Isolement de la ligne de gaz combustible]
		C413 : PLC [[Assurer les missions de mise en sécurité du four par action sur les vannes SDV 3210/ 3211]

Tableau 3.1 Décomposition du four H321 (suite)

3.4 Identification des scénarios d'accidents

L'identification des scénarios d'accidents pouvant se produire dans le four rebouilleur H 321 est faite moyennant la méthode HAZOP, l'utilisation de la méthode HAZOP permet d'identifier les causes, les conséquences et les barrières de mesures de sécurité mises en œuvre dans le système pour faire face au développement de ces scénarios.

Le tableau 3.2 de HAZOP montre ces différentes causes et conséquences et barrières de sécurités existantes au niveau du four rebouilleur H-101.

SYSTEME ÉTUDIE : Four Rebouilleur 06-H-321, N° **du dessin (P&ID) :** 537-434-162-BA-0, N° **de RÉVISION :** 0.									
PARTIE CONSIDERÉE : Serpentin du four depuis l'admission d'huile (avant la mesure du débit), jusqu'à la sortie (après contrôle de la température)					**INTENTION DE CONCEPTION :** **Entrées :** Alimentation en huile, chaleur du four				
N°	**Mot-guide**	**Élément**	**Déviation**	**Causes possibles**	**Conséquences**	**Protections**	**Commentaires**	**Mesures à prendre**	**Responsable des mesures**
1	NE PAS FAIRE/ MOINS	Débit d'huile	Pas/ Moins de débit	La vanne FV 3200 fermée	Pas du liquide dans H-321, endommagement de serpentin (incendie) & arrêt d'unité (possible arrêt module)	- Opérateurs - FAL : alarme - Arrêt d'urgence de H-321			
				Mauvaise manipulation sur l'une des vannes manuelles à l'entrée de H-321 (fermée)	Pas de débit dans l'un des pass du H-321, température élevée, endommagement de serpentin (incendie) & arrêt d'unité (possible arrêt module)	- FAL alarme -Arrêt d'urgence de H-321 - Opérateurs			

Tableau 3.2 Feuille de présentation HAZOP

SYSTEME ÉTUDIE : Four Rebouilleur 06-H-321									
N°	**Mot-guide**	**Élément**	**Déviation**	**Causes possibles**	**Conséquences**	**Protections**	**Commentaires**	**Mesures à prendre**	**Responsable des mesures**
1	NE PAS FAIRE/ MOINS	Débit de gaz combustible	Pas/ Moins de débit	La vanne PCV 3211 fermée	Pas de fuel gaz pour H-321, basse température à la sortie de H-321, passage possible de produit en OFF-SPEC	- PAL : alarme - Arrêt d'urgence de H-321			
				La vanne FV 3200 fermée	Pas de fuel gaz pour H-321, basse température à la sortie de H-321, passage possible de produit en OFF-SPEC	- PAL : alarme - Arrêt d'urgence de H-321 -			

Tableau 3.2 Feuille de présentation HAZOP (suite)

SYSTEME ÉTUDIE : Four Rebouilleur 06-H-321									
N°	**Mot-guide**	**Élément**	**Déviation**	**Causes possibles**	**Conséquences**	**Protections**	**Commentaires**	**Mesures à prendre**	**Responsable des mesures**
5	PLUS	Débit de gaz combustible	Plus de débit	La vanne PCV 3211 ouverte	Haut débit de fuel gaz pour H-321, haute pression de fuel gaz pour les bruleurs, haute température à la sortie de H-101(explosion) & arrêt d'unité (possible arrêt module)	- PAH : alarme - Arrêt d'urgence de H-321			
				La vanne FV 3200 ouverte	Haut débit de fuel gaz pour H-321, haute pression de fuel gaz pour les bruleurs, haute température à la sortie de H-101(explosion) & arrêt d'unité (possible arrêt module)	- PAH : alarme - Arrêt d'urgence de H-321			

Tableau 3.2 Feuille de présentation HAZOP (suite)

3.5 Détermination du SIL des scénarios

3.5.1 Détermination des paramètres C,P,F et W

3.5.1.1 Conséquence

Le choix des conséquences à étudier est fonction de la méthodologie d'évaluation des risques adoptée par l'entreprise et des ressources qu'elle doit mettre en place pour affiner l'analyse [. Ainsi, les conséquences basées sur plusieurs critères :

- Les personnes : Blessure, Mort ;
- L'environnement : pollution, rejets des matières dangereux
- Perte de production: Dégradation de la capacité de l'installation, arrêt de l'unité ou l'usine).

