Aide à la décision dans la réduction de l'incertitude des SIL : une approche floue/possibiliste

Mohamed Sallak, Jean-François Aubry, Christophe Simon

▶ **To cite this version:**

Mohamed Sallak, Jean-François Aubry, Christophe Simon. Aide à la décision dans la réduction de l'incertitude des SIL : une approche floue/possibiliste. e-STA Sciences et Technologies de l'Automatique, 2006, 3 (3), pp.Revue électronique. hal-00118741

HAL Id: hal-00118741
https://hal.science/hal-00118741

Submitted on 6 Dec 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Aide à la décision dans la réduction de l'incertitude des SIL : une approche floue/possibiliste

Mohamed Sallak [1], Jean-François Aubry [1], Christophe Simon [2]

[1]CRAN-ENSEM-INPL
2, Avenue de la forêt de Haye
54506, Vandoeuvre-Lès-Nancy, France

[2] CRAN-ESSTIN-UHP
2, Rue Jean Lamour
54519, Vandoeuvre-Lès-Nancy, France

mohamed.sallak@ensem.inpl-nancy.fr, jean-françois.aubry@isi.u-nancy.fr,
christophe.simon@esstin.uhp-nancy.fr

Résumé— **De nombreuses installations industrielles présentent des risques pour les personnes, l'environnement ou les équipements. Elles ont par conséquent fait l'objet d'études de risque et nécessitent parfois la mise en œuvre de Systèmes Instrumentés de Sécurité (SIS). Pour concevoir ces systèmes, deux normes sont utilisées : l'ANSI/ISA S84.01-1996 et l'IEC 61508. Cependant, les fiabilistes ont beaucoup de difficultés à mettre en œuvre les prescriptions de ces deux normes, notamment pour la détermination du niveau d'Intégrité de Sécurité (SIL) de chaque SIS. En outre, les méthodes de détermination des SIL proposées jusqu'à présent ne prennent pas en compte les incertitudes entachant les paramètres de fiabilité des composants du SIS. Dans cet article, nous proposons une approche floue/possibiliste pour déterminer le niveau de SIL des SIS à partir des paramètres de fiabilité incertains de leurs composants. L'introduction de deux nouveaux facteurs d'importance possibilistes permettra de réduire efficacement l'incertitude entachant le niveau de SIL obtenu.**

Mots-clés— **Système Instrumenté de Sécurité, niveau d'Intégrité de Sécurité, approche floue/possibiliste, incertitude, facteurs d'importance.**

I. Introduction

Lorsque les installations industrielles présentent des risques potentiels pour les personnes, l'environnement ou les biens, diverses sécurités sont mises en œuvre. Celles-ci participent soit à la prévention (en minimisant la probabilité d'apparition d'un risque), soit à la protection (pour limiter les conséquences d'un dysfonctionnement). Les Systèmes Instrumentés de Sécurité (SIS) sont souvent utilisés comme moyens de prévention pour réaliser ces Fonctions Instrumentées de Sécurité (SIF). Pour concevoir ces systèmes, deux normes sont utilisées : l'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 acceptable pour l'installation.
Les fiabilistes ont beaucoup de difficultés à mettre en œuvre les prescriptions de ces deux normes, notamment pour la détermination du niveau d'Intégrité de Sécurité (SIL) des SIS [3]. En conséquence, il est devenu primordial de trouver des méthodes fiables qui permettent de déterminer le niveau de SIL des SIS. En outre, les méthodes de détermination des SIL [2], [4], [5], [6], [7], [8], proposées jusqu'à présent, ne prennent pas en compte les incertitudes qui entachent les paramètres de fiabilité des composants du SIS. L'objectif de ce travail est de proposer une approche floue/possibiliste pour déterminer le niveau de SIL d'un SIS à partir des paramètres de fiabilité incertains de ses composants. L'introduction de deux nouveaux facteurs d'importance possibilistes permettra de mettre en évidence les composants contribuant le plus à l'incertitude entachant le niveau de SIL obtenu et de la réduire efficacement.
L'article est organisé de la façon suivante. La section II décrit la procédure pour atteindre les cibles de sécurité d'un procédé selon les normes ANSI/ISA S84.01-1996 [1] et IEC 61508 [2]. La section III présente l'approche proposée pour la détermination des SIL et introduit les nouveaux facteurs d'importance possibilistes. La section IV est dédiée à un exemple applicatif défini dans la littérature qui illustre l'approche présentée. Enfin, nous traçons le bilan de notre approche et des facteurs d'importance introduits en section V et présentons les perspectives de ce travail.

II. Procédure pour atteindre les cibles de sécurité d'un procédé

Dans cette section, nous décrivons la procédure générale pour atteindre les cibles de sécurité d'un procédé 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.

