Allocation de SIL par aggrégation d'avis d'experts

Christophe Simon, Mohamed Sallak, Jean-François Aubry

ALLOCATION DE SIL PAR AGREGATION D'AVIS D'EXPERTS
SIL ALLOCATION BY AGGREGATION OF EXPERT OPINIONS

Simon C.
CRAN UMR 7039, CNRS-UHP-INPL
ESSTIN, 2 rue Jean Lamour
54519 Vandœuvre lès Nancy

Sallak M. et Aubry J.F.
CRAN UMR 7039, CNRS-UHP-INPL
ENSEM, 2 Avenue de la forêt de Haye
54506 Vandœuvre lès Nancy

Résumé

Les exigences sociétales actuelles imposent que les installations industrielles présentent le moins de risques possibles durant leur utilisation. Pour réduire la probabilité d'apparition du risque, les Systèmes Instrumentés de Sécurité (SIS) sont utilisés pour la mise en œuvre d'actions de mise en repli lorsque le système se place dans des conditions d'exploitation dangereuses. Pour concevoir ces SIS, deux normes sont utilisées : ANSI/ISA S84.01-1996 et l'IEC 61508. Ces deux normes définissent le niveau d'Intégrité de Sécurité (SIL) nécessaire pour se conformer aux exigences de réduction de risques requises pour les systèmes. A cette fin, le graphe de risque propose une approche pour l'allocation du niveau de SIL. Notre objectif est de formaliser une approche floue du graphe de risque ainsi que des systèmes de cotation subjective des paramètres de risque pour mieux appréhender l'imprécision et l'incertitude dans le processus d'allocation du niveau de SIL.

Summary

The society current requirements impose that the industrial provide a safe working environment during the use of system process. The Safety Instrumented System (SIS) consists of instrumentation that is implemented for the purpose of mitigating a risk or bringing the process to a safe state in the event of a process failure. The ANSI/ISA S84.01-1996 and IEC 61508 safety standards provide guidelines for the design of SIS. The standards define the requirement of Safety Integrity Level (SIL) of SIS. The risk graph method is widely used for the SIL allocation. Our objective is to formalize a fuzzy approach of the risk graph method as well as a subjective evaluation of risk parameters for a better manipulation of the inaccuracy and uncertainty during the SIL allocation.

Introduction

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. Pour réduire la probabilité d'apparition du risque, les Systèmes Instrumentés de Sécurité (SIS) sont utilisés pour réaliser des Fonctions Instrumentées de Sécurité (SIF) dont le rôle est la surveillance des paramètres de fonctionnement et la mise en œuvre d'actions de mise en repli lorsque le système se place dans des conditions d'exploitation dangereuses. Pour concevoir ces SIS, deux normes sont utilisées : ANSI/ISA S84.01-1996 [1] et l'IEC 61508 [2]. Ces deux normes sont basées sur le principe de l'évaluation de la réduction du risque nécessaire pour atteindre un niveau de risque sociétalement admissible. Après une analyse préliminaire des risques et une évaluation quantitative de la probabilité d'apparition des risques identifiés, il est nécessaire d'évaluer la réduction nécessaire du risque en fonction d'un niveau d'intégrité de sécurité (SIL) exigé. L'IEC 61508 [1] encadre cette démarche et propose, entre autre, la méthode du graphe de risque pour allouer le niveau de SIL requis. Cette allocation est réalisée par avis d'experts sur la base du graphe de risque.

Nous proposons dans cette communication, une méthode d'évaluation subjective adaptée à la problématique de l'allocation du niveau de SIL. Cette méthode a été appliquée dans de nombreux problèmes d'évaluation par des experts ([3], [4], [5]). Nous explicitons la technique de cotation spécifique qui permet à chaque expert d'utiliser un référentiel de valeurs qui lui est propre. Nous précisons la technique utilisée pour permettre à l'expert d'exprimer l'imprécision de sa perception en s'appuyant sur les nombres flous et la théorie des possibilités. Nous indiquons ensuite la procédure qui permet d'agréger les distributions de possibilités correspondant aux cotations des différents experts et comment tenir compte du niveau de compétence de l'expert. Enfin, nous montrons la transposition du graphe de risque pour la détermination du niveau de SIL à allouer à partir d'informations imprécises et incertaines.

Procédure pour atteindre les allocations de SIL

Dans cette section, nous décrivons la procédure générale pour atteindre les allocations de sécurité d'un système afin d'assurer la conformité aux normes de sécurité ANSI/ISA S84.01-1996 [1] et IEC 61508 [2]. Ensuite, nous présentons les différentes méthodes qualitatives et quantitatives utilisées pour la détermination des SIL.

Systèmes Instrumentés de Sécurité (SIS)

Un SIS est un système visant à mettre un procédé en position de replis de sécurité (c'est-à-dire un 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 ...).
Un SIS se compose de trois parties (cf. Figure 1) :

- Une partie capteur chargée de surveiller la dérive d'un paramètre (pression, température ...) vers un état dangereux.
- Une partie système de traitement logique chargée de récolter le signal provenant du capteur, de traiter celui-ci et de commander l'actionneur associé.
- Une partie actionneur chargée de mettre le procédé dans sa position de sécurité et de la maintenir.