On s'intéresse dans notre étude aux scénarios donnant comme conséquence une atteinte à l'homme.

Scénario	Conséquence	Description
Haut débit du fuel gaz	Extinction de la flamme et son réapparition peut provoquer une explosion	Critique plusieurs morts
Faible débit d'huile à l'entrée du four	Endommagement du serpentin (Incendie)	Marginale blessures graves ou mort d'une personne

Tableau 3.3 Description des conséquences de scénarios

3.5.1.2 Taux de demande

Le taux de demande est calculé à partir des fréquences des événements initiateurs des scénarios et qui sont identifiés par l'analyse préliminaire HAZOP

Scenario	**Evénement initiateur**	**Fréquence**	**Réf**
Sc1 : Haut débit du fuel gaz (explosion)	-Défaillance de la vanne FV 3202	1/10 an	[ICS 09, JK 04]
	-Défaillance de la vanne PCV 3202	1/10 an	[ICS 09, JK 04]
Sc2 : Faible débit d'huile (Incendie)	-Défaillance de la vanne FV 3200	1/10 an	[ICS 09, JK 04]

Tableau 3.4 Fréquence des événements initiateurs des scénarios

3.5.2 Fuzzification des données de scénarios

Les données d'entrées sur les scénarios en terme de taux de demande ont été déjà obtenues dans la § 3.5.1.1 et § 3.5.1.2 Concernant la conséquence, il est clair que les conséquences correspondantes identifiées sont de l'ordre critique se rapportant à le mort de plusieurs personnes pour le premier scénario et marginale se rapportant à une blessure graves ou mort d'une personne pour le deuxième scénario 2.

Les données relatives à la vitesse d'évitement et la PFD de l'alarme/opérateur doivent être introduites au système d'inférence floue de Mamdani (pour fuzzification) sous forme de valeurs uniques (singletons), pour obtenir la probabilité d'évitement des scénarios étudiés