A. Systèmes Instrumentés de Sécurité

Un SIS est un système visant à mettre le procédé en position de repli 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 de paramètres (pression, température ...) vers un état dangereux.
- Une partie système de traitement logique chargée de récolter le signal provenant de la partie capteur, de traiter celui-ci et de commander la partie actionneur associée.
- Une partie actionneur chargée de mettre le procédé dans sa position de sécurité et de la maintenir.

La probabilité de défaillance sur demande (PFD) du SIS est déterminée par le calcul et la combinaison des probabilités de défaillances de ses composants. Ces probabilités dépendent de paramètres de sureté de fonctionnement des composants tels que les taux de défaillance et de réparation des composants, ou le facteur qui caractérise les défaillances de cause commune [2].

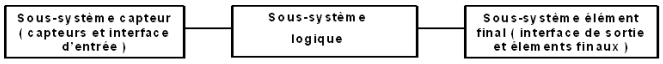

Fig. 1. Structure générale d'un Système Instrumenté de Sécurité

B. 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 procédé 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.

La table I donne le SIL du SIS en fonction de la valeur de son PFD et de sa fréquence de sollicitation.

SIL	Faible demande (PFD_{avg})	Demande élevée (Défaillances/heure)
4	$10^{-5} \leq PFD \leq 10^{-4}$	$10^{-9} \leq N \leq 10^{-8}$
3	$10^{-4} \leq PFD \leq 10^{-3}$	$10^{-8} \leq N \leq 10^{-7}$
2	$10^{-3} \leq PFD \leq 10^{-2}$	$10^{-7} \leq N \leq 10^{-6}$
1	$10^{-2} \leq PFD \leq 10^{-1}$	$10^{-6} \leq N \leq 10^{-5}$

TABLE I
NIVEAUX D'INTÉGRITÉ DE SÉCURITÉ SELON LA NORME IEC 61508

C. Méthodes qualitatives et quantitatives pour la détermination des SIL

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

1. Méthodes qualitatives [2], [8] : Il s'agit de méthodes qui permettent de déterminer le niveau de SIL à partir de la connaissance des risques associés au procédé.

2. Méthodes semi quantitatives [2], [9], [10] : La méthode la plus répandue est la matrice de risque. Cette matrice donne le niveau de SIL en fonction de la gravité de risque et de sa fréquence d'occurrence.

3. Méthodes quantitatives [5], [10], [8] : Il s'agit des méthodes qui permettent de calculer le PFD des SIS à partir des probabilités de défaillances 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 aux SIS faiblement sollicités. Par ailleurs, nous utiliserons la méthode des arbres de défaillances qui est basée sur le calcul du PFD du SIS (probabilité d'occurrence de l'événement sommet de l'arbre) à partir des probabilités de défaillances de ses composants (probabilités d'occurrences des événements élémentaires de l'arbre).

III. Détermination du SIL par une approche floue/possibiliste

Pour déterminer le niveau de SIL des SIS, le rapport technique ISA-TR84.00.02-2002 [5] a récemment recommandé l'utilisation de la méthode des arbres de défaillances dans les procédés nécessitant des fonctions de sécurité de SIL 2 ou 3.
L'analyse des arbres de défaillances conventionnelle est basée sur l'approche probabiliste. La probabilité d'occurrence de l'événement sommet (probabilité de défaillance du système complet) est calculée à partir des probabilités d'occurrence des événements élémentaires (probabilités de défaillances des composants du système). Cette méthode a été largement utilisée dans le passé. Cependant, pour les experts, il est souvent difficile d'obtenir une large quantité de données pour déterminer, d'une manière précise, les probabilités de défaillances des composants du système [11]. Ce problème se pose, en particulier, pour les SIS qui sont faiblement sollicités. En effet, ceux-ci présentent des défaillances très rares ne permettant pas d'affecter des valeurs précises aux paramètres de fiabilité de leurs composants. Il est donc nécessaire de proposer d'autres approches pour analyser les arbres de défaillances.
Les premiers travaux d'analyse floue des arbres de défaillances appartiennent à Tanaka et al. [12]. Ces travaux sont basés sur la représentation de la probabilité d'occurrence des événements de base par des nombres flous trapézoïdaux pour calculer la probabilité d'occurrence de l'événement sommet. Singer [13] a analysé les arbres de défaillances en utilisant des nombres flous du type L-R pour faciliter les opérations arithmétiques. Par la suite, Soman et Misra [14] ont proposé une méthode connue sous le nom de l'identité de résolution et basée sur la méthode des α-coupes pour traiter les arbres de défaillances comportant

des événements répétés. Des compléments d'informations sur l'utilisation des arbres de défaillances flous peuvent être trouvés dans [15], [16], [17], [18].