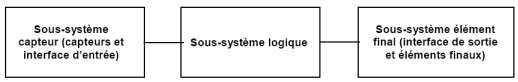


Figure 1 : Structure générale d'un SIS

La probabilité moyenne de défaillance du SIS est déterminée par le calcul et la combinaison des probabilités moyennes de défaillance de ses composants. Ces probabilités dépendent des taux de défaillance et de réparation des composants, du facteur qui caractérise les défaillances de cause commune … [2].

Conformité aux normes ANSI/ISA S84.01-1996 et IEC 61508

Les normes ANSI/ISA S84.01-1996 [1] et IEC 61508 [2] établissent les prescriptions relatives à la spécification, la conception, l'installation, l'exploitation et la maintenance du SIS, afin d'avoir toute confiance dans sa capacité à amener et/ou à maintenir le procédé dans un état de sécurité. Les étapes de base requises pour assurer la conformité à ces deux normes de sécurité sont :

1. Etablir une cible de sécurité (risque acceptable) du système et évaluer le risque existant.
2. Identifier les fonctions de sécurité requises et les affecter aux niveaux de protection.
3. Déterminer si la fonction instrumentée de sécurité est requise.
4. Implémenter la fonction instrumentée de sécurité dans un SIS et déterminer le SIL du SIS.

5. Vérifier que le SIS permet d'atteindre la cible de sécurité exigée au départ.

Le tableau 1 donne le niveau SIL du SIS en fonction de la valeur de sa probabilité moyenne de défaillance PFD_{avg} et de sa fréquence de sollicitation.

Sollicitation	Demande faible	Demande élevée
SIL	PFD_{avg}	défaillances/heures
4	$10^{-5} \leq PFD_{avg} \leq 10^{-4}$	$10^{-9} \leq N \leq 10^{-8}$
3	$10^{-4} \leq PFD_{avg} \leq 10^{-3}$	$10^{-8} \leq N \leq 10^{-7}$
2	$10^{-3} \leq PFD_{avg} \leq 10^{-2}$	$10^{-7} \leq N \leq 10^{-6}$
1	$10^{-2} \leq PFD_{avg} \leq 10^{-1}$	$10^{-6} \leq N \leq 10^{-5}$

Tableau 1 : Définition du SIL selon la norme IEC 61508

Méthodes de détermination des niveaux de SIL

La détermination du SIL d'un SIS peut s'obtenir par différentes méthodes:

1. Méthodes qualitatives [1, 6]: Il s'agit de méthodes qui permettent de déterminer le niveau de SIL à partir de la connaissance des risques associés au système.
2. Méthodes semi quantitatives [1, 7]: La méthode la plus répandue est la matrice de risque. Cette matrice donne le niveau de SIL en fonction de la gravité du risque et de sa fréquence d'occurrence.
3. Méthodes quantitatives [6, 7, 8]: Il s'agit des méthodes qui permettent de calculer la disponibilité des SIS à partir des taux de défaillance et de réparation de leurs composants. Les méthodes les plus répandues sont:

- Les équations simplifiées ;
- Les arbres de défaillances ;
- Les approches Markoviennes.

Dans cet article, nous nous intéressons uniquement à l'étude des SIS faiblement sollicités et à l'approche qualitative de l'allocation de SIL.

Méthode du graphe de risque

Généralités

La méthode qualitative la plus utilisée pour déterminer le niveau de SIL est la méthode dite du « graphe de risque » [2]. 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.

Synthèse du graphe de risque

La procédure simplifiée s'appuie sur l'équation suivante:

$$R = f \times C \qquad [1]$$

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).

Ces paramètres de risque sont considérés comme suffisamment génériques pour concerner la plupart des applications. Toutefois certaines peuvent nécessiter des paramètres de risque supplémentaires comme les systèmes utilisés dans les nouvelles technologies. Dans cet article, on considère uniquement les quatre paramètres définis précédemment mais il n'y a aucune restriction à l'intégration d'une formulation plus complète.

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 2.

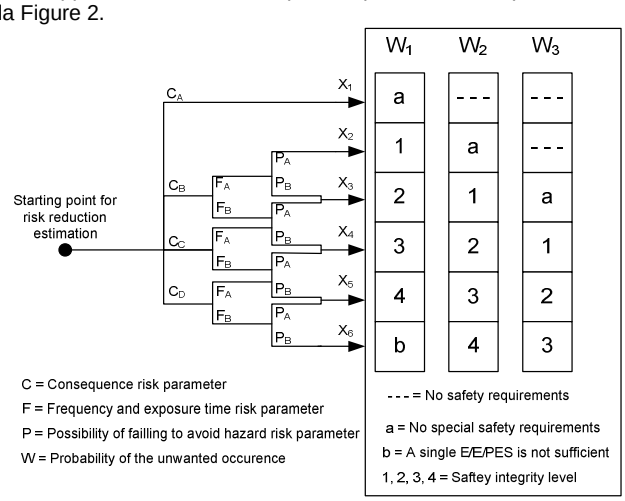


Figure 2 : Graphe de risque

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 X_1, X_2, $X_3 \ldots X_n$. 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 (W_1, W_2 et W_3). 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 W_1, W_2 ou W_3 permet de réaliser la contribution d'autres mesures de réduction du risque. Le décalage dans les échelles W_1, W_2 et W_3 est nécessaire pour avoir trois niveaux différents de réduction des risques à partir d'autres mesures. Cette échelle est composée de l'échelle W_3, 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 W_2 une contribution moyenne et l'échelle W_1 une contribution maximale. Pour une sortie spécifique du graphe de risque (c'est-à-dire X_1, $X_2 \ldots$ou X_6) et, pour une échelle W spécifique (c'est-à-dire W_1, W_2 et W_3), 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.