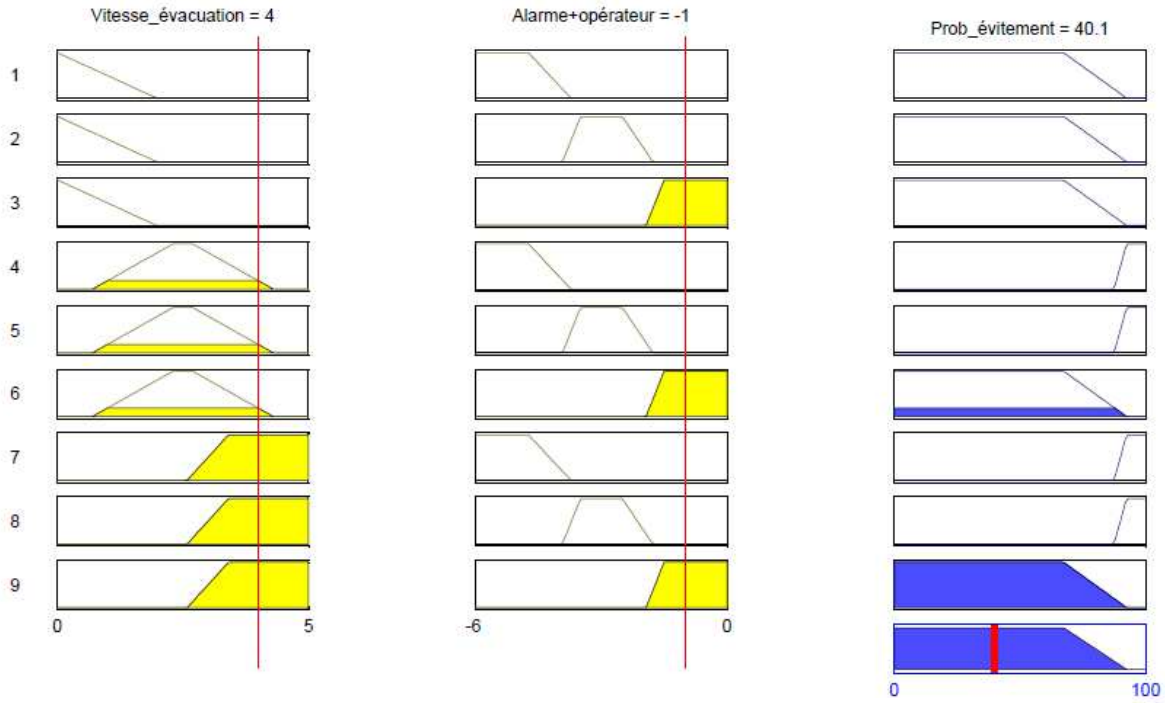


Figure 3.3 Processus d'inférence de la probabilité d'évitement

3.5.3 Résultats obtenues

En utilisant le simulateur du Matlab, l'ensemble d'opérations d'inférence se fait de manière automatique. La figure suivante représente une illustration du processus d'inférence floue pour le scénario 1.

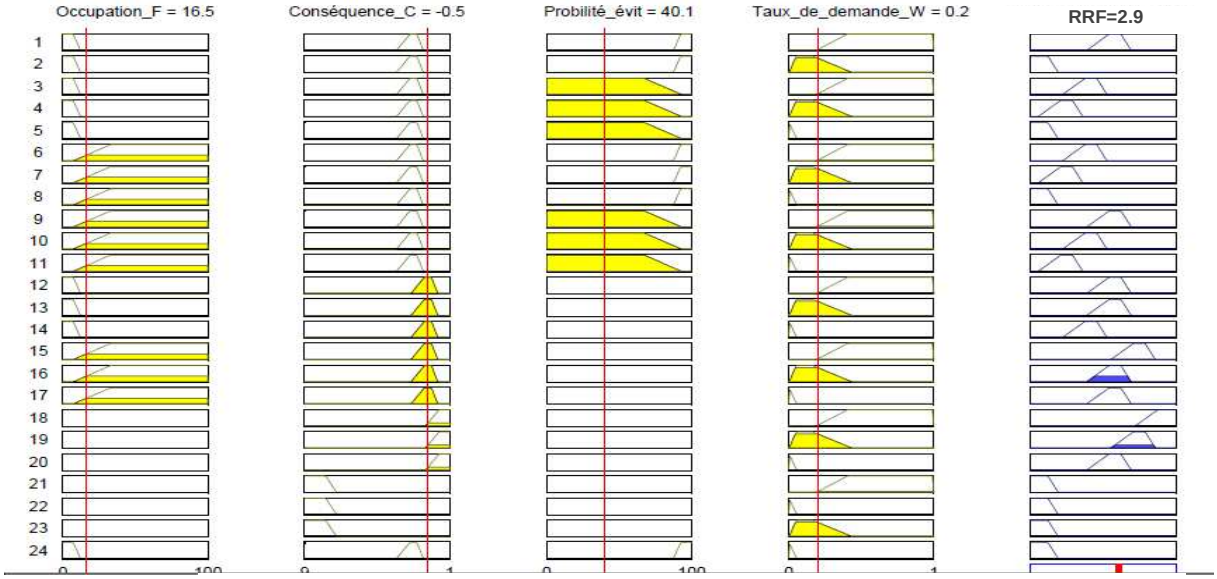


Figure 3.4 Processus d'inférence des règles flous : cas Sc1

Un récapitulatif de résultats de l'évaluation est représenté sur **le tableau 3.**

Scénario	**Entrée**				**Sortie (SIL)**	
	C	F	P	W	Graphe de risque conventionnel	Graphe de risque flou
Haut Débit du fuel gas	[0,1- 1]	[0-25]	41	0,2	SIL 3	SIL2- 0,8/SIL3-0.4
Faible débit de l'huile	[0,01-0,1]	[0-25]	41	0,1	SIL 2	SIL1- 0,7/SIL2-0.5

Tableau 3.5 Comparaison des résultats de l'évaluation du SIL des scénarios.

▪ ***Discussion des résultats***

La comparaison des résultats des deux approches d'évaluation du SIL montre une différence comme montré sur le tableau précédent.