A. Nombres flous

Soit x une variable continue de fonction d'appartenance $\mu(x) \in [0,1]$, et qui satisfait aux conditions suivantes :

- $\mu(x)$ est continue par morceaux ;
- $\mu(x)$ est convexe ;
- $\mu(x)$ est normale (il existe au moins une variable x_0 telle que $\mu(x_0) = 1$).

L'ensemble flou dont la fonction d'appartenance satisfait à ces conditions est appelé nombre flou.
Cependant, les opérations arithmétiques utilisées pour manipuler les nombres flous requièrent beaucoup de ressources. Kaufman et Gupta [19] ont montré que ces efforts de calculs sont largement simplifiés par la décomposition des fonctions d'appartenance des nombres flous en $\alpha-$coupes ($0 \leq \alpha \leq 1$). En effet, si on considère un nombre flou $\widetilde{A}$ de fonction d'appartenance $\mu_{\widetilde{A}}(x)$ (cf. Fig. 2), on peut obtenir plusieurs intervalles en utilisant la méthode des $\alpha-$coupes. $A_L^{(\alpha)}$ et $A_R^{(\alpha)}$ représenteront respectivement les limites droites et gauches de la fonction d'appartenance $\mu_{\widetilde{A}}(x)$ à chaque $\alpha-$coupe.

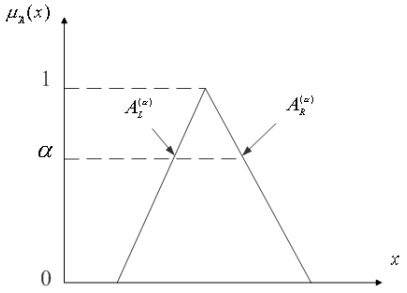

Fig. 2. Décomposition d'un nombre flou en α-coupes

Les opérations arithmétiques appliquées à deux nombres flous $\widetilde{A}$ et $\widetilde{B}$ donnent les expressions suivantes :

$$\widetilde{C} = \widetilde{A} + \widetilde{B} \rightarrow [C_L^{(\alpha)}, C_R^{(\alpha)}] = [A_L^{(\alpha)} + B_L^{(\alpha)}, A_R^{(\alpha)} + B_R^{(\alpha)}]$$

$$\widetilde{C} = \widetilde{A} - \widetilde{B} \rightarrow [C_L^{(\alpha)}, C_R^{(\alpha)}] = [A_L^{(\alpha)} - B_L^{(\alpha)}, A_R^{(\alpha)} - B_R^{(\alpha)}]$$

$\widetilde{C} = \widetilde{A}.\widetilde{B} \rightarrow$
$[C_L^{(\alpha)}, C_R^{(\alpha)}] = [min(A_L^{(\alpha)}.B_L^{(\alpha)}, A_R^{(\alpha)}.B_L^{(\alpha)}, A_L^{(\alpha)}.B_R^{(\alpha)}, A_R^{(\alpha)}.B_R^{(\alpha)}), max(A_L^{(\alpha)}.B_L^{(\alpha)}, A_R^{(\alpha)}.B_L^{(\alpha)}, A_L^{(\alpha)}.B_R^{(\alpha)}, A_R^{(\alpha)}.B_R^{(\alpha)})]$

$$\widetilde{C} = \widetilde{A} \div \widetilde{B} \rightarrow [C_L^{(\alpha)}, C_R^{(\alpha)}] = [A_L^{(\alpha)}, A_R^{(\alpha)}] \times [\tfrac{1}{B_R^{(\alpha)}}, \tfrac{1}{B_L^{(\alpha)}}]$$

Dans cet article, seuls les opérateurs + et . sont utilisés.

B. Probabilités floues

L'analyse des arbres de défaillances conventionnelle est basée sur l'approche probabiliste. Comme les probabilités d'occurrences des événements élémentaires sont incertaines dans notre étude, nous utiliserons des probabilités floues de défaillances au lieu d'utiliser des valeurs de probabilités singulières.

Une probabilité floue est un ensemble flou défini dans l'espace de probabilités. Elle représente un nombre flou entre 0 et 1 qui est affecté à la probabilité d'occurrence d'un événement.

C. Théorie des possibilités

La théorie des possibilités [20] a été développée pour permettre de raisonner sur des connaissances imprécises, en introduisant un moyen de prendre en compte les incertitudes sur ces connaissances. Elle permet de dire dans quelle mesure la réalisation d'un événement est possible et dans quelle mesure elle est certaine.

