Sécurité 4.0: Eléments d'évaluation dynamique quantitative des risques des procédés

André Laurent

Sécurité 4.0: Eléments d'évaluation dynamique quantitative des risques des procédés

André LAURENT
Université de Lorraine,
CNRS, Laboratoire Réactions et Génie des Procédés, UMR 7242,
ENSIC, 1, rue Grandville BP 20451 F 54001 Nancy Cedex, France

Résumé

L'évaluation des risques industriels implique d'utiliser une ou plusieurs méthodes quantitatives d'analyse des risques. Ces méthodes conventionnelles s'appliquent essentiellement à des situations statiques de fonctionnement des procédés. Dans le nouvel environnement des technologies 4.0, la prise en compte de la dynamique des systèmes, en conjonction avec l'importante émergence des flux de nouvelles données, est nécessaire. Ce document propose d'examiner l'apport de la simulation, des réseaux bayésiens et de la logique floue à la complétude dynamique des méthodes. Des exemples d'illustration sont présentés et discutés pour les méthodes respectives HAZOP, de l'arbre des défaillances, de l'arbre des événements, du graphe du nœud papillon et LOPA.

Abstract

Industrial process risk assessment involves the use of one or more quantitative risk analysis methods. These conventional methods are essentially applied to static process operating situations. In the new environment of 4.0 technologies, system dynamics need to be taken into consideration, in conjunction with the significant emergence of new data flows. This paper examines the contribution of simulation, Bayesian networks and fuzzy logic to the dynamic completeness of risk assessment methods. Illustrative examples are presented and discussed for the respective methods HAZOP, fault tree, event tree, bow-tie graph and LOPA.

Avertissement
Les éléments d'évaluation dynamique décrits dans ce document sont essentiellement basés sur la simulation dynamique, les réseaux bayésiens et la logique floue. Chaque exemple illustratif traité d'amélioration d'une méthode d'analyse des risques peut être lu séparément, les notions minimales théoriques ayant été systématiquement rappelées.

Citation
La retraite n'efface ni les compétences, ni les savoirs, qui peuvent continuer à être partagés et transmis. (Claude Halmos)

Table des matières

Introduction

Le premier retour d'expérience de l'impact des technologies de l'industrie du futur, en particulier celles pour la communication, l'interconnexion et la gestion des données, montre l'incidence de leurs potentialités sur l'évaluation de la sécurité 4.0.
Par exemple, Khan et al. [2021] ont illustré sur la figure 1 la chronologie de l'évolution croissante du nombre de paramètres des procédés industriels suivant la nature du procédé, depuis l'ère du procédé discontinu à celle du procédé numérisé. Chaque petit cercle au sein d'un grand cercle matérialise schématiquement le nombre relatif de paramètres en fonction de chaque période observée.

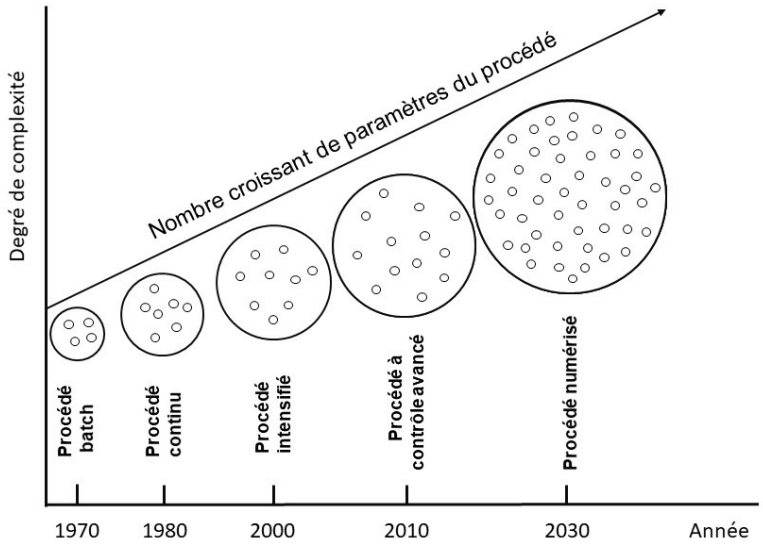

Figure 1: Chronologie de l'évolution des procédés industriels - d'après Khan et al. [2021].

Le développement des divers capteurs, des instruments de surveillance et des systèmes automatisés a ainsi permis de recueillir de nombreuses données de fonctionnement des procédés. L'Internet des objets (IoT) et l'Internet Industriel des objets (IIoT) ont founi les moyens de connecter ces données. Selon Bai et al. [2022] les diverses informations obtenues et listées dans

le cas d'une unité de procédé chimique offrent entre autres une perspective pour le processus d'évaluation des risques:

- Données des procédés - le procédé chimique est généralement équipé de systèmes de contrôle distribués (DCS, SCADA), afin d'améliorer le contrôle de la qualité et de la sécurité. Par conséquent, le coût d'acquisition des données a considérablement diminué et les données du procédé peuvent être consultées facilement et à peu de frais à partir des systèmes DSC et SCADA;

- Données des alarmes - pour la même raison, il est devenu plus pragmatique de définir et d'installer des alarmes pour certaines variables de surveillance importantes. Les données d'alarme sont un ensemble de données du fonctionnement anormal du procédé, qui constituent une forme condensée de données et sont donc devenues un indicateur important lors de l'évaluation des risques;

- Données expérimentales de la recherche - un nombre croissant d'institutions commencent à rendre publiques les données brutes issues de la recherche ; l'acquisition de données expérimentales pour l'analyse des risques devient pratiquement réalisable;

- Données opérationnelles - en cas de changements importants dans les conditions du procédé ou de scénarios inattendus, des actions manuelles peuvent remplacer les actions automatisées; leurs résultats sont également enregistrés dans des journaux de suivi et utilisés comme informations pour répondre à des scénarios anormaux;

- Banque d'images - avec la création de bases de données partagées, les ensembles de données d'images pour la reconnaissance d'images et l'inspection sont de plus en plus utilisés dans les scénarios industriels. En règle générale, chaque grande usine dispose de dix à cent caméras et la quantité de données collectées par ces caméras est considérable;

- Vidéo données - pour surveiller le fonctionnement des usines et des machines et suivre les opérateurs en temps réel, des équipements de surveillance par vidéo sont déployés dans toutes les usines chimiques. Par exemple, la reconnaissance des casques des opérateurs et la surveillance des flammes sur la base de vidéos capturées en direct sont progressivement utilisées dans divers scénarios de production. Une plus grande précision peut être obtenue car chaque image de la vidéo contient en fait des données temporelles;

- Données des détecteurs de gaz - différents détecteurs de gaz inflammables et toxiques sont aujourd'hui disponibles sur le marché. Ces détecteurs de gaz sont utilisés dans les laboratoires et les usines chimiques pour protéger le personnel et les équipements. Les données collectées par ces capteurs peuvent être accessibles via l'IoT et utilisées pour modéliser et évaluer les conditions de fuite de gaz;

- Banque de textes - de nombreuses données textuelles sont disponibles dans les journaux d'usine et les documents relatifs à la sécurité des usines chimiques, tels que les rapports d'analyse des risques, les rapports d'accidents historiques et les rapports sur les accidents

évités de justesse. Ces données ne sont pas encore très structurées, mais peuvent être utilisées pour obtenir des informations utiles à l'évaluation des risques à l'aide du traitement de langage naturel (NLP);

- Banque de données chimiques - les bases de données chimiques actuellement utilisées stockent un grand nombre de paramètres relatifs aux propriétés des substances toxiques et à risque. L'extraction et la modélisation de ces paramètres permettent d'évaluer correctement les risques liés aux systèmes chimiques;

- Répertoire de données de simulation - lors de la conception d'une usine chimique, des logiciel gratuits ou commerciaux sont utilisés pour prendre en compte et simuler les procédés de l'usine. Les données de simulation et les données expérimentales d' extrapolation peuvent ensuite être utilisées pour faciliter l'évaluation ultérieure de la sécurité. Avec le développement de la réalité virtuelle et des technologies de jumeaux numériques, la disponibilité des données de simulation s'est progressivement accrue;

- Banque d'audio signaux et de vibration - en fonctionnement normal ou défectueux, les équipements émettent des signaux audio caractéristiques et en particulier lors de vibrations directes. En conséquence, ces données temporelles du signal audio peuvent être analysées à l'aide d'algorithmes spécifiques pour déterminer rapidement les modes de défaillance de l'équipement, les classer et les corriger instantanément.

L'ensemble de ces données devrait pouvoir être utilisé pour améliorer le processus de production, l' évaluation des risques, les interfaces opérateur 4.0, les systèmes de contrôle de la sécurité, les barrières de sécurité, les systèmes de gestion des alarmes, les signaux d'alerte précoce, la surveillance de la corrosion, la télédétection, la connectivité accrue, l'application de modèles prédictifs reposant sur des données en temps réel et sur l'apprentissage automatique etc.
L'objectif de ce document est de privilégier l'approche de l'évaluation des risques d'un procédé dans le contexte de la sécurité 4.0 de l'usine du futur. Il est nécessaire de prendre simultanément en compte les installations traditionnelles et les nouvelles installations, qui résultent du déploiement des techniques numériques, comme par exemple dans les équipements microstructurés.
Amin et al. [2019] ont identifié dans une compilation bibliographique les principaux outils utilisés pour la sécurité des procédés et l'analyse des risques. Ils ont observé la présence de deux segments principaux de méthodes:

- le premier comprend les réseaux bayésiens (BN), les réseaux bayésiens dynamiques (DBN), l' analyse de l'arbre des défaillances (FTA), l'analyse de l'arbre des événements (ETA) et le nœud papillon (BT);

- le second comporte des études de danger et d'exploitabilité (HAZOP). les systèmes experts liés à HAZOP et l'analyse des couches de protection (LOPA).