Nous constatons que le SIL déterminé par graphe de risque flou est caractérisé par une appartenance progressive à plus d'un niveau.

Dans le cas du premier scénario, le SIL appartient aux niveaux 2 et 3 avec des degrés d'appartenance respectivement 0 .8 et 0.4. De même, pour le scénario 2, le SIL appartient également à deux niveaux 1 et 2 avec des degrés d'appartenance respectivement 0 .7 et 0.5.

Cette comparaison montre qu'il ya surestimation du SIL dans le cas des deux scénarios malgré que cette surestimation conduit à un résultat conservative menant à la conception d'une intégrité de la sécurité suffisante, elle conduit également à des couts d'installation du SIS et d'entretien plus élevés.

3.6 Conclusion

L'objet de ce chapitre est l'application du modèle graphe de risque floue proposé sur un système opérationnel four rebouilleur H 321 et la comparaison des résultats à ceux obtenus par le graphe de risque conventionnel.

Une application à un système opérationnel a servi de support à la validation du modèle proposé.

Le modèle graphe de risque flou proposé a des avantages suivants

- Il préserve les quatre paramètres utilisés de graphe conventionnel
- Les échelles avec valeurs linguistiques sont utilisées pour évaluer les paramètres de risque et l'étalonnage du modèle peut être fait en faisant varier les valeurs de paramètres du graphe.

Conclusion générale

Bien que les graphes de risque conventionnels sont faciles et simples à mettre en œuvre, ils peuvent conduire à des résultats incohérents qui peut entrainer une surestimation ou sous-estimation du SIL. En effet l'utilisation des paramètres décrits qualitativement peut conduire à des fausses interprétations. D'autre part, l'étalonnage des paramètres du graphe de risque à l'aide des intervalles discrets viole la transition progressive entre les intervalles.

Travail réalisé

Notre travail a la prétention d'avoir abordé le problème de détermination du SIL par la méthode graphe de risque et d'avoir tenté de développer et valider le modèle flou proposé. Les concepts d'ensemble flou, de variable linguistique et de règle floue issus de cette logique nous ont permis de prendre en compte :

- Le problème de représentation des données relatives aux paramètres du graphe (C,F,P et W). En effet, les échelles floues ont la capacité de décrire la continuité des catégories avec une transition progressive de l'une à l'autre ;
- Le problème de caractérisation du SIL : Un indice du SIL pouvant appartenir à plus d'une catégorie avec des degrés d'appartenances différents.

Le modèle du graphe de risque flou proposé est basé sur un système d'inférence à base de règles floues appliqué à l'évaluation du SIL. Le graphe de risque flou constitue un complément du graphe conventionnel qui sert de table de décision pour le premier. Le modèle graphe de risque flou est doté d'une flexibilité qui lui permet de traiter les variables linguistiques et incertaines. Les paramètres d'entrée appliqués au système d'inférence sont soit des données d'expertise, soit le résultat d'un modèle d'analyse des risques tels que l'arbre de défaillances et l'arbre d'événement.

Les résultats de l'étude de SIL inhérents à un système « four rebouilleur » montrent que le modèle flou développé offre la possibilité de préserver l'information figurant sur le graphe conventionnel mais avec l'opportunité de pouvoir manipuler et traiter les données incertaines et imprécises relatives au système, qu'elles soient qualitatives ou quantitatives.

Le modèle flou proposé présente un avantage très clair par rapport à graphe de risque conventionnel, celui de permettre une prise de décision sur la base d'un niveau du SIL précis et par conséquent, de mener à bien une démarche de réduction des risques dans le cadre d'un investissement rationnel.

Bibliographie

[BAU 05] C. Baudrit, Représentation et propagation de connaissances imprécises et incertaines : application à l'évaluation des risques liés aux sites et aux sols pollués , Université de Toulouse III Paul Sabatier, France, 2005.

[BEU 06] Beugin, J. (2006). Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé. PhD thesis, Université de Valenciennes et du Hainaut-Cambrésis, France.

[BEU 07] Beugin, J., Renaux, D., and Cauffriez, L. (2007). A sil quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems. Reliability Engineering and System Safety, 92 :16861700.