Une distribution de possibilités $\pi(.)$ définie sur l'ensemble de référence Ω est une application de Ω dans l'intervalle [0,1] :

$$\pi : \Omega \rightarrow [0,1]. \tag{1}$$

Une mesure de possibilités Π peut être induite à partir de la distribution de possibilités $\pi(.)$ par la relation :

$$\pi(x) = \Pi(\{x\}), \tag{2}$$

La mesure de possibilités Π attribue à chaque sous-ensemble A de l'ensemble de référence Ω un réel dans $[0,1]$ évaluant à quel point l'événement A est possible.
Une mesure de possibilités Π donne une information sur l'occurrence d'un événement A relatif à l'ensemble de référence Ω, mais elle ne suffit pas pour décrire l'incertitude existante sur cet événement. Pour compléter l'information sur A, une mesure de nécessité N permet d'indiquer le degré avec lequel la réalisation de A est certaine. N est la grandeur duale de la mesure de possibilités. Cette mesure attribue à tout A un réel dans [0,1]. La nécessité d'un événement correspond à l'impossibilité de l'événement contraire :

$$\forall A \subset \Omega \qquad N(A) = 1 - \Pi(\overline{A}) \tag{3}$$

D. Approche floue/possibiliste

Dans cet article, l'analyse des arbres de défaillances est basée sur la théorie des possibilités. Ainsi, nous allons attribuer un degré d'incertitude à chaque valeur de la probabilité de défaillance d'un composant. La distribution de possibilités de la probabilité de défaillance du SIS est déterminée à partir des distributions de possibilités des probabilités de défaillances des composants du SIS.

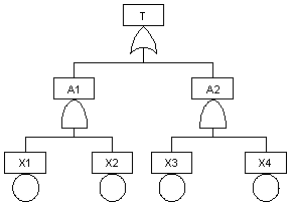

Fig. 3. Arbre de défaillances

Techniquement, l'incertitude des probabilités de défaillance des composants de base est prise en compte en utilisant des probabilités floues de formes triangulaires. Dans l'arbre représenté dans la figure 3, si on suppose que les événements X_i sont indépendants et de probabilités de défaillances très faibles (approximation des événements

rares), alors la distribution de possibilités de la probabilité d'occurrence de l'événement sommet est obtenue par :

$$\pi_{P_T} = \pi_{P_{A_1}} + \pi_{P_{A_2}}$$

avec :

$$\pi_{P_{A_1}} = \pi_{P_{X_1}}.\pi_{P_{X_2}}; \quad \pi_{P_{A_2}} = \pi_{P_{X_3}}.\pi_{P_{X_4}}.$$

où π_{P_T} est la distribution de possibilité de la probabilité de défaillance du système complet et $\pi_{P_{X_i}}$ la distribution de possibilités de la probabilité de défaillance d'un composant i.

E. Facteurs d'importance possibilistes

Les facteurs d'importance ont été principalement introduits dans les études des arbres de défaillances. Ils indiquent la contribution des probabilités de défaillances des composants de base à la probabilité de défaillance du système complet. Birnbaum [21] a défini le facteur d'importance marginal par :

$$B_i(t) = Q(1_i, q(t)) - Q(0_i, q(t)) \tag{4}$$

où $Q(1_i, q(t))$ est l'indisponibilité du système quand le composant i fonctionne et $Q(0_i, q(t))$ l'indisponibilité du système quand le composant i est défaillant. Dans l'approche floue/possibiliste, les indisponibilités $Q(1_i, q(t))$ et $Q(0_i, q(t))$ ne sont plus des valeurs singulières, mais des nombres flous, d'où le besoin d'une nouvelle définition de ces facteurs d'importance.
Pan et Tai [16] ont proposé deux facteurs d'importance basés sur le calcul de la variance des indisponibilités des systèmes et des composants. Les facteurs d'importance flous on été introduit par Furata et Shiraishi [22]. Liang et Wang [23] puis Suresh et al. [15] ont défini des facteurs d'importance basés sur les distances euclidiennes entre les ensembles flous et les nombres flous triangulaires. Dans notre travail, nous nous basons sur la méthode des α-coupes et la théorie des possibilités pour proposer deux nouveaux facteurs d'importance.

Le premier facteur que nous proposons permet d'identifier les composants critiques du système du point de vue de la fiabilité et de la disponibilité. Ainsi, le facteur d'importance possibiliste PIM_i d'un composant i est donné par la relation suivante :

$$PIM_i = defuz(\widetilde{PIM_i}) \tag{5}$$

où $defuz$ est la méthode de défuzzification du centroïd (centre de gravité de la distribution de possibilités) utilisée pour obtenir une valeur singulière à partir de la distribution de possibilités de $\widetilde{PIM_i}$ qui est donnée par :

$$\widetilde{PIM_i} = \pi_P - \pi_{P^i} \tag{6}$$

où π_P est la distribution de possibilités de la probabilité de défaillance du SIS quand le composant i est défaillant et π_{P^i} la distribution de possibilités de la probabilité de défaillance du SIS quand le composant i fonctionne.