Ces méthodes regroupent des techniques qualitatives et quantitatives, dont les plus utilisées sont les outils HAZOP, FTA, ETA, BN, BT, Petri-net (PN), Analyse hiérarchique des procédés

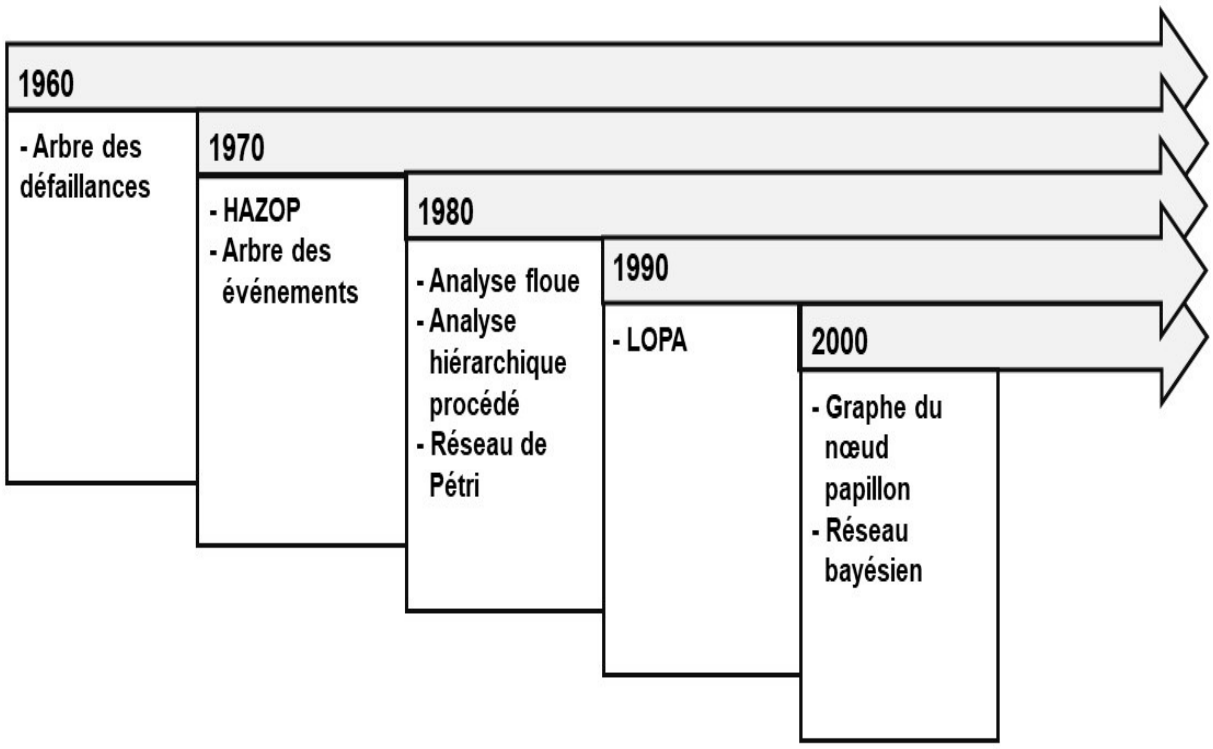

Figure 2: Evolution temporelle des principales méthodes d'analyse de la sécurité des procédés - adapté d'après Amin et al. [2019].

(AHP) et la théorie de la logique floue (FT). La figure 2 traduit l'évolution temporelle entre 1960 et 2000 des principales méthodes d'analyse de la sécurité des procédés, où les présences du graphe du nœud papillon et du réseau bayésien sont considérées comme récentes. Amin et al. [2019] ont aussi rapporté trois classes de fréquence d'utilisation des outils:

- Très fréquents = FTA, HAZOP et FT;
- Modérément fréquents = BN, AHP, et ETA;
- Moins fréquents = LOPA, PN et BT.

La littérature rapporte par ailleurs pratiquement plusieurs inventaires détaillés des méthodes et techniques classique d'analyse et d'évaluation des risques ([Debray, 2006], [Laurent, 2011], [Khan et al., 2015] et [Adriaensen et al., 2019]. La méthode HAZOP, les méthodes des arbres, le graphe du noeud papillon et la méthode LOPA sont traditionnellement utilisées dans l'application des bonnes pratiques d'évaluation qualitative, semi-quantitative et quantitative. Ces méthodes conventionnelles présentent cependant des limitations. Elles s'appliquent à une situation statique de fonctionnement et ne parviennent pas à saisir la variation du risque qui se produit lors de l'évolution du procédé et de son environnement. Elles ne sont pas en mesure de prendre en compte les variations des variables, les causes communes de défaillance et la

dépendance conditionnelle entre les événements contribuant à un accident ou plus globalement d'introduire de nouvelles informations et preuves. En outre, les événements primaires et les barrières de sécurité sont supposés indépendants entre eux. Elles considèrent aussi les relations entre les événements comme étant principalement binaires et ne tiennent pas compte des dépendances entre les facteurs contributifs. Elles ne sont pas non plus en mesure d'utiliser les informations sur les précurseurs d'accidents pour réviser les profils de risque. Enfin, les estimations probabilistes sont souvent encore basées sur des données obtenues au fil des années, qui peuvent introduire une certaine incertitude dans l'analyse. En bref, cette approche statique ne correspond plus à la réalité.

Pour faire face aux risques dans un environnement changeant et surmonter les limites de ces méthodes traditionnelles, la prise en compte de la dynamique des risques, en conjonction avec des informations récentes et précises, dans ces méthodes d'évaluation est donc maintenant une nécessité, afin de sensibiliser les opérateurs 4.0 et les différentes parties prenantes aux exigences de la sécurité 4.0 des procédés [Qian et al., 2023].

Chapitre 1

Approche dynamique de la méthode HAZOP

Khan et al. [2015] ont rapporté les diverses utilisations potentielles de la méthode HAZOP en analyse qualitative, en analyse semi-quantitative, en analyse hybride intégrée couplée, par exemple avec la méthode d'Analyse des Modes de Défaillances, de leurs Effets et de la Criticité (AMDEC) et en analyse automatisée avec des systèmes experts dans l'évaluation des risques. Baybutt [2015] a relevé et discuté les inconvénients et faiblesses de la méthode HAZOP. Parmi les huit catégories distinctes recensées les principaux inconvénients sont:

- l'omission possible d'un événement non documenté, de certains dangers et problèmes opératoires;
- le temps de mise en œuvre de la méthode, son coût et la mobilisation d'experts confirmés;
- la seule prise en compte de scénario à simple déviation, avec omission des dérives multiples simultanées;
- la non prise en compte des tentatives de rattrapage des opérateurs lors des dérives opératoires.

L'objectif de cette partie est de proposer des exemples d'intégration de la simulation dynamique d'un procédé avec la mise en œuvre de la méthode HAZOP, afin de montrer les capacités de la méthode dynamique quantitative HAZOP.

1.1 La méthode HAZOP conventionnelle

Le premier objectif de la méthode HAZOP est l'analyse de l'intégrité opérationnelle d'un système par l'identification systématique et la détermination des causes et des conséquences des déviations susceptibles de survenir au cours de l'exploitation des installations (marche nominale de routine ; phases transitoires de démarrage et d'arrêt; opérations d'entretien et de maintenance). Les atteintes à cette intégrité opérationnelle d'un système peuvent aussi générer une

ou des situations présentant des risques, dont la nécessaire identification préalable constitue le second objectif de la méthode HAZOP. Les objectifs de la méthode HAZOP sont limités à l'identification des problèmes potentiels, sans tenter explicitement leur résolution. Les conclusions de l'analyse des risques effectuée par la méthode HAZOP sont communiquées à la conception, à l'ingénierie, à l'assistance procédé et à l'exploitation, dont la mission est de proposer des solutions acceptables aux problèmes recensés.
Le principe de la méthode HAZOP consiste d'abord à décrire le fonctionnement des différentes phases d'un procédé de façon détaillée en le décomposant en une suite d'opérations élémentaires à l'aide des schémas détaillés de l'installation. Ensuite le recensement des divers types d'écarts ou de déviations possibles des paramètres de l'installation est effectué à l'aide d'une liste de mots-clefs ou de mots-guides. Chaque mot-clef qualifie donc un type d'écart, dont les causes sont identifiées et les conséquences examinées. La référence systématique à un mot-clef traduit l'équivalence de la perte de fonction potentielle de l'opération élémentaire, ou du sous-système ou du système. L'analyse déductive appliquée permet donc de recenser les défaillances, alors que l'analyse inductive conduit à recenser les effets.
L'ensemble de cette analyse est traduite par la réalisation de tableaux où sont indiquées les causes possibles des dérives, leurs conséquences et les actions requises ou les modifications techniques nécessaires pour assurer le bon fonctionnement et/ou la sécurité et la sûreté du système. Il faut remarquer que certains écarts peuvent entraîner des effets sur la production sans générer systématiquement les conséquences néfastes des risques sur le fonctionnement de l'installation. Enfin les déviations potentiellement dangereuses sont hiérarchisées pour déterminer les actions à mettre en oeuvre.
En résumé, la méthode HAZOP est fondée sur le principe systématique suivant:

- choisir un paramètre de fonctionnement,
- générer une dérive de ce paramètre à l'aide d'une liste de mots clefs,
- rechercher les causes possibles de la dérive étudiée,
- déterminer les conséquences éventuelles associées à cette dérive,
- vérifier en cas de risques la présence ou l'existence de systèmes de correction, de prévention, de protection ou de mitigation, sinon les définir.