Recueil et agrégation des avis d'experts

Le graphe de risque s'appui sur les quatre paramètres C, F, P et W que nous avons mentionnés ci-dessus. Le contexte sociétal et la transposition de l'avis des experts dans ce domaine rendent le processus particulièrement subjectif. En outre, une échelle numérique chiffrée peut entraîner une perte de dynamique dans la notation à cause de la conséquence associée à la valeur chiffrée. On remarque également qu'une note unique traduit rarement une évaluation et l'expert préfère souvent utiliser un intervalle. Enfin, une valeur unique ne permet pas lors de la phase d'agrégation de trouver un consensus autre que la moyenne pondérée ou non pondérée. En proposant des intervalles, on peut éventuellement trouver une intersection permettant d'établir un consensus.

Pour l'ensemble de ces raisons, il est donc plus pertinent de remplacer l'échelle de valeur discrète par une échelle continue, graduée nominalement, délimitée par des qualificatifs antagonistes aux extrémités, afin de permettre aux experts d'exprimer leur perception imprécise de la conséquence. La même démarche d'analyse peut être réalisée sur les paramètres

F et P. Le paramètre W est un paramètre résultat d'une analyse quantitative. Toutefois, nous avons montré dans [9] que l'approche quantitative était soumise à des imprécisions dont les effets peuvent être pris en compte par la théorie des possibilités. Les avis des experts sont ensuite collationnés sous forme de courbes trapézoïdales et nous les modélisons par des distributions de possibilités. L'intérêt par rapport à une modélisation sous forme d'intervalles stricts est d'introduire une gradation dans les intervalles choisis par l'expert. Pour chaque paramètre, les distributions de possibilités sont agrégées par une règle conjonctive tout en tenant compte de la pondération des experts vue comme une incertitude au sens de la théorie des possibilités [13]. L'allocation du niveau de SIL requis est obtenue en parcourant le graphe de risque comme un arbre flou de décision. Le degré de possibilité d'allocation de chaque niveau de SIL est obtenu et la décision d'allocation est prise en tenant compte de chaque mesure de possibilités obtenue.

Echelle d'évaluation

La pratique habituelle du recueil d'avis sur la base d'une taxinomie stricte est le questionnaire élaboré avec des cases à cocher (Figure 3). Dans ce cas, plusieurs difficultés peuvent être rencontrées aussi bien pour l'expert que pour le concepteur du questionnaire. Si on utilise une taxinomie stricte, l'expert ne peut exprimer son incertitude et l'imprécision de sa perception qu'en cochant deux cases au moins. Cette situation est difficile à appréhender dans le graphe de risque car elle reporte la décision sur l'espace de conclusion (niveau de SIL). Si il ne souhaite pas utiliser cette technique, l'expert sera contraint de mettre en relation le choix de la modalité du paramètre à évaluer avec l'impact que celui-ci aura sur la décision. Le concepteur doit élaborer une taxinomie donnant suffisamment de dynamique tout en empêchant le statu quo. L'élément de questionnaire de la Figure 3 est une solution habituellement proposée.

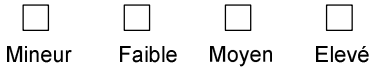


Figure 3 : Elément classique de questionnaire

Les travaux sur l'évaluation subjective apportent une solution à ces problèmes [13, 14, 15]. Plutôt que d'évaluer les paramètres de risque sur une échelle numérique qui peut entraîner une distorsion notamment vers les valeurs extrêmes, nous proposons d'utiliser un axe continu gradué nominalement et borné par des qualificatifs antagonistes comme le montre la Figure 4.

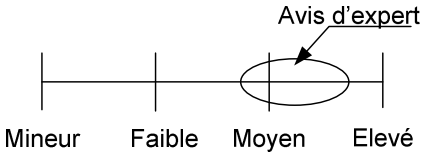


Figure 4 : Echelle d'évaluation

Evaluation subjective des paramètres de risque

Afin de permettre aux experts d'exprimer leur perception imprécise des paramètres C, F, P et W, on leur propose d'utiliser l'échelle d'évaluation de chaque paramètre dans une forme proche de celle de la Figure 4. Afin de capturer chaque évaluation sous une forme informatiquement exploitable, nous proposons d'utiliser des nombres flous trapézoïdaux. Chaque expert donne ainsi deux intervalles imbriqués. L'intervalle le plus large, servant de support, correspond au sous-ensemble de l'axe d'évaluation en dehors duquel l'expert est certain que la valeur réelle ne se trouve pas. L'intervalle le plus étroit, servant de noyau, correspond au sous-ensemble de l'axe d'évaluation dans lequel l'expert pense que la valeur réelle a le plus de possibilités de se trouver.
Ainsi, pour la conséquence C, on donne un exemple d'évaluation où les variables utilisées sont données par (cf. Figure 5):

- Mineur : préjudice mineur.
- Faible : préjudice sérieux permanent.
- Moyen : mort de quelques personnes.
- Elevée : plusieurs personnes tuées.

La même démarche d'analyse est réalisée sur les paramètres F, P et W.