Nous proposons aussi, un autre facteur d'incertitude possibiliste PUM_i d'un composant i qui est donné par la relation suivante :

$$PUM_i = defuz(\widetilde{PUM_i}) \tag{7}$$

La distribution de possibilité de $\widetilde{PUM_i}$ est donnée par :

$$\widetilde{PUM_i} = \pi_P - \pi_{P_{i=cts}} \tag{8}$$

où π_P est la distribution de possibilités de la probabilité de défaillance du SIS et $\pi_{P_{i=cts}}$ la distribution de possibilités de la probabilité de défaillance du SIS quand on annule l'incertitude qui entache la probabilité de défaillance du composant i (c'est-à-dire qu'on considère une valeur précise de la probabilité de défaillance de ce composant).
Ce facteur d'incertitude possibiliste permet d'identifier les composants dont l'incertitude de la probabilité de défaillance contribue significativement à l'incertitude entachant la probabilité de défaillance du système complet.

IV. Application

A. Description du système

On considère un système constitué d'un réservoir sous pression contenant un liquide inflammable volatil (cf. Fig. 4). Ce réservoir peut rejeter des gaz dans l'atmosphère.

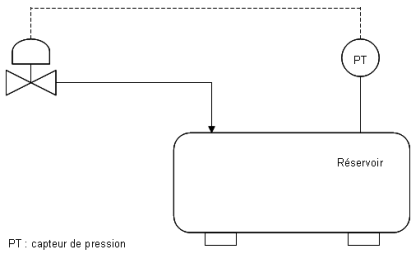

Fig. 4. Réservoir sous pression

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) et qu'une fonction instrumentée de sécurité de niveau SIL2 doit être implémentée dans un SIS pour réduire le taux de rejet du réservoir. Notre objectif est de vérifier si le SIS proposé au concepteur est capable de satisfaire à l'exigence SIL2 requise pour réaliser la fonction instrumentée de sécurité de réduction du rejet des gaz. Le SIS utilisé a été défini dans le document technique ISA-TR84.00.02-2002 [5] (cf. Fig. 5).

La figure 6 représente l'arbre de défaillances du SIS [5] lors de sa sollicitation pour réaliser la fonction de sécurité

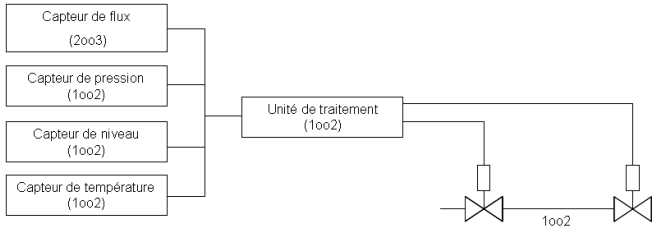

Fig. 5. Configuration du SIS

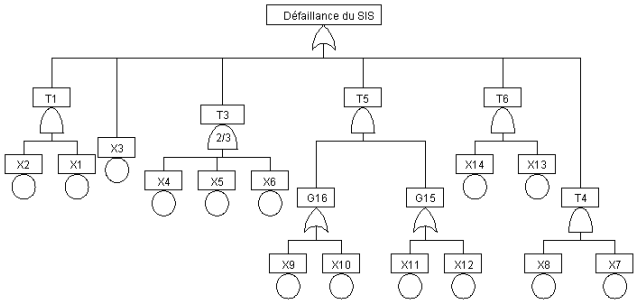

Fig. 6. Arbre de défaillances de l'exemple

Composants du SIS	a_i	m_i	b_i
X1, X2 : Capteurs de pression	0.01	0.032	0.049
X3 : Unité de traitement	0.005	0.006	0.0061
X4, X5, X6 : Capteurs de flux	0.0126	0.017	0.0211
X7, X8 : Capteurs de température	0.0326	0.04	0.0403
X9, X11 : Solénoïdes des vannes	0.01	0.028	0.0311
X10, X12 : Bloc-vannes	0.01	0.028	0.0311
X13, X14 : Capteurs de pression	0.0199	0.0399	0.049

TABLE II
PARAMÈTRES DES DISTRIBUTIONS DE POSSIBILITÉS DES PROBABILITÉS DE DÉFAILLANCES DES COMPOSANTS

demandée. Notre premier objectif est de calculer à partir des distributions de possibilités des événements de base de l'arbre de défaillances (chaque événement de base représente la défaillance d'un composant du SIS), la distribution de possibilités de l'événement sommet qui représente la défaillance du SIS lors de sa sollicitation.