L'organisation et la mise en œuvre de la méthode HAZOP sont détaillées dans le chapitre 12 du livre "Sécurité des procédés chimiques" [Laurent, 2011].

1.2 Exemple d'une réaction exothermique dans un réacteur semi-fermé

Il est proposé de présenter la méthodologie d'analyse des risques d'une réaction exothermique mise en œuvre dans un réacteur semi-fermé. Elle s'appuie sur la simulation dynamique, afin de décrire la cinétique et de quantifier les effets des phénomènes dangereux identifiés par la méthode HAZOP.

1.2.1 Méthodologie

La figure 1.1 illustre les quatre étapes de la méthodologie proposée par Berdouzi et al. [2018]:

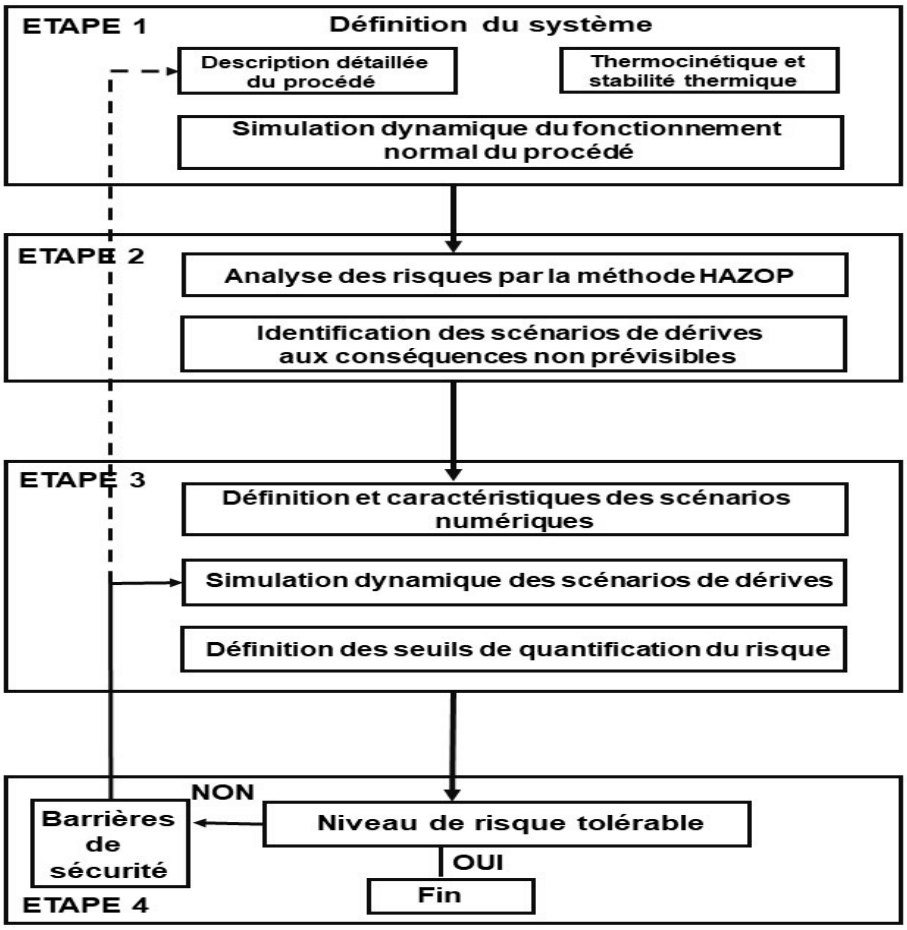

Figure 1.1: Les étapes de la méthodologie - adapté d'après Berdouzi et al. [2018].

- Etape 1 - définition du système - opérations unitaires - conditions opératoires - thermocinétique - stabilité thermique - modèles thermodynamique et thermique - régulation;
- Etape 2 - analyse des risques par la méthode HAZOP - scénarios de dérives, en particulier ceux aux conséquences partiellement prévisibles ou inconnues et ceux aux dérives simultanées ou consécutives;
- Etape 3 - définition et caractéristiques des scénarios numériques;
- Etape 4 - quantification des risques et influence des performances des mesures de maîtrise des risques.

1.2.2 Description du procédé

1.2.2.1 Description de la réaction

La réaction mise en œuvre est l'oxydation d'une solution aqueuse de thiosulfate de sodium par le peroxyde d'hydrogène conduisant à la formation de trithionate de sodium, de sulfate de sodium et d'eau suivant le schéma réactionnel:

$$2Na_2S_2O_3 + 4H_2O_2 \longrightarrow Na_2S_3O_6 + Na_2SO_4 + 4H_2O \tag{1.1}$$

Cette réaction d'oxydo-réduction est irréversile, très rapide et fortement exothermique. La cinétique réactionnelle, qui est supposée d'ordre un pour chacun des réactifs, est décrite par l'équation:

$$r = k[Na_2S_2O_3][H_2O_2] \tag{1.2}$$

où r est la vitesse de réaction et k la constante de vitesse exprimée par la relation:

$$k = k_0 \exp[\frac{-E_A}{RT}] \qquad \text{avec } k_0 = 2 \times 10^7\, m^3\, mol^{-1}\, s^{-1} \text{ et } E_A = 6,82 \times 10^4\, J\, mol^{-1} \tag{1.3}$$

1.2.2.2 Description du réacteur semi-fermé

La réaction est mise en œuvre dans un réacteur semi fermé de 100 L de volume avec un taux de remplissage par charge de 80% fonctionnant à la pression atmosphérique. La figure 1.2 représente le schéma instrumenté du réacteur.

La configuration du réacteur semi-fermé comporte:

- l'alimentation en solution aqueuse de thiosulfate via la vanne VLV1;
- la coulée du peroxyde d'hydrogène via la vanne VLV2;
- l'entrée d'azote via la vanne VLV3:
- le débit de sortie du produit via la vanne VLV5;
- les régulateurs de température TC1 et TC2, équipés des blocs retards, régulant respectivement la température pendant la phase de réaction et la phase de chauffage;
- le régulateur de pression PC du réacteur et la vanne de régulation VLV4 relarguant à l'évent;
- la soupape de sécurité PSV (barrière de sécurité).

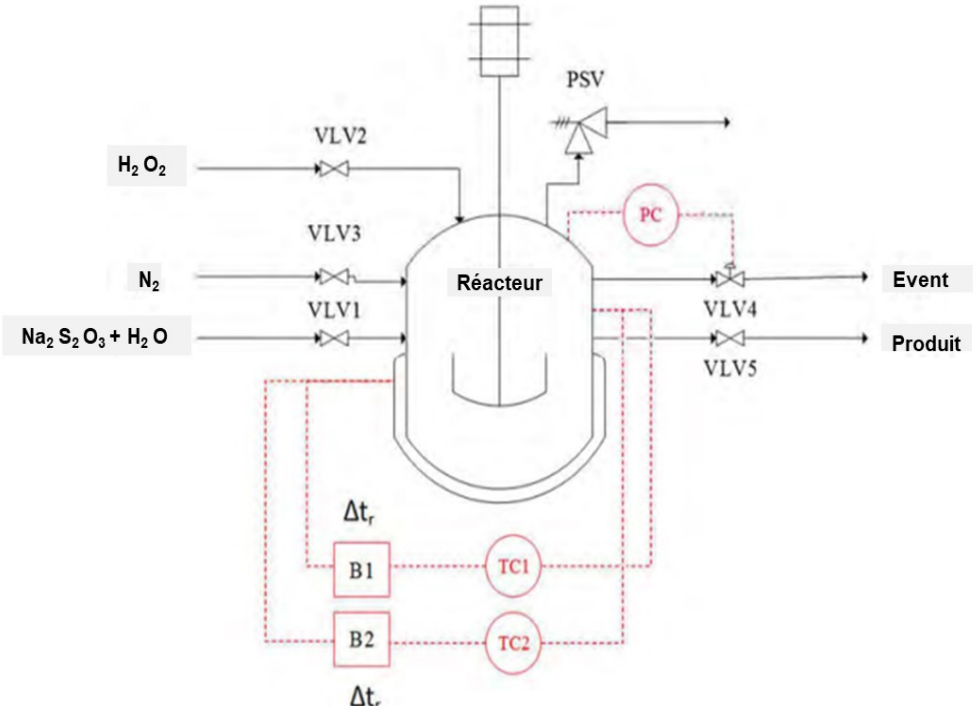

Figure 1.2: Schéma instrumenté du réacteur semi-fermé - adapté d'après Berdouzi et al. [2018].

1.2.2.3 Description du protocole expérimental

Le protocole opératoire du procédé en conditions normales de fonctionnement, indiqué sur la figure 1.3, est composé de quatre étapes:

- l'alimentation de la solution aqueuse de thiosulfate de sodium à 293 K pendant 20 minutes;
- le préchauffage du milieu de 293 K à 333 K pendant 28 minutes;
- la coulée du peroxyde d'hydrogène à 333 K pendant 60 minutes;
- l'étape de réaction, qui débute à la coulée et dure 156 minutes jusqu'à obtention d'un taux de conversion du thiosulfate de 90%.

1.2.3 Simulation dynamique du procédé en fonctionnement normal

L'examen des évolutions expérimentales respectives dans le réacteur semi-fermé de la température, des quantités molaires de matière (thiosulfate de sodium - peroxyde d'hydrogène - sulfate de sodium), des variations de pression et du débit d'évacuation de la soupape de sécurité permet de comparer et de valider les résultats de la simulation avec des écarts relatifs inférieurs à 10% en fonctionnement normal.