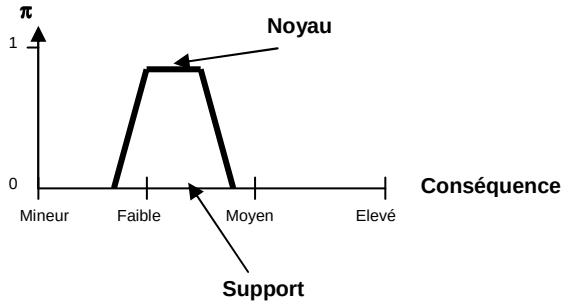


Figure 5 : Evaluation de la conséquence C

Agrégation des évaluations

Nous disposons pour chaque expert e_i d'un ensemble d'évaluations, sous forme de distributions de possibilités $\pi_{ei,cj}$ où c_j représente le paramètre de risque $i \in \{C, P, F, W\}$. Nous avons également pour chaque expert son niveau d'expertise $NE(e_i, c_j)$ dans l'évaluation de chaque paramètre.
Dans le cadre possibiliste, plusieurs modes d'agrégation des évaluations sont possibles. Le premier est le mode conjonctif. Il est utilisé lorsque l'on considère tous les experts comme fiables et correspond à l'intersection des évaluations. Ce mode est sensible à des évaluations discordantes. Lorsque l'on considère que dans un groupe d'expert l'un d'eux est fiable mais sans savoir lequel, on utilise alors le mode disjonctif, *i.e.* l'union des évaluations. Ce mode peut conduire à des résultats peu informatifs. D'autres modes, que nous ne détaillerons pas ici, sont encore possibles [14].
Dans notre exemple, nous cherchons à agréger les évaluations en tenant compte du retour d'expérience dont dispose chaque expert relativement aux quatre paramètres. Ainsi l'agrégation des évaluations va être réalisée pour chaque paramètre relativement à l'expertise des experts. Le niveau d'expertise $w_{eij} = NE(e_i, c_j)$ d'un expert vient modifier la distribution de possibilités [10] représentant son évaluation π selon la relation suivante:

$$\pi'_{e_i,c_j} = \max\left(\pi_{e_i,c_j}, 1 - w_{eij}\right) \quad [2]$$

Ainsi, si l'expert est fiable, $w_{eij}=1$, et son évaluation n'est pas modifiée. Lorsque l'expert est moins fiable, $0 \leq w_{eij} < 1$, un niveau d'incertitude vient modifier l'évaluation. Finalement, si l'évaluateur n'est pas fiable du tout, $w_{eij}=0$, alors on obtient une distribution de possibilités égale à 1 sur l'ensemble du support. Cette distribution représente l'ignorance sur la position de l'évaluation puisque l'expert n'est pas fiable.
Dans notre exemple, nous considérons trois niveaux d'expertise pour lesquels nous attribuons les valeurs *expert* → w_{eij} =1, à intermédiaire → w_{eij} =0.6 et à néophyte → w_{eij} =0.3. Ce niveau d'expertise est a priori défini par l'expert lui-même, en relation avec le domaine d'application à traiter. Toutefois, il est possible de concevoir d'autres procéder de réglage.
Finalement, les distributions résultantes, considérées comme fiables, sont agrégées suivant la règle conjonctive suivante [9]:

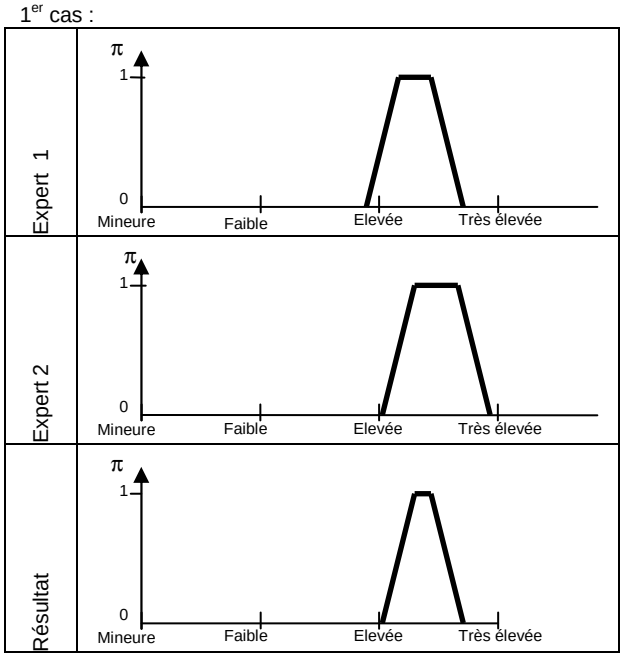
$$\pi'_{c_j} = \min_{e_i}\left(\pi'_{e_i,c_j}\right) \quad [3]$$

Dans le cas d'évaluations conflictuelles des experts, il peut arriver que le résultat ne soit pas normalisé, *i.e.* qu'une valeur au moins soit à 1. Dans ce cas, nous appliquons la règle de normalisation :

$$\pi'_{c_j} = \pi_{c_j} + \left(1 - \sup\left(\pi_{c_j}\right)\right) \quad [4]$$

Les exemples qui suivent montrent comment sont agrégées les évaluations du paramètre (C) par deux experts dans des cas de figures différents.