B. Approche floue/possibiliste

Les distributions de possibilités des probabilités de défaillances des composants sont du type triangulaire et caractérisées par 3 paramètres m_i, a_i et b_i (qui sont donnés par les experts), tel que m_i est la valeur modale avec $\pi_{PFD}(m_i) = 1$, a_i est la limite à gauche de m_i et b_i est la limite à droite de m_i. Dans la table II, nous donnons les valeurs de ces 3 paramètres pour chaque composant du SIS. Les composants du système étudié sont non réparables, indépendants et de probabilités de défaillances très faibles.

En utilisant les 6 coupes minimales de l'arbre de défaillances : $\{T_1, T_2, T_3, T_4, T_5, T_6\}$, la distribution de possibilités de la probabilité d'occurrence de l'événement sommet est donnée par :

$$\pi_{PFD_{SIS}} = \pi_{P_{T_1}} + \pi_{P_{T_2}} + \pi_{P_{T_3}} + \pi_{P_{T_4}} + \pi_{P_{T_5}} + \pi_{P_{T_6}}$$

où $\pi_{P_{T_i}}$ est la distribution de possibilités de la probabilité d'occurrence de la coupe minimale i et $\pi_{PFD_{SIS}}$ la distribution de possibilités de la probabilité de défaillance du SIS complet. Les distributions de possibilités des probabilités d'occurrence des coupes minimales sont données par les relations suivantes :

$\pi_{P_{T_1}} = \pi_{P_{X_1}}.\pi_{P_{X_2}}$;
$\pi_{P_{T_2}} = \pi_{P_{X_3}}$;
$\pi_{P_{T_3}} = \pi_{P_{X_4}}.\pi_{P_{X_5}} + \pi_{P_{X_4}}.\pi_{P_{X_6}} + \pi_{P_{X_5}}.\pi_{P_{X_6}}$;
$\pi_{P_{T_4}} = \pi_{P_{X_7}}.\pi_{P_{X_8}}$;
$\pi_{P_{T_5}} = (\pi_{P_{X_9}} + \pi_{P_{X_{10}}}).(\pi_{P_{X_{11}}} + \pi_{P_{X_{12}}})$;
$\pi_{P_{T_6}} = \pi_{P_{X_{13}}}.\pi_{P_{X_{14}}}$.

où $\pi_{P_{X_i}}$ est la distribution de possibilités de la probabilité d'occurrence de l'événement i.
En utilisant la méthode des $\alpha-$coupes et les opérations arithmétiques définies précédemment, on détermine la distribution de possibilités de la probabilité d'occurrence de l'événement sommet (distribution de possibilités de la probabilité de défaillance du SIS) à partir des distributions de possibilités des probabilités de défaillances des composants.

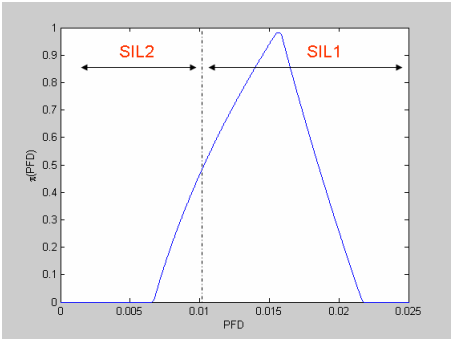

Fig. 7. Distribution de possibilité du PFD du SIS

La Figure 7 donne la distribution de possibilités de la probabilité d'occurrence de l'événement sommet. Cette probabilité de défaillance varie de $7.4 * 10^{-3}$ jusqu'à $2.21 * 10^{-2}$, ce qui donne pour le SIS étudié un niveau de SIL1 ($PFD \in [10^{-2}, 10^{-1}]$) ou un niveau SIL2 ($PFD \in [10^{-3}, 10^{-2}]$) selon la Table I. On remarque qu'il existe une incertitude concernant le niveau de SIL du SIS (1 ou 2), c'est pourquoi nous proposons d'utiliser des facteurs d'importance possibilistes pour essayer de réduire cette incertitude.

C. Facteur d'importance possibiliste (PIM)

Les résultats du calcul des facteurs d'importance possibilistes (PIM) des composants du SIS sont donnés dans la table III. Nous notons que le composant le plus important est l'unité de traitement avec un facteur de 0.99. Cela signifie que l'unité de traitement est le composant le plus critique pour la fiabilité et l'indisponibilité du SIS. Pour réduire l'incertitude qui entache le niveau de SIL obtenu, nous supprimons l'incertitude qui entache la probabilité de défaillance de l'unité de traitement en considérant que cette probabilité est précise. La figure 8 représente la distribution de possibilités de la probabilité de défaillance du SIS avant (courbe en trait plein) et après la suppression de l'incertitude de la probabilité de défaillance de l'unité de traitement (courbe tiretée). Nous remarquons que l'incertitude qui entache le niveau de SIL n'a pratiquement pas été réduite. Dans la situation matérialisée par notre exemple, le PIM n'est donc pas l'indicateur le plus significatif pour la réduction de l'incertitude sur le niveau de SIL lorsque l'on ajuste la précision de la probabilité de défaillance du composant le plus critique. Toutefois, ce facteur d'importance