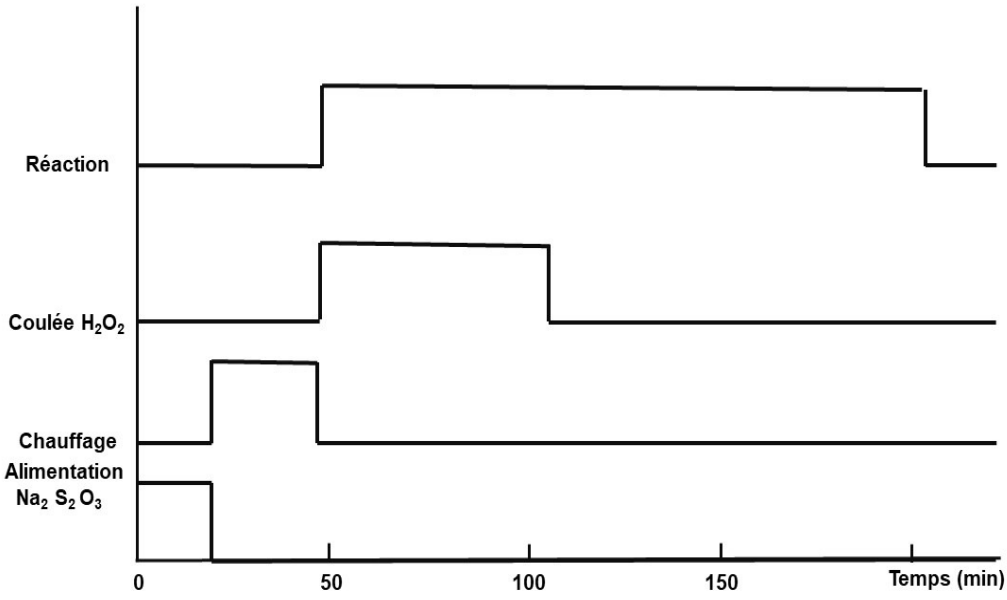

Figure 1.3: Chronogramme du protocole expérimental - adapté d'après Berdouzi et al. [2018].

1.2.4 Analyse HAZOP du réacteur semi-fermé

L'analyse HAZOP réalisée sur le procédé étudié dans le réacteur semi-fermé a permis de recenser 24 potentialités de cas de dérives. Les paramètres examinés sont le refroidissement, la température, la pression, le niveau, les concentrations, les quantités alimentées et coulées, la contamination du peroxyde d'hydrogène et l'inversion des réactifs. Cette analyse a permis de faire ressortir des scénarios dont les conséquences sont difficilement prévisibles laissant des interrogations par rapport à l'évaluation de leurs occurrences ou de leurs amplitudes.
Le tableau 1.1 présente ainsi un nombre plus limité de scénarios numériques retenus pour la simulation avec leurs causes et conséquences hypothétiques.
De même en raison de certaines autres limites de la méthode HAZOP, Berdouzi et al. [2018] ont aussi considéré quelques scénarios plus complexes comportant des dérives consécutives ou simultanées, dont les descriptifs sont les suivants:

- Scénario S9 - plus de température dû à la perte de refroidissement au début de la coulée (t=48 min) et soupape PSV sous dimensionnée;
- Scénario S10 - plus de température dû à la perte de refroidissement au début de la coulée (t=48 min) et soupape PSV bloquée (ouverture incomplète);
- Scénario S11 - plus de refroidissement dû à une erreur procédurale d'un opérateur lors de

Dérives	Causes	Conséquences hypothétiques	Scénario numérique
Pas de refroidissement	Pas d'eau de refroidissement	emballement ?	S1
	Canalisation d'eau de refroidissement bouchée	emballement ?	S1
	Vanne de régulation de débit d'eau de refroidissement fermée	emballement ?	S1
	Rupture guillotine de la canalisation d'eau	emballement ?	S1
	Gel des canalisations d'eau de de refroidissement	emballement ?	S1
Moins de refroidissement	Erreur opérateur sur la température de consigne supérieure du régulateur	emballement ?	S2 S3 S4
Plus de refroidissement	Erreur opérateur sur la température de consigne inférieure du régulateur	effet si la température revient à la consigne ?	S5
Plus de concentration $[H_2O_2]$	Erreur opérateur sur la préparation de la solution	valeur taux de conversion ? décomposition ?	S6 S7
Qualité dégradée de produit	Réactif H_2O_2 contaminé	emballement ? décomposition ? vitesse réaction ? valeur taux de conversion ?	S8

Tableau 1.1: Récapitulatif des scénarios numériques pour la simulation dynamique - d'après Berdouzi et al. [2018].

la définition de la température de consigne (t=48 min) et la température revient à la valeur des conditions opératoires normales de 333 K à la fin de l'étape de coulée (t=108 min);

- Scénario S12 - plus de concentration en réactif H_2O_2 (réactif pur) et contamination du réactif peroxyde d'hydrogène.

1.2.5 Exemples de simulation des scénarios de dérives

La simulation dynamique permet d'acquérir a priori l'évolution des différentes variables du procédé du réacteur semi-fermé. Afin de comparer et de hiérarchiser les scénarios examinés pour les dérives retenues, il est préalablement nécessaire de définir des valeurs seuils et des intervalles d'acceptabilité pour quantifier classiquement les risques en termes de probabilité et de gravité. Habituellement, en démarche d'application de la maîtrise des risques, lorsqu'une dérive survient, elle peut conduire à une évolution du paramètre concerné telle que ce dernier franchisse plusieurs seuils et traverse plusieurs zones ou plages successives respectives comme l'intervalle de fonctionnement optimal, le domaine de fonctionnement opérationnel, le seuil d'alerte de limite entre la zone de régulation en fonctionnement normal et la zone d'urgence, le seuil d'alarme de conduite, le seuil d'alarme de sécurité associé aux moyens rapides d'actions des automatismes de sécurité et le seuil de danger ou d'urgence avec la limite de la sécurité ultime. Précisons ici que le fonctionnement d'une barrière de prévention relève de la maîtrise du système et doit être considéré comme normal, même s'il est non souhaité. Par contre une

sécurité ultime est une barrière, dont le fonctionnement dans le cadre du système est considéré comme un incident par l'exploitant (éclatement d'un disque de rupture ou ouverture d'une soupape par exemple). Berdouzi et al. [2018] ont ainsi considéré trois catégories de seuils matérialisés par les indices 1 - 2 et 3 spécifiques à chaque dérive. Par exemple, le tableau 1.2 indique les valeurs de l'indice de quantification du risque de surchauffe.

		Valeur de l'indice		
		1	2	3
Gravité	ΔT_{max} (K)	$\Delta T_{max} \leq 10$	$10 < \Delta T_{max} < 40$	$\Delta T_{max} \geq 40$
Probabilité	Δt^T (min) pour $\Delta T = 10K$	$\Delta t^T \geq 30$	$10 < \Delta t^T < 30$	$\Delta t^T \leq 10$

Tableau 1.2: Indices de quantification du risque de surchauffe - d'après Berdouzi et al. [2018].

De la même façon, le tableau 1.3 indique les valeurs de l'indice de quantification du risque de surpression.

		Valeur de l'indice		
		1	2	3
Gravité	ΔP_{max} (bar)	$\Delta P_{max} \leq 0,2$	$0,2 < \Delta P_{max} < 0,8$	$\Delta P_{max} \geq 0,8$
Probabilité	Δt^P (min) pour $\Delta P = 1bar$	$\Delta t^P \geq 30$	$10 < \Delta t^P < 30$	$\Delta t^P \leq 10$

Tableau 1.3: Indices de quantification du risque de surpression - d'après Berdouzi et al. [2018].

1.2.5.1 Examen de la simulation numérique du scénario S1 de perte de refroidissement

La description du scénario S1 simple est détaillée à titre d'exemple pour montrer l'intérêt des résultats obtenus par couplage de la méthode HAZOP et de la simulation. Pour mémoire, l'initialisation de la simulation dynamique a d'abord été réalisée en régime permanent comme indiqué dans la section 1.2.3. Les modèles des différents scénarios ont été établis sous Aspen Plus et Aspen Plus Dynamics. Les scénarios numériques étudiés ont été retranscrits sous forme de programmes en langage compatible ASM pour les simulations.
La figure 1.4 rapporte les résultats de simulation dynamique du scénario S1 lors d'une perte de refroidissement. La partie (a) de la figure 1.4 indique les évolutions de la température réactionnelle T et des quantités molaires de matières du réactif thiosulfate de sodium et du produit sulfate de sodium en fonction du temps.
Après la mise initiale sous azote à 293 K du réacteur semi-fermé, l'étape d'alimentation en réactif thiosulfate de sodium à 293 K est effectuée en 20 minutes. Le milieu est ensuite préchauffé à 333 K durant 28 minutes. La perte de refroidissement du réacteur est initiée au temps de 48 minutes. Le profil de température montre que la température maximale atteinte (MTSR - Maximum Temperature of the Synthesis Reaction) est de 394 K au temps de 95 minutes, ce qui

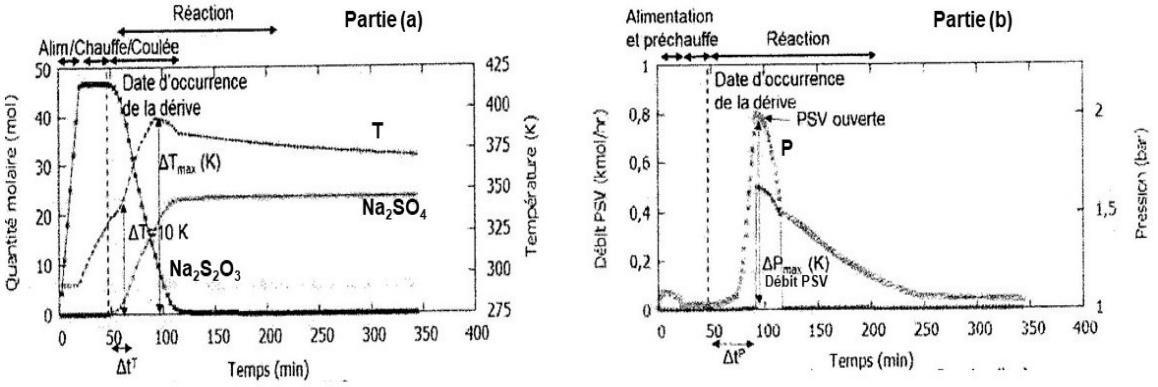

Figure 1.4: Evolutions de la température et des quantités molaires (repère a) - Evolutions de la pression et du débit de la soupape PSV (repère b) - adapté d'après Berdouzi et al. [2018].