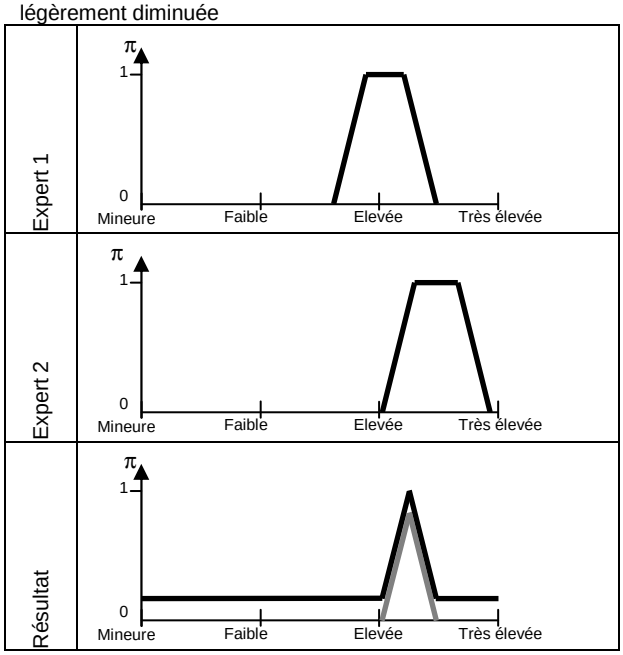
1er cas :



Dans ces trois premiers exemples, nous avons considéré que les deux experts ont des niveaux d'expertise *expert.*

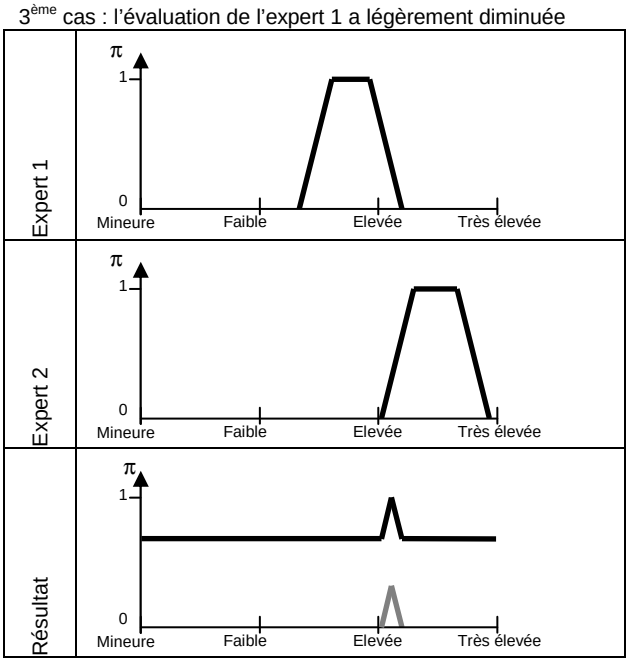
Nous pouvons voir que les deux experts sont en accord, puisque les noyaux de leur évaluation ont une partie commune que l'on retrouve comme noyau du résultat.

2ème cas : seule l'évaluation de l'expert 1 a changée, elle a légèrement diminuée



Ici, les deux experts ne sont pas tout à fait d'accord. Ainsi, les noyaux de leurs évaluations n'ont plus de zone commune. En gris clair on voit le résultat de l'agrégation qui n'est pas normalisé montrant ainsi le conflit. Le résultat final en noir après normalisation montre l'incertitude due au conflit existant entre les deux examinateurs. On peut voir que l'incertitude n'est pas très importante puisque le noyau de l'évaluation se démarque nettement.

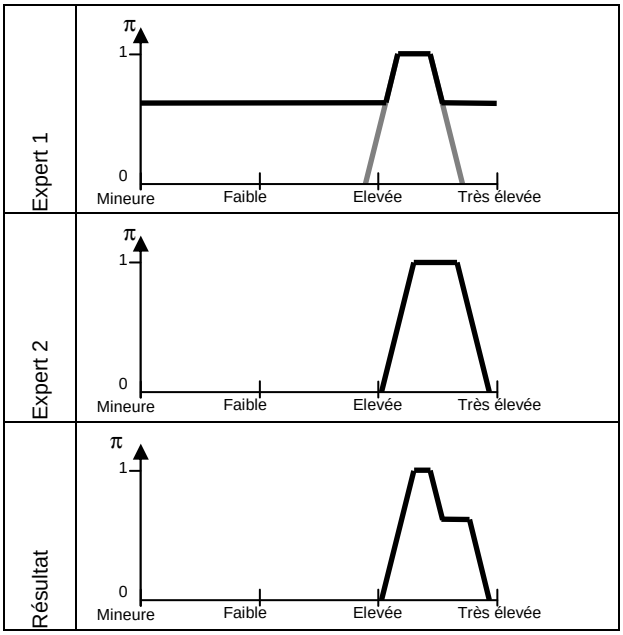
3ème cas : l'évaluation de l'expert 1 a légèrement diminuée