permet d'évaluer la contribution d'un composant dans la probabilité de défaillance du SIS. Il est donc possible de contribuer à la réduction de l'incertitude sur la probabilité de défaillance du SIS en modifiant la valeur modale de la distribution de possibilités du composant le plus critique (courbe en tiretée-pointillée) qui est l'unité de traitement, mais cela suppose le changement des composants utilisés. Un second facteur d'importance possibiliste peut nous aider dans la réduction de l'incertitude.

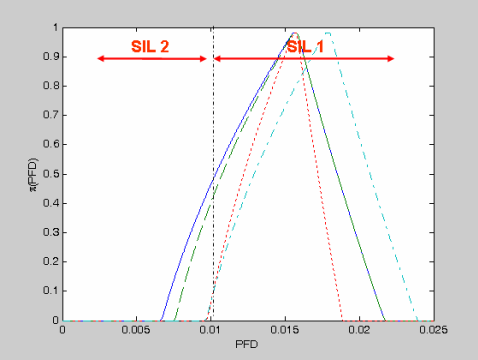

Fig. 8. Distributions de possibilités du PFD du SIS selon les modifications

Composants du SIS	PIM	Rang
Capteur de pression	0.035	7
Unité de traitement	0.992	1
Capteur de flux	0.038	6
Capteur de température	0.042	3
Solénoïde des vannes	0.042	3
Bloc-vannes	0.042	3
Capteur de niveau	0.082	2

TABLE III
FACTEUR D'IMPORTANCE POSSIBILISTE (PIM)

D. Facteur d'incertitude possibiliste (PUM)

La table IV donne les résultats du calcul des facteurs d'incertitude possibilistes (PUM) des composants du SIS. Nous notons que le classement des composants du SIS n'est plus le même. Le composant le plus important est le capteur de température avec un facteur de 0.045. Pour réduire l'incertitude qui entache le niveau de SIL, nous proposons de supprimer l'incertitude qui entache la probabilité de défaillance du capteur de température. Sur la figure 8, la distribution de possibilités de la probabilité de défaillance du SIS après la suppression de l'incertitude sur la probabilité de défaillance du capteur de température est indiquée en pointillés. Nous remarquons que l'incertitude qui entache le niveau de SIL a été pratiquement éliminée. Ainsi, nous sommes presque sûr que le niveau de SIL du SIS est 1. Dans notre cas, nous concluons que pour réduire l'incertitude du niveau de SIL sans changer de composants, le facteur d'incertitude possibiliste est le plus efficace.

V. CONCLUSION

Dans cet article, nous avons proposé une approche floue/possibiliste basée sur l'utilisation de distributions de possibilités pour représenter l'incertitude des probabilités de défaillances des composants des SIS et la méthode des α-coupes, afin de déterminer le niveau de SIL des SIS. Ainsi, nous avons obtenu une distribution de possibilités de la probabilité de défaillance sur demande du SIS, qui a mis en évidence l'existence d'incertitudes concernant le niveau de SIL de ce SIS.

Composants du SIS	PUM	Rang
Capteur de pression	0.038	5
Unité de traitement	0.039	2
Capteur de flux	0.006	7
Capteur de temperature	0.045	1
Solénoide des vannes	0.039	2
Bloc-vannes	0.039	2
Capteur de niveau	0.039	2

TABLE IV
FACTEUR D'INCERTITUDE POSSIBILISTE (PUM)

Par ailleurs, l'introduction de nouveaux facteurs d'importance possibilistes et en particulier le facteur d'incertitude possibiliste a permis d'identifier les composants dont l'incertitude de la probabilité de défaillance contribue significativement à l'incertitude entachant la probabilité de défaillance du SIS, et donc de son niveau de SIL. Ces deux facteurs sont d'un grand intérêt pour aider le fiabiliste à réduire efficacement l'incertitude sur la détermination du SIL d'un SIS. Le facteur PIM permet d'évaluer l'importance de la contribution de chaque composant sur le niveau de SIL du système. Il permet au fiabiliste de rechercher l'amélioration du niveau de SIL et de son incertitude par la modification de la valeur modale de la distribution de possibilités de la probabilité de défaillance du composant le plus critique. Le facteur PUM apporte un second point de vue sur la contribution des composants à l'incertitude sur la probabilité de défaillance du SIS. Ce nouveau facteur guide le fiabiliste dans la réduction de l'incertitude sur la probabilité de défaillance par la réduction de l'incertitude sur la probabilité de défaillance des composants. Par les deux facteurs proposés dans cet article, nous avons apporté une aide à la décision aux fiabilistes, pour réduire d'une manière efficace les incertitudes dans la détermination des SIL.