équivaut à ΔT_{max} = 61 K. La montée en température pour atteindre ΔT_{max} est de 47 min. Il est aussi constaté que l'écart ΔT=10 K est atteint après la valeur Δt^T de 13 min.
La partie (b) de la figure 1.4 indique les évolutions de la pression P dans le ciel du réacteur et le débit molaire d'évacuation de la soupape de sécurité PSV en fonction du temps. En parallèle au pic de température de la partie (a), le diagramme de pression montre que la soupape PSV commence à s'ouvrir à un temps t de 94 min lorsque la pression ΔP_{max} atteint 2 bars. Il faut aussi un temps Δt^P = 46 min sous 1 bar pour atteindre l'ouverture de la soupape depuis l'occurence de la dérive d'absence de refroidissement. La soupape PSV se referme à un temps de 118 min, après évacuation, lorsque la pression devient inférieure à 1,5 bar.
En termes de quantification de l'évaluation du risque, le tableau 1.2 indique une valeur de l'indice de gravité de 3 pour ΔT_{max} = 61 K et une valeur de l'indice de probabilité de 2 pour Δt^T = 13 min. La criticité du risque de surchauffe du scénario S1 par perte de refroidissement est donc 6. De même, le tableau 1.3 indique une valeur de l'indice de gravité de 3 pour ΔP_{max} = 2 bars et une valeur de l'indice de probabilité de 1 pour Δt^P = 46 min. Par conséquent, la criticité du risque de surpression du scénario S1 est de 3. Il est alors possible de placer ce scénario S1 dans une classique matrice de risques.

1.2.5.2 Examen de la simulation numérique du scénario S12 comportant deux dérives simultanées

Le scénario S12 comporte simultanément les deux dérives "Plus de concentration en réactif H_2O_2 (réactif pur)" et "Contamination du réactif peroxyde d'hydrogène par des cations (Fe^{3+})". L'analyse détaillée des évolutions de la température de la masse réactionnelle et des quantités de matière d'une part, de la pression dans le ciel du réacteur et du débit d'évacuation de la soupape d'autre part permet d'évaluer les valeurs des indices respectifs de gravité (G) et de probabilité (P) pour la surchauffe et la surpression. Le tableau 1.4 regroupe les valeurs numériques de quantification du scénario S12.

Surchauffe	ΔT_{max}=51 K	Δt^T = 3,6 min	G=3	P=3
Surpression	ΔP_{max} = 1 bar	Δt^P = 6,6 min	G=3	P=2

Tableau 1.4: Données quantitatives d'évaluation du risque du scénario 12 - adapté d'après Berdouzi et al. [2018].

Le tableau 1.4 permet par exemple de conclure que le risque de surchauffe d'indice global 9 est inacceptable dans son placement dans la matrice de risque. Il est donc nécessaire de prévoir des mesures complémentaires de maîtrise des risques de protection.
En résumé, cet exemple illustre l'amélioration de la méthode HAZOP par l'apport de la simulation dynamique qui permet:

- d'effectuer une analyse paramétrique des conditions de fonctionnement;
- d'éviter la majoration du risque en quantifiant les effets d'une dérive;
- d'analyser les dérives de faibles amplitudes qui peuvent se propager et impacter des opérations unitaires le long du procédé;
- d'étudier les effets des dérives simultanées ou successives.

1.3 Exemple de la conduite d'un procédé de polymérisation du styrène

Mokhtarname et al. [2020], Mokhtarname et al. [2021] et Mokhtarname et al. [2022] ont proposé une nouvelle approche quantitative dynamique HAZOP 4.0, qu'ils ont appliquée, à l'aide d'un algorithme de supervision de procédé multivariable, à l'exemple d'un procédé continu de polymérisation de styrène. Ces auteurs considèrent que ce procédé de polymérisation est particulièrement complexe en raison des caractéristiques suivantes:

- la nature de la réaction en chaîne de la polymérisation et l'absence de possibilité de mesurer les conditions de traitement des réactions intermédiaires;
- la dynamique hautement non linéaire due à une cinétique de réaction complexe;
- la sensibilité à la quantité de monomère et de solvant;
- la réaction hautement exothermique avec possibilité d'emballement thermique;
- la dense connectivité entre les différents nœuds, notamment en raison du flux recyclé.

1.3.1 Présentation de la méthode HAZOP 4.0

Afin de faciliter l'analyse des conséquences d'un dysfonctionnement d'un procédé complexe, Mokhtarname et al. [2022] ont proposé dans la figure 1.5 l'organigramme de la méthode HAZOP 4.0 pour améliorer la procédure d'analyse des risques. Les étapes indiquées sur fond blanc rappellent celles de la méthode HAZOP classique. Les étapes complémentaires nouvelles de la méthode HAZOP 4.0 sont repésentées sur fond gris. Mokhtarname et al. [2022] ont introduit deux étapes majeures pour compléter par simulation dynamique la procédure classique:

1.3.1.1 Identification des scénarios crédibles en considérant des critères types complexes

Pour prendre en compte les effets des amplitudes et des durées des causes de déviations, des défaillances multiples, des effets de propagation et des effets domino, Mokhtarname et al. [2022] ont suggéré de considérer des critères type de complexité associés aux causes et conséquences des déviations:

- CT1 - nécessité de prendre en compte les effets de l'amplitude et de la durée des causes et des défaillances possibles;
- CT2 - nécessité d'examiner plus en détail les causes et défaillances multiples, qui pourraient être des défaillances multiples d'équipements et de dispositifs;
- CT3 - nécessité d'estimer également les effets de propagation et les effets domino possibles.

Ces critères sont évalués par les dires d'experts lors des sessions de travail de l'équipe pratiquant la méthode HAZOP. D'autres critères type de complexité peuvent être définis par l'équipe en fonction de la nature de chaque procédé.

1.3.1.2 Analyse multivariée des conséquences des variables critiques du procédé pour les scénarios HAZOP identifiés

Mokhtarname et al. [2022] ont proposé d'appliquer des techniques de contrôle des procédés multivariables traitant les variations systématiques de toutes les causes possibles d'amplitudes différentes, ainsi que leurs combinaisons crédibles pour une amélioration significative de l' efficacité des études HAZOP. Les auteurs argumentent la finalité du bien fondé de leur innovation avec les commentaires suivants:

- Dans les applications courantes des techniques de contrôle des procédés multivariables, les conditions anormales de fonctionnement d'un procédé par rapport à celles d'un procédé souhaité sont détectées par un indicateur des variations de performance. Lors de l'étude HAZOP l'attention est concentrée davantage sur les limites critiques. Il en résulte que la technique de la surveillance multivariable des procédés est retenue pour identifier les conditions critiques des variations du procédé;

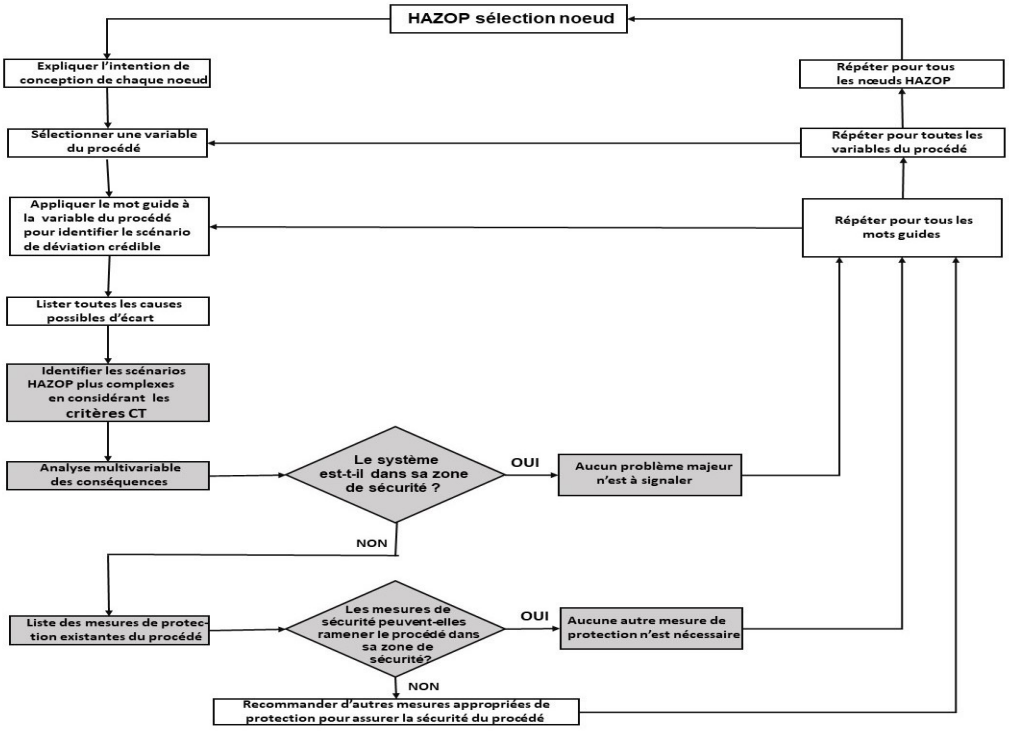

Figure 1.5: Organigramme de la procédure d'analyse par la méthode HAZOP 4.0 - adapté d'après Mokhtarname et al. [2022].