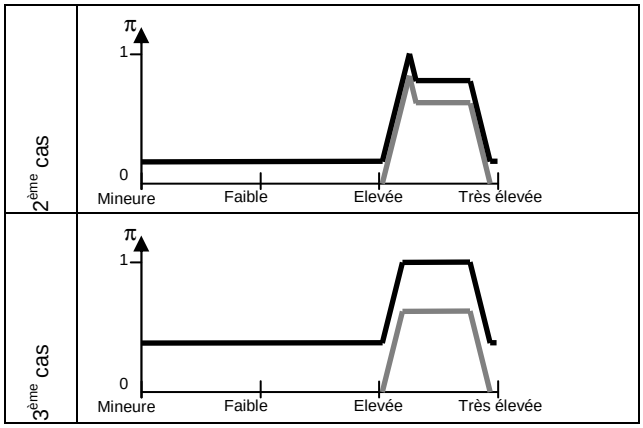
Ici, le conflit entre les experts est beaucoup plus important, et au final, le noyau de l'évaluation se démarque peu. C'est donc le désaccord entre les experts qui fait apparaitre une incertitude significative dans l'évaluation du critère c_j.

Nous reprenons les trois exemples précédents, mais cette fois les experts n'ont pas le même niveau d'expertise. Le premier est néophyte tandis que le deuxième est expert.

1er cas : pour l'expert 1, nous retrouvons en gris son évaluation, et en noir la distribution utilisée après prise en compte de son niveau d'expertise à l'aide de l'équation 2.



Dans les deux autres cas nous obtenons comme résultats :



Cette technique de cotation permet de disposer d'une évaluation de chaque paramètre de base du graphe de risque. L'ensemble des évaluations tient compte de l'imprécision et de l'incertitude de chaque expert et de son niveau d'expertise ou encore de l'incertitude liée à la discordance des avis des experts. Finalement, l'évaluation de chaque paramètre va pouvoir être combinée selon la logique du graphe de risque.

Graphe de risque flou

Le graphe de risque, dans sa structure présentée à la figure 2, ne permet pas l'exploitation des évaluations agrégées des experts. Il faut donc proposer un système reproduisant la logique du graphe tout en tenant compte des distributions de possibilités fournies par les experts. Les systèmes d'inférence floue vont nous offrir cette possibilité. Ormos et Ajtonyi [12] ont proposé un système d'inférence floue reposant sur un modèle propositionnel de Mamdani.

Partitions floues et fuzzification

Pour exploiter le système d'inférence floue, nous devons définir les partitions floues des 4 paramètres de risque (Figure 5) dans le référentiel fourni aux experts. Ces partitions floues permettent le calcul de la compatibilité entre les évaluations et les concepts caractérisés par les termes linguistiques du référentiel. Cette mesure de compatibilités, calculée par l'opérateur min, détermine la valeur des prémisses des règles d'inférence.

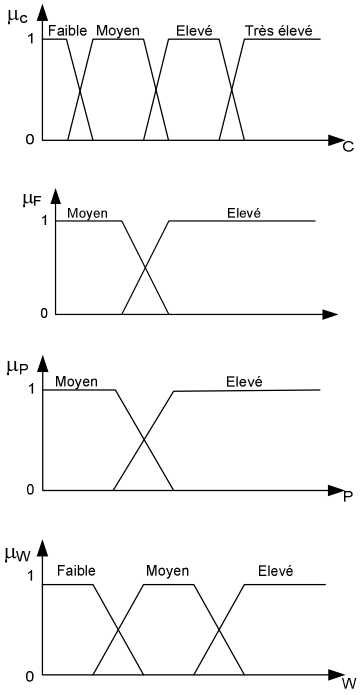


Figure 5 : Echelle d'évaluation

Inférence

Les règles d'inférence permettent de relier les variables floues d'entrée qui représentent les quatre paramètres de risque à la variable floue de sortie qui est le niveau de SIL, à l'aide de différents opérateurs. Les règles d'inférences font appel aux opérateurs T-normes (opérateurs ET) et T-conormes (opérateurs OU), qui s'appliquent aux variables floues. Dans le cas de la logique binaire ces opérateurs sont définis de façon simple et univoque. Dans le cas de la logique floue, la définition de ces opérateurs n'est plus univoque et on utilise le plus souvent les relations présentées dans le tableau 2 [11].

T-norme	T-conorme	Négation	Nom
min(x,y)	max(x,y)	1 - x	Zadeh
x.y	x + y - xy	1 - x	probabiliste
max(x + y - 1, 0)	min(x + y, 1)	1 - x	Lukasiewicz
x si y = 1 y si x = 1 0 sinon	x si y = 0 y si x = 0 1 sinon	1 - x	drastique

Tableau 2 : Opérateur d'agrégation des règles d'inférence

Les opérations minimum et maximum présentent l'avantage de la simplicité lors du calcul, par contre, elles privilégient l'une des deux variables. Les opérations de produit et valeurs moyennes sont plus complexes à calculer mais elles produisent un résultat qui tient compte des valeurs des deux variables.
Dans cet article, la combinaison de ces différentes règles se fait à l'aide de l'opérateur « ET ». La justification du choix de l'opérateur se fonde sur l'interprétation du graphe de risque donné dans la norme IEC 61508 (cf. Figure 2). En effet, une telle énumération est comprise dans le sens :
Si (C est Elevé) ET (F est moyen) ET (P est mineur) ET (W est mineur) ALORS (SIL est SIL1)
ET
Si (C est Moyen) ET (F est Moyen) ET (P est Moyen) ET (W est Elevé) ALORS (SIL est SIL2)
ET ...
Selon la règle du modus ponens [11], c'est l'évaluation de la compatibilité entre les avis agrégés des experts et les fonctions d'appartenance qui va donner l'amplitude d'exécution de la règle et par conséquence de la conclusion.