[BOU 95] B. Bouchon - Meunier, La logique floue et ses applications - Vie artificielle , Ed. Addison - Wesley France, Paris, 1995.

[BOW 95] J. B. Bowles and C. E. Peláez, « Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis », Reliability Engineering & System Safety, vol. 50, no. 2, pp. 203–213, 1995.

[CHA 02] Charpentier, P. (2002). Artchitecture d'automatisme en sécurité des machines : Etude des conditions de conception liées aux défaillances de mode commun. PhD thesis, Nancy Université, Institut Nationnal Polytechnique de Lorraine, France.

[DEA 99] S.Dean, IEC 61508-Assessing the Hazard and Risk, Sauf consulting Ltd, 1999.

[DEM 67] A. P. Dempster, « Upper and lower probabilities induced by multivalued mapping », Annals of mathematical statistics, no. 39, pp. 325-339

[DES 03] Desroches, A., Leroy, A., and Vallée, F. (2003). La gestion des risques : principes et pratiques, volume 1. Lavoisier, France.

[DUB 88] D. Dubois and H. Prade, « Possibility theory : An approach to computerized processing of uncertainty », Plenum Press, 1988.

[DUB 94] D. Dubois et H. Prade, « La fusion d'informations imprécises », Traitement du Signal, pp. 447–458, 1994.

[EN50126 99] EN50126, Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS), 1999.

[EN50128 01] EN50128, Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems, 2001.

[EN50129 98] EN50129 , Safety related electronic systems for signalling, 1998.

[EXI] Exida. Safety Equipment Reliability Handbook. 2nd Edition.

[FAR 67] Farmer., F. R. ,Siting criteria : a new approach. Atom, chapter 128, page 152166, 1967.

[GUL 04] W.G. Gulland, Methods of determining Safety Integrity level (SIL) requirements-Pros and Con, in : Safety Critical Symposium, 2004, pp. 105-122.

[GUO 06] Guo, H. and Yang, X, A simple reliability block diagram method for safety integrity verification. Reliability Engineering and System Safety, 92 :12671273, 2006.

[ICS 06] Groupe de travail ICSI « Fréquence des événements initiateurs d'accidents et disponibilité des barrières de protection et de prévention », Institut pour une Culture de Sécurité Industrielle, 2006.

[IEC61508 98] IEC61508, Functional safety of electrical/electronic/programmable electronic (e/e/pe) safety related systems. International Electrotechnical Commission (IEC), 1998.

[IEC61511 00] IEC61511, Functional safety : Safety instrumented systems for the process industry sector. International Electrotechnical Commission (IEC), 2000.

[INN 08] Innal, F. ,Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances Analyse critique de la norme CEI 61508. PhD thesis, Université Bordeaux I, France, 2008.

[JK 04] JK joint venture « Vendor instrument integrity level report »,In Amenas,2004.

[MAS 92] D. W. Massaro, «Broadening the domain of the Fuzzy Logical Model of Perception». In: H.L. Pick, P. Van Den Broek et D.C. Knill (Eds), Cognition: Conceptual and methodological issues, Washington, DC, 1992.

[MAZ 08] Mazouni, M.-H, Pour une Meilleure Approche du Management des Risques : De la modélisation Ontologique du Processus Accidentel au Système Interactif d'Aide à la Décision. PhD thesis, Nancy Université, Institut Nationnal Polytechnique de Lorraine, France, 2008.

[MEC 11] Mechri.W,Evaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis.Doctorat thesis,Tunis université, Ecole Nationale d'Ingénieurs de Tunis,2011.

[MKH 08] Mkhida, A, Contribution à l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité intégrant de l'Intelligence. PhD thesis, Nancy Université, Institut Nationnal Polytechnique de Lorraine, France, 2008.

[NAI 09] R. Nait-Saïd, F. Zidani and N. Ouzraoui, Modified risk graph method using fuzzy rule-based approach, Journal of Hazardous Materials, vol. 164, no. 2-3, pp. 651-658, 2009.

[OHS 99] OHSAS18001, Système de management de la santé et de la sécurité au travail-Spécification - BSI, Afnor, 1999.