- Pour déterminer si l'état du procédé est critique ou non, chaque variable du procédé est examinée individuellement dans les études HAZOP conventionnelles pour voir si elle a atteint sa limite critique. Cependant cette analyse univariée ne fonctionne pas bien pour les processus multivariées, où il existe de nombreuses interactions et corrélations. Pour résoudre ce problème, des techniques numériques de suivi de procédés multivariables peuvent être incorporées dans la procédure pour des analyses plus précises et plus réalistes de l'étude HAZOP;
- La simulation dynamique des procédés est déjà souvent réalisée, mais en dehors des sessions de réflexion HAZOP en raison de la complexité de l'analyse et de son caractère chronophage. L'algorithme de monitoring proposé est un outil précieux, qui peut être simultanément utilisé pendant les séances de travail HAZOP en réduisant de manière significative le temps et les efforts nécessaires par rapport à la méthode conventionnelle;
- Le compte rendu, l'enregistrement et le suivi des résultats des travaux créés par la conjonction de l'application de la méthode HAZOP et de la simulation dynamique sont beaucoup plus complets et permettent d'interpréter plus facilement les scénarios possibles en termes de causes et d'effets.

Le modèle de la nouvelle approche quantitative dynamique HAZOP 4.0 peut être développé sur une plateforme, soit à l'aide d'un jumeau numérique pour une installation existante, soit

sur un simulateur pour un procédé en cours de design [Salimi et al., 2022], [Mokhtarname et al., 2022a]. Le modèle comporte les deux parties principales que sont le développement de zones d'exploitation normale et sûre de sécurité (c'est-à-dire l'élaboration de l'algorithme de monitoring) et l'analyse des scénarios HAZOP. Il convient de noter que le développement du modèle (c'est-à-dire l'inclusion des régions de fonctionnement normal et sûr) est effectué avant l'analyse HAZOP principale. Le modèle de monitoring proposé consiste en deux couches de limites de décision. La première couche est construite sur la base des données relatives à l'état de fonctionnement normal (NOC), en termes de performances et de conditions opératoires souhaitées. La deuxième couche est construite sur la base des limites des conditions sûres de fonctionnement (SOC) du procédé, en considérant que le comportement anormal du procédé est défini par des variables à leurs limites critiques. L'équipe HAZOP peut alors évaluer les effets des différents scénarios dans les respect des régions NOC et SOC. Les détails de la structure et de l'algorithme du modèle de cette approche sont décrits par Mokhtarname et al. [2022].

1.3.2 Schéma du procédé

La mise en œuvre de la polymérisation radicalaire en masse du styrène est réalisée dans une cascade de deux réacteurs parfaitement agités continus. La figure 1.6 présente le schéma de l'installation.

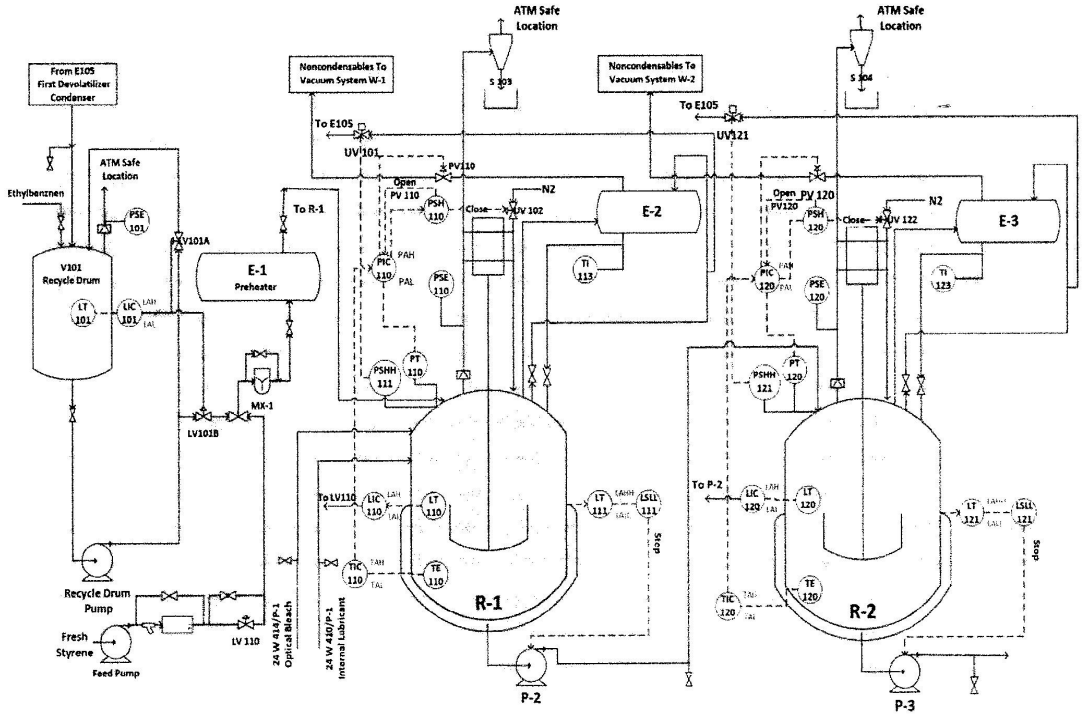

Figure 1.6: Schéma de l'installation du procédé de polymérisation du styrène - adapté d'après Mokhtarname et al. [2022].

Dans ce procédé, le monomère de styrène frais provenant du stockage est mélangé avec la charge, récupérée dans le réservoir de recyclage V101, composée de monomère n'ayant pas réagi et de solvant recyclé à partir de la sortie du 2 ième réacteur. Le mélange homogène passe ensuite par le préchauffeur E1 pour atteindre la température d'initiation de 343 K avant d'être introduit dans le premier réacteur R1. La réaction de polymérisation est initiée thermiquement et se réalise dans la cascade des deux réacteurs R1 et R2 disposés en série, chacun de 25 m^3 de volume. Le débit massique global de l'alimentation d'entrée et le temps de passage dans les deux réacteurs sont respectivement de 6 tonnes par heure et 2 heures. La polymérisation du styrène étant fortement exothermique, l'enthalpie de réaction dans les deux réacteurs est évacuée par deux échangeurs de chaleur à tubes et calandre E2 et E3 séparés. L'eau est le fluide de refroidissement. Les deux échangeurs de chaleur ont été conçus pour faire face à des conditions d'emballement thermique. Les systèmes de vide W1 et W2 connectés aux échangeurs de chaleur sont utilisés pour ajuster le taux de vaporisation par le biais des vannes de pression PV110 et PV120. Un flux d'azote gazeux non condensable est injecté dans les deux réacteurs pour évacuer le monomère vaporisé et le mélange de solvants vers les échangeurs de chaleur. Les mélanges de monomère et solvant condensés sont retournés par reflux dans les réacteurs et les gaz non condensables sont purgés par la pompe à vide. Les conditions opératoires de fonctionnement du procédé sont récapitulées dans le tableau 1.5.

Réacteur	Pression (barg)	Température (K)	Contenu solide (%)
R1	0	413	35
R2	0,1	423	60

Tableau 1.5: Conditions opératoires du procédé - d'après Mokhtarname et al. [2022]

La figure 1.6 illustre aussi toutes les mesures de sécurité du procédé. Les systèmes de contrôle du procédé constituent la première couche de protection, qui contribue à la sécurité et aux performances globales de l'installation en maintenant automatiquement les variables clés à proximité de leurs valeurs opératoires. Dans ce processus, les boucles critiques sont les boucles de contrôle de la température et de la pression des réacteurs R1 et R2. La température d'un réacteur est régulée par l'indicateur et contrôleur de température (TIC) qui fonctionne en cascade sur l'indicateur et contrôleur de pression (PIC). Le PIC régule la vanne PV sur la ligne de vapeur connectée au système de vide pour ajuster le taux de vaporisation. Si la boucle de contrôle en cascade ne peut pas compenser les variations de pression dans le réacteur, des alarmes du procédé sont activées pour alerter les opérateurs. Pour les variations importantes de pression, le pressostat haut (PSH) coupe automatiquement l'azote du réacteur et ouvre la vanne PV du système de vide. Si cette barrière de protection ne parvient pas non plus à réduire la pression du réacteur, un pressostat haute haute pression (PSHH) est activé pour connecter le réacteur à un système de vide plus puissant. Enfin si tous ces dispositifs ne sont pas en mesure d'empêcher une nouvelle augmentation de la pression dans le réacteur, la dernière ligne de défense est constituée par l'élément ultime de sécurité sous pression d'un disque de rupture (PSE) pour empêcher l'explosion de la cuve du réacteur.

1.3.3 Schéma cinétique réactionnel

La complexité de la polymérisation radicalaire en masse du styrène est due à un mécanisme cinétique complexe comprenant:

- l'initiation thermique;
- la propagation;
- le transfert de chaîne;
- la terminaison.