Partition floue de sortie et défuzzification

En correspondance avec le graphe de risque et le référentiel de sortie, deux partitions floues sont possibles. Les niveaux de SIL définissent une échelle ordinale à partir de l'ensemble {a, SIL1, SIL2, SIL3, SIL4, b}. Toutefois, les niveaux de SIL font référence à une échelle continue de l'ensemble des valeurs de réduction de risque nécessaire. Dans ce cas, la partition floue correspond à l'ensemble d'intervalles définis par le tableau 1.
La décision correspond à l'étape de défuzzification. Plusieurs méthodes existent [11], le centre de gravité est privilégié dans une recherche de consensus sur un référentiel continu de sortie. La méthode du maximum est préférée dans le cas d'un référentiel ordinal.
Dans cet article, l'échelle ordinale et la défuzzification par le maximum sont choisies.

Application

On considère un système constitué d'un réservoir sous pression contenant un liquide inflammable volatil (cf. Figure 6). Ce réservoir peut rejeter des gaz dans l'atmosphère.
On suppose que le risque acceptable est défini sous forme d'un taux moyen de rejet de gaz inférieur à 10^{-4} par an. Une analyse des phénomènes dangereux liés à ce système a montré que les systèmes de protection disponibles (alarmes et niveaux de protection) sont insuffisants pour assurer ce risque acceptable (le non dépassement du seuil imposé pour le rejet des gaz).

Notre objectif est de déterminer le niveau d'intégrité de sécurité (SIL) d'une fonction instrumentée de sécurité (SIF) qui permettra d'atteindre le niveau de seuil imposé, à partir de la connaissance des risques associés au réservoir.

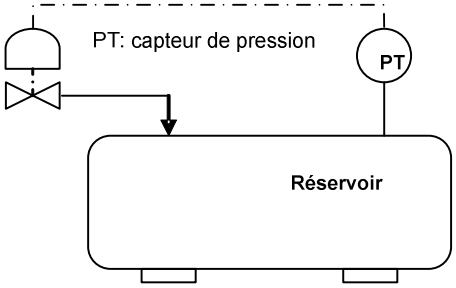


Figure 6 : Réservoir sous pression

On donne, ci-dessous, les données relatives à la classification des paramètres de risque [2] que nous avons appliqués.

- Signification des quatre fonctions d'appartenance de la conséquence (C) :
  - Faible : Préjudice mineur
  - Moyen : Préjudice sérieux permanent touchant une ou plusieurs personnes
  - Elevé : Mort de plusieurs personnes
  - Très élevé : Plusieurs personnes tuées
- Signification des deux fonctions d'appartenance de la fréquence d'exposition dans une zone dangereuse (F) :
  - Moyen : Exposition rare à fréquente dans une zone dangereuse
  - Elevé : Exposition fréquente à permanente dans une zone dangereuse
- Signification des deux fonctions d'appartenance de la possibilité d'éviter les événements dangereux (P) :
  - Moyen : Possible sous certaines conditions
  - Elevée : Presque impossible
- Signification des trois fonctions d'appartenance de la probabilité d'occurrence non souhaitée (W) :
  - Faible : Une probabilité très faible que des occurrences non souhaitées surviennent ou seulement quelques occurrences non souhaitées sont probables
  - Moyen : Une probabilité faible que des occurrences non souhaitées surviennent ou seulement quelques occurrences non souhaitées sont probables
  - Elevé : Une probabilité forte que des occurrences non souhaitées surviennent ou il est probable que des occurrences non souhaitées surviennent fréquemment.

Par la suite, chaque expert définit pour chaque paramètre de risque la distribution de possibilités correspondant à son évaluation (cf. Figure 8) à partir des données relatives à la classification des paramètres de risque que nous avons appliqués. Les avis des experts seront agrégés selon la méthode décrite dans la section relative aux méthodes d'agrégations.

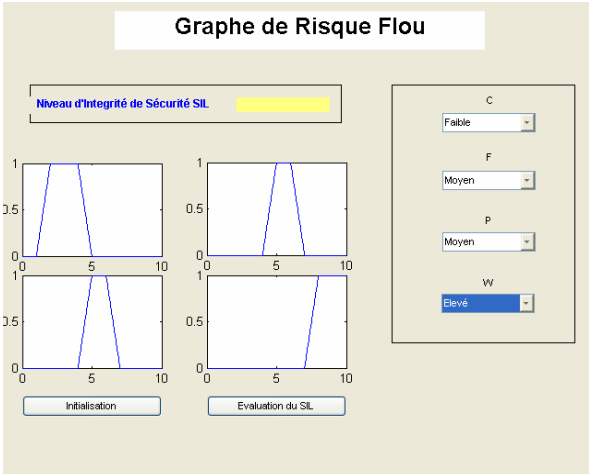


Figure 8 : Choix des fonctions d'appartenance

En appliquant les règles d'inférences décrites précédemment et après la défuzzification, on obtient le niveau de SIL recherché. On peut aussi représenter la variation du niveau de SIL en fonction des différents paramètres de risque. La Figure 9 donne une représentation du niveau de SIL en fonction de la conséquence (C) et de la fréquence d'exposition dans une zone dangereuse (F). Le principal apport de la méthode d'agrégation proposée est qu'elle permet d'obtenir une distribution du niveau de SIL en fonction des différents paramètres de risque en tenant compte aussi des conflits des experts lors de leur évaluation de ces paramètres.