Les perspectives de ce travail consisteront à intégrer dans la méthode d'aide à la décision que nous avons proposé, l'aspect de la maintenance et du coût des composants des SIS, ainsi qu'une comparaison des résultats obtenus avec ceux obtenus par une approche probabiliste classique.

RÉFÉRENCES

[1] ANSI/ISA-S84.01-1996. *Application of Safety Instrumented Systems for the process control industry.* Instrumentation Society of America (ISA), 1996.

[2] IEC61508. *Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety related systems.* International Electrotechnical Commission (IEC), 1998.

[3] M. Sallak, J-F. Aubry, and C. Simon. Evaluating safety integrity level in presence of uncertainty. In *Journal of KonBin*, volume 1, pages 411–419, Krakow, Poland, 2006. International Conference on Safety and Reliability.

[4] IEC61511. *Functional safety : Safety Instrumented Systems for the process industry sector.* International Electrotechnical Commission (IEC), 2000.

[5] ISA-TR84.00.02-2002. *Safety Instrumented Fonctions (SIF), Safety Integrity Level (SIL), Evaluation Techniques*. Instrumentation Society of America (ISA), 2002.

[6] A. E. Summers. Viewpoint on ISA TR84.0.02 : simplified methods and fault tree analysis. *ISA Transactions*, 39 :125–131, 2002.

[7] L. Beckman. Expanding the applicability of ISA TR84.02 in the field. *ISA Transactions*, 39 :357–361, 2000.

[8] P. Stavrianidis and K. Bhimavarapu. Safety Instrumented Functions and Safety Integrity Levels (SIL). *ISA Transactions*, 37 :337–351, 1998.

[9] C. Simon, M. Sallak, and J-F. Aubry. Allocation de sil par agrégation d'avis d'experts. Lille, France, 2006. 15ème Colloque National de Maîtrise des Risques et Sûreté de Fonctionnement, Lambda-mu 15.

[10] K. Bhimavarapu, L. Moore, and P. Stavrianidis. Performance based safety standards : an integrated risk assessment program. *ISA TECH*, 1, 1997.

[11] M. Sallak, J-F. Aubry, and C. Simon. Impact de l'imprécision des taux de défaillances dans les arbres de défaillances et facteurs d'importance flous. Lyon, France, 2005. Journées Doctorales Modélisation, Analyse et Conduite des Systèmes dynamiques, JDMACS 2005.

[12] H. Tanaka, L. T. Fan, F. S. Lai, and K. Toguchi. Fault tree analysis by fuzzy probability. *IEEE Transactions on Reliability*, 32 :453–457, 1983.

[13] D. Singer. A fuzzy set approach to fault tree and reliability analysis. *Fuzzy Sets and Systems*, 34 :145–155, 1990.

[14] K.P. Soman and K.B. Misra. Fuzzy fault tree analysis using resolution identity. *1*, page 193, 1993.

[15] P.V. Suresh, A.K. Babar, and V. Venkat Raj. Uncertainty in fault tree analysis : a fuzzy approach. *Fuzzy Sets and Systems*, 83 :205–213, 1996.

[16] Z. J. Pan and Y. C. Tai. Variance importance of system components by Monte Carlo. *IEEE Transactions on Reliability*, 37 :521–523, 1988.

[17] Hong Zhong Huang, Xin Tong, and Ming J. Zuo. Posbist fault tree analysis of coherent systems. *Reliability Engineering and System Safety*, 84 :141–148, 2004.

[18] J. Feng and M.D. Wu. The profust fault tree and its analysis. *Journal of National University of Defense Technology*, 23 :85–88, 2001.

[19] A. Kaufman and M. M. Gupta. *Introduction to Fuzzy Arithmetic Theory and Application*. Van Nostrand Reinhold Company, New York, 1991.

[20] D. Dubois and H. Prade. Possibility theory. an approach to computerized processing of uncertainty. *Plenum Press*, 1988.

[21] Z. W. Birnbaum. On the importance of different components in a multicomponent system. In *Multivariate Analysis II*. P. R. Krishnaiah, Ed, N. Y :Academic, 1969.

[22] H. Furuta and N. Shiraishi. Fuzzy importance in fault tree analysis. *Fuzzy Sets and Systems*, 12 :205–213, 1984.

[23] G.S. Liang and M.J.J. Wang. Fuzzy fault tree analysis using failure possibility. *Microelectronics and Reliability*, 33 :583–597, 1993.