En considérant que M représente le monomère du styrène, S le solvant, P_x et D_x les chaines vivantes et mortes de longueur x, la cinétique réactionnelle de polymérisation du styrène de cet exemple est résumée comme par les équations suivantes:

$$\text{Initiation thermique} \qquad 3\,M \xrightarrow{k_{Ti}} 2\,P_1 \tag{1.4}$$

$$\text{Propagation} \qquad P_x + M \xrightarrow{k_P} P_{x+1} \tag{1.5}$$

Transfert de chaîne vers :

$$\text{Monomère} \qquad P_x + M \xrightarrow{k_{trm}} D_x + P_1 \tag{1.6}$$

$$\text{Solvant} \qquad P_x + S \xrightarrow{k_{trs}} D_x + P_1 \tag{1.7}$$

$$\text{Terminaison} \qquad P_x + P_y \xrightarrow{k_{tc}} D_{x+y} \tag{1.8}$$

où l'équation d'Arrhénius est appliquée pour estimer les constantes de vitesse de réaction en fonction de la température.

1.3.4 Validation de la procédure pour l'analyse du fonctionnement opératoire normal

La procédure proposée est appliquée au réacteur R1 de polymérisation. Les quatre variables critiques tel que la pression, la température, le niveau du réacteur et la température de sortie du condenseur sont considérées comme des variables de contrôle. Le modèle mathématique retenu est détaillé par Mokhtarname et al. [2021]. Pour mémoire, dans les conditions normales de fonctionnement, le gel de polymère (c'est-à-dire la combinaison du monomère de styrène liquide, de l'éthylbenzène et du polystyrène en tant que produit) et le mélange de vapeurs (c'est-à-dire la combinaison du monomère de styrène vaporisé, de l'éthylbenzène et du gaz N2) sont à l'équilibre. L'objectif du modèle dynamique du procédé est de simuler les conditions opératoires normales et de sécurité à l'aide du logiciel MATLAB. La validation du modèle est testée

avec de nombreuses données industrielles approuvées par les opérateurs et les experts. Durant la phase d'entrainement du modèle, un nombre approprié appelé Principales Composantes (PC) est déterminé. Ces PC sont en fait de nouvelles projections des variables du processus d'origine dans un autre espace avec moins de variables effectives et sans corrélation. Dans cet exemple, Mokhtarname et al. [2022] ont montré qu'il est ainsi possible de réduire le nombre PC à la valeur 2, alors que la valeur de la dimension originale des données était de 4. La figure 1.7 montre une présentation des zones matérialisant les conditions de fonctionnement normal (NOC) et celles de fonctionnement en sécurité (SOC) dans l'espace 2D des Principales Composantes.

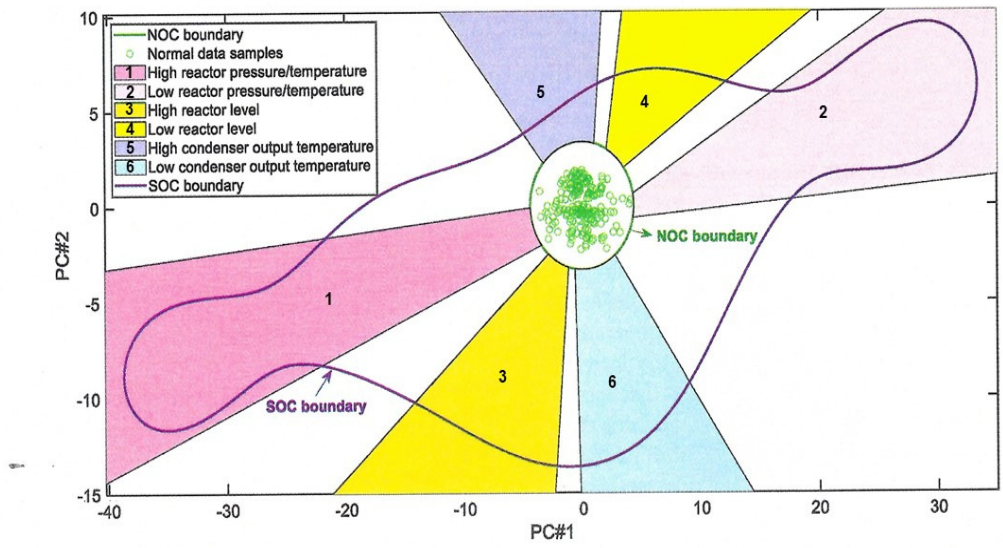

Figure 1.7: Limites des zones de conditions de fonctionnement normales (NOC) et sûres (SOC) dans l'espace 2D des Composantes Principales (PC#1) et (PC#2) - adapté d'après Mokhtarname et al. [2022].

Les points représentatifs des données de fonctionnement opératoire normal sont regroupés dans la zone identifiée NOC. Les différentes causes d'une déviation de chaque variable du procédé partagent la même relation statistique qui peut être mesurée quantitativement. La direction d'évolution des données relatives aux défaillances est une bonne mesure pour caractériser les écarts par rapport à la valeur initiale de conception. Les tendances de direction des défaillances des variables du procédé, comme indiquées avec les repères "haute ou basse pression du réacteur", "haute ou basse température du réacteur", "haut ou bas niveau du réacteur" et "haute ou basse température de sortie du condenseur". sont également mises en évidence dans la figure 1.7. Il est important de noter que les régions identifiées par des couleurs et des repères numériques ne sont pas vraiment précises et bien formées, mais qu'elles servent surtout à trans-

mettre pédagogiquement le concept adopté. Cette présentation permet néanmoins de mieux interpréter les résultats de la simulation et de rendre l'analyse des risques plus facilement compréhensible pour l'équipe HAZOP. En effet, la distance des données sur les défaillances par rapport à la région normale peut être utilisée comme un indicateur de l'importance de chaque défaillance. De même, le temps nécessaire pour approcher la zone critique SOC est une autre mesure importante puisqu'elle détermine la vitesse à laquelle les opérateurs de l'unité de production ou les dispositifs de protection du procédé doivent être en mesure de réagir à la situation défectueuse détectée. Le temps de réponse de la sécurité peut être aussi facilement obtenu à partir des résultats de la simulation.

1.3.5 Identification préliminaire HAZOP des scénarios complexes

A ce stade, il est nécessaire d'identifier divers scénarios complexes. Le tableau 1.6 en indique quelques exemples. L'objectif est ensuite de montrer comment les algorithmes de conduite et de surveillance des processus multivariables seront utiles pour aider l'équipe chargée de l'étude HAZOP.

Dérives	Causes possibles	Description de la complexité	Critère de complexité	Conséquences potentielles
Haute pression dans le réacteur	Défaillance vanne PV110 ou de son systéme de contrôle	Le pourcentage d'ouverture PV110 a un effet très important sur la gravité des conséquences	CT1	L'augmentation de la température influence la vitesse de polymérisation et la qualité du produit
		La fermeture PC110 génére vite les conditions d'un emballement	CT1	Cas critique d'emballement
	Excès d'injection d'azote suite erreur opérateur	Si cette dérive est accompagnée de la défaillance PV110 il y a risque d'emballement	CT1 CT2	Emballement thermique Augmentation de la charge du système de vide
		Grosse variation du débit d'azote et vanne PV110 fermée	CT1 CT2	Emballement thermique Augmentation de la charge du système de vide
Haute température dans le réacteur	Alimentation surchauffée dans l'échangeur E1	Une forte surchauffe augmente la charge du condenseur et les conditions d'emballement	CT1 CT2	colmatage partiel de E1 - augmentation du taux de polymerisation dans les conduites en amont de R1
		L'effet de cette déviation est augmentée si PV110 ou son système de contrôle défaillent	CT1 CT2	Augmentation de la vitesse de polymérisation et du % en solide dans R1
	Concentration basse en solvant éthylbenzène	Les variations de concentration en solvant ont des conséquences	CT1	Augmentation de la vitesse de polymérisation et du % en solide dans R1

Tableau 1.6: Exemples de scénarios complexes avec déviations HAZOP - adapté d'après Mokhtarname et al. [2022].

1.3.6 Exemple d'application de la procédure pour l'analyse de la déviation d'une augmentation de température

L'exemple traité pour l'illustration de la procédure considère le scénario de la déviation d'une augmentation de la température de l'alimentation du réacteur R1 en raison d'une défaillance de l'échangeur E1, qui surchauffe anormalement l'alimentation. La simulation du comportement de ce scénario est d'abord réalisée en l'absence de mesure de maîtrise des risques. Les conséquences évaluées par simulation, en fonction des différentes amplitudes des variables critiques du procédé et des temps de réponse, permettent de proposer des mesures de correction par protection. La vérification de l'adéquation du rôle de ces barrières est effectuée par une nouvelle simulation.
Pour mémoire, en fonctionnement opératoire normal, la température du réacteur R1 est de 415 K avec une zone de régulation de ± 10 K, alors que la température de préchauffage de l'alimentation à la sortie de l'échangeur E1 est de 343 K. La simulation est initiée en imposant des déviations en forme de fonction échelon de 20% et de 40% de la température initiale de l'alimentation. La température du réacteur R1 tend à augmenter dès l'application de la déviation. L'action de la cascade des contrôleurs indicateurs TIC et PIC du réacteur R1 ouvre la vanne PV110, ce qui provoque une augmentation de la vaporisation du contenu du réacteur en accroissant la charge du condenseur et la température de condensation du liquide. Cette action contribue à réduire la température du réacteur. La figure 1.8 matérialise la description du comportement du réacteur R1, d'abord en l'absence de régulation de contrôle. La position de l'augmentation de la température dans la zone 1 "Haute température de R1" est d'autant plus éloignée de la zone NOC que l'échelon est important. La simulation montre aussi que l'augmentation de la température du réacteur R1 est bien compensée en présence de la boucle de régulation TIC - PIC. La position des résultats simulés positionnés à proximité de la zone NOC et de la zone 5 "Haute température de sortie du condenseur" confirme bien que l'accroissement de la charge du condenseur entraine une augmentation de la température de sortie du condenseur. En résumé, dans cet exemple il est possible de conclure que l'effet de l'augmentation de la température d'alimentation sur la température du réacteur R1 n'est pas significatif, même pour des amplitudes de défaillance importantes (40%), le fonctionnement du régulateur de température en cascade garantissant la conduite du réacteur R1 en l'absence de défaillance de la vanne PV110.