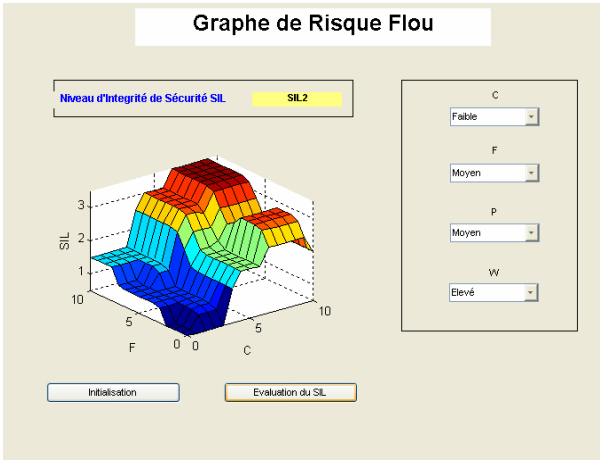


Figure 9 : Evaluation du niveau de SIL

En outre, après défuzzification, on déduit le niveau d'intégrité de sécurité (SIL) de la fonction instrumentée de sécurité (SIF) qui permettra d'atteindre le niveau de seuil imposé, à partir de la connaissance des risques associés au réservoir qui est le niveau SIL 2 (cf. Figure 9).

Conclusion

Dans cet article, nous avons proposé une méthode qualitative d'allocation de SIL à l'aide d'un graphe de risque flou et d'un système d'évaluation subjective pour le recueil et l'agrégation d'avis d'experts. Cette méthode utilise une technique de cotation qui permet à chaque expert d'utiliser un référentiel de valeurs qui lui est propre pour exprimer l'imprécision de sa perception de l'importance des paramètres de risque, en s'appuyant sur les nombres flous et la théorie des possibilités.
Cette approche a été appliquée sur un exemple d'application cité de la littérature [8] en proposant un outil basé sur l'utilisation d'un système d'inférence floue.
Cette approche présente l'avantage de donner des échelles de cotation non spécifiques au domaine d'application. Il est donc envisageable d'utiliser cette approche dans des contextes internationaux où les référentiels ne sont pas homogènes et les pratiques différentes de l'art expertal. En outre, la méthodologie est particulièrement ouverte à la prise en compte d'autres paramètres de risque. Nous devons également évaluer l'influence des différents choix d'opérateurs flous dans la méthodologie mais aussi l'appropriation de l'outil par les experts.

Références

[1] ANSI/ISA-S84.01-1996, Application of Safety Instrumented Systems for the process control industry, Instrumentation Society of America (ISA), 1996.
[2] IEC 61508, Functional safety of Electrical/ Electronic/Programmable Electronic (E/E/PE) safety related systems, International Electrotechnical Commission (IEC), 1998.
[3] Dubois D., Prade H., The three semantics of fuzzy sets, Fuzzy sets and systems, 90, 1997, 141-150.
[4] Sandri S.A., Dubois D., Kalfsbeek H., Elicitation, Assessment, and Pooling of Expert Judgements Using Possibility Theory, IEEE Transactions on Fuzzy Systems, 3, 1995, 313-335.

[5] Zadeh L.A., Fuzzy Sets, Information and control, 8, 1965, 338-353.
[6] Stavrianidis P., Bhimavarapu K., Safety Instrumented Functions and Safety Integrity Levels (SIL), 1998, ISA Transactions, 37, 337–351.
[7] Bhimavarapu K., Moore L., Stavrianidis P., Performance based safety standards: an integrated risk assessment program, ISA TECH, 1, 1997.
[8] ISA-TR84.00.02-2002, Safety Instrumented Functions (SIF), Safety Integrity Level (SIL), Evaluation Techniques, Instrumentation Society of America (ISA), 2002.
[9] Sallak M., Aubry J.F., Simon C., Arbres de Défaillances à taux imprécis et facteurs d'importance flous, Journées Doctorales MACS, Lyon, 5-7 Septembre 2005.
[10] Sandri S.A., Dubois D., Kalfsbeek H., Elicitation, Assessment, and Pooling of Expert Judgements Using Possibility Theory, IEEE Transactions on Fuzzy Systems, 3, 1995, 313-333.
[11] Bouchon-Meunier B., La logique floue et ses applications, Addison-Wesley France, 1990.
[12] Ormos L., Ajtonyi I., Soft computing method for determining the safety of technological system by IEC61508, 1st Romanian - Hungarian Joint Symposium on Applied Computational Intelligence, 2004.
[13] Simon C., Voisin A., Grosjean L., Levrat E., Evaluation subjective appliquée à la notation d'étudiants, CETSIS'05, Nancy, 25-27 octobre 2005.
[14] Voisin A., Levrat E., Evaluation of a sensory measurement fuzzy system for car seat comfort, 10th IEEE International Conference on Fuzzy Systems, Melbourne, Australia, December 2-5, 2001.
[15] Évaluation subjective, Méthodes, applications et enjeux, Coll. "Les Cahiers des Clubs CRIN", 166 pages – 1997, Éditeur : ECRIN