[ORM 04] L.Ormos, I.Ajtonyi, Soft computing method for detemining the safety of technological system by IEC 61508, in :Romanian-Hungarian Joint Sympsiom on Applied Computational Inelligence, Timisoara, 2004.

[RAU 93] Rauzy, A, New algorithms for fault trees analysis. Reliability Engineering & System Safety, 59(5) :203-211, 1993.

[RAU 04] Rausand, M. and Hoyland, A, System Reliability Theory ; Models, Statistical Methods and Applications. New York, Wiley, 2nd edition, 2004.

[RAU 06] Rauzy, A., Dutuit, Y., and Signoret, J.-P, Assessment of safety integrity levels with fault trees. In ESREL Estoril, Portugal, 2006.

[SAL 06a] Sallak, M., Simon, C., and Aubry, J.-F, Aide à la décision dans la réduction de l'incertitude des sil : une approche floue/possibiliste. e-STA, Revue des Sciences et Technologies de l'Automatique, 2006.

[SAL 06b] Sallak, M., Simon, C., and Aubry., J.-F, Evaluating safety integrity level in presence of uncertainty. In In KONBiN, The 4th International Conference on Safety and Reliability, Krakow, Poland, 2006.

[SAL 07] Sallak, M, Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : Application aux Systèmes Instrumentés de Sécurité. PhD thesis, Nancy Université, Institut Nationnal Polytechnique de Lorraine, France, 2007.

[SAL 08] Sallak, M., Simon, C., and Aubry, J.-F, A fuzzy probabilistic approach for determining safety integrity level. IEEE Transactions on Fuzzy Systems, 16(1) :239-248, 2008.

[SCH 10] Schonbeck, M., Rausand, M., and Rouvroye, J, Human and organisational factors in the operational phase of safety instrumented systems : A new approach. Safety Science, 48 :310-318, 2010.

[SHA 05] R. K. Sharma, D. Kumar and P. Kumar, « Systemic failure mode effect analisis (FMEA) using fuzzy linguistic modeling », International Journal of Quality & Reliability Management, vol. 22, no 9, pp. 986-1004, 2005.

[SIG 04] Signoret, J.-P, High integrity protection system (hips)overcoming sil calculation difficulties. Technical report, TOTAL document, Pau, 2004.

[SIG 06] Signoret, J.-P, Managing risks in hips by making sil calculations effective. In IQPC2006, Aberdeen, Great Britain, 2006.

[SIG 07] Signoret, J.-P., Dutuit, Y., and Rauzy, A, High integrity protection systems (hips) : Methods and tools for efficient safety integrity levels (sil) analysis and calculations. In Risk, Reliability and Societal Safety Aven and Vinnem (eds), 2007.

[SIM 07] Simon, C., Sallak, M., and Aubry., J.-F, SIL allocation of sis by aggregation of experts opinions. In ESREL, Safety and Reliability Conference, Stavanger, Norvège, 2007.

[SMI O4] D.J. Smith, K.J.L. Simpson, Functional Safety : A straightforward Guide to Applying IEC 61508 and related Standards, Elsiever Butterworth-Heinemman, 2004.

[VIL 87] Villemeur, A, Evaluation de la fiabilité, disponibilité et maintenabilité des systèmes réparables : la méthode de l'Espace des Etats. Number 2. Eyrolles, 1987.

[VIL 98] Villemeur, A, Sûreté de fonctionnement des systèmes industriels. Number 2. Eyrolles, 1998.

[ZAD 65] L. Zadeh, Fuzzy sets , Information and Control, vol. 8, pp. 338–353, 1965.

[ZAD 75] L. Zadeh, The concept of a linguistique variable an dits application to approximate reasoning—I—II , Information Sciences, vol. 8, no. 3, pp. 199-249, 301-357, 1975.

[ZAD 78] L. Zadeh, Fuzzy sets as a basis for a theory of possibility , Fuzzy Sets and Systems, vol. 1, pp. 3–28, 1978.

[ZAD 92] L. Zadeh, « The calculus of fuzzy if/then rules », AI Expert, vol. 7, pp.23-27, 1992.

[ZHA 03] Zhang, T., Long, W., and Sato, Y ,Availability of systems with self- diagnostic components-applying markov model to iec 61508-6. Reliability Engineering Systems Safety, 80 :133141, 2003.