Remarque
Dans le cadre d'un enseignement de sécurité des procédés de niveau Master, il est possible d'adopter une progression pédagogique de la sensibilisation au couplage de la méthode HAZOP et de la simulation en enchainant successivement les étapes suivantes:

- débuter par l'observation de diagramme d'évolution simple d'une défaillance en fonction du temps à l'aide des résultats de Mokhtarname et al. [2020];

- enchainer avec l'examen des évolutions simultanées de plusieurs paramètres en fonction du temps proposées par Mokhtarname et al. [2021];

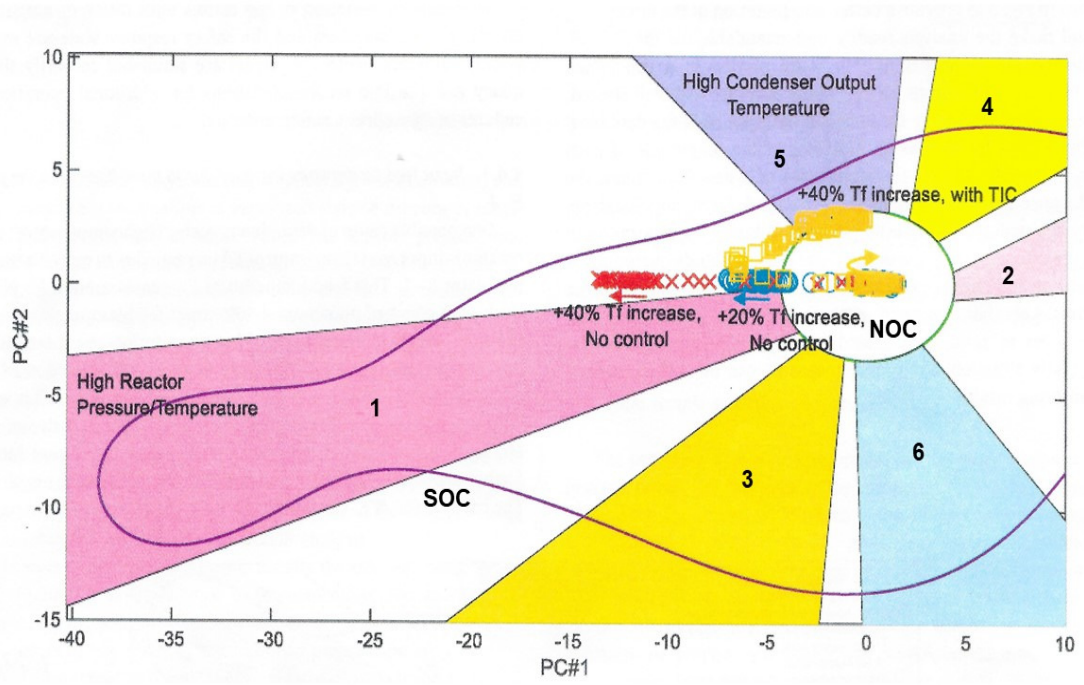

Figure 1.8: Position dans l'espace 2D (PC#1) et (PC#2) des résultats simulés de la déviation "Haute température dans le réacteur R1" dans le cas d'une température d'alimentation trop élevée de 20% et 40% sans et avec régulation de contrôle - adapté d'après Mokhtarname et al. [2022].

- examiner enfin les résultats simulés présentés sous la forme des diagrammes de zones intégrant les notions de NOC et SOC utilisés par Mokhtarname et al. [2022].

Il est recommandé de faire partager aux apprenants l'intéressant contenu pédagogique de la démonstration vidéo proposée par Salimi et al. [2022], accessible suivant le lien `https://lnkd.in/e-VrPNAj`.

Chapitre 2

Approche dynamique quantifiée de la méthode de l'arbre des défaillances

2.1 Rappel de la méthode classique de l'arbre des défaillances

La méthode de l'arbre des défaillances est aussi connue sous les noms d'arbre des causes, d'arbre des défauts ou d'arbre des fautes. C'est la seule méthode, parmi les différentes autres méthodes d'analyse des risques, procédant d'une démarche déductive en progressant des effets vers les causes, c'est-à-dire en sens inverse du déroulement du temps. L'acceptation de cette classification implique de s'attacher prioritairement au mode d'examen du système analysé et non au mode de raisonnement intrinsèque à la méthode.
La méthode de l'arbre des défaillances a pour objet de déterminer les diverses combinaisons possibles d'événements entraînant la réalisation d'un événement indésirable unique et redouté et de représenter graphiquement ces combinaisons au moyen d'une structure arborescente. Cette méthode d'analyse permet donc, grâce à un raisonnement déductif basé sur un certain nombre de principes et de règles, d'accéder aux multiples causes d'un événement final unique préalablement bien identifié et de représenter ces causes sous forme d'un arbre. L'arbre des défaillances est un diagramme logique qui décrit l'enchaînement, en parallèle ou en série, d'événements qui conduisent à l'événement final indésiré appelé événement de tête de l'arbre des défaillances. L'arbre des défaillances est formé de niveaux successifs d'événements, tel que chaque événement est généré à partir des événements de niveau inférieur par l'intermédiaire de divers opérateurs ou portes logiques. Ces événements sont en général des défauts associés à des défaillances d'équipements et matériels, à des erreurs humaines, à des défauts de logiciels, à des lacunes organisationnelles... pouvant conduire à l'événement indésirable. Le processus déductif d'analyse est conduit jusqu'à l'obtention des événements de base indépendants entre eux et si possible à probabilité d'occurrence estimable.
Les éléments et symboles de représentation utilisés, les principes et les règles d'élaboration, la mise en oeuvre de la méthode, la construction et l'exploitation de l'arbre en termes d'analyse qualitative, semi-quantifiée et quantitative sont détaillés dans le chapitre 13 de l'ouvrage "Sécurité des procédés chimiques" [Laurent, 2011].

2.2 Approche dynamique de la méthode de l'arbre des défaillances

Ruijters and Stoelinga [2015], Kabir [2017] et Aslansefat et al. [2020] ont présenté des revues de synthèse de la méthode de l'arbre des défaillances, de ses extensions et surtout des diverses potentialités des améliorations dynamiques de son application. En effet, le caractère statique de la méthode de l'arbre des défaillances limite son utilisation et doit lui faire préférer d'autres types de modélisation plus complexes pour tenir compte de la dynamique des systèmes. La modélisation pourrait alors échapper au concepteur non spécialisé et sa validation deviendrait de ce fait hasardeuse. Pour mémoire, les événements de base d'un arbre sont généralement régis par des lois d'apparition et de disparition (processus de défaillance et de réparation par exemple) et il n'est pas toujours possible ou judicieux de leur attribuer une probabilité d'occurrence fixe (valeur moyenne). De plus, l'arbre de défaillance suppose une totale indépendance entre les événements de base. Or ceux-ci peuvent être liés par des relations de dépendance quand la réalisation d'un événement favorise (dépendance stochastique) ou impose (forçage d'état) la réalisation d'autres événements de l'arbre. Les événements sont liés par une relation de dépendance de type stochastique quand l'occurrence de l'un modifie les conditions probabilistes d'occurrence des autres événements. Les événement sont liés par une relation de dépendance de type forçage d'état quand l'occurrence de l'un modifie l'état des autres événements. Ces relations découlent de la nature même du système considéré. Les événements peuvent enfin être affectés par des dépendances temporelles qui modifient leur état ou leurs conditions probabilistes après une certain temps écoulé depuis le début de la mission du système ou depuis l'apparition d'événements particuliers. Ces dépendances sont souvent déterministes et concernent généralement des phases de mission ou des changements de fonctionnement.
La présentation sera limitée à l'extension proposée par Cepin and Mavko [2002] et aux améliorations dynamiques respectives des réseaux bayésiens et de la logique floue.

2.2.1 Extension dynamique d'un arbre des défaillances avec des conditions temporelles

Cepin and Mavko [2002] considèrent qu'un arbre classique des défaillances comporte un événement de tête, des événements de base, des portes logiques et des événements maison appelés aussi événements déclencheurs. Un événement maison est utilisé pour représenter un événement qui devrait normalement se produire. Un événement maison peut être activé ou désactivé. Lorsqu'un événement maison est activé (vrai), cet événement est présumé s'être produit et sa probabilité est fixée à 1. Lorsqu'un événement maison est désactivé (faux), cet événement est présumé ne pas s'être produit et sa probabilité est fixée à 0. Ces événements maison sont utiles pour rendre des parties d'un arbre soit fonctionnelles, soit non fonctionnelles.

2.2.1.1 Arbre classique des défaillances

Cepin and Mavko [2002] proposent de représenter mathématiquement un arbre classique des défaillances par les équations suivantes:

$$G_i = f(G_p, B_j, H_s) \qquad i, p \in (1...P), j \in (1...J), s \in (1...S) \tag{2.1}$$

où G_i est la porte i, B_j est l'événement de base j, H_s est l'événement maison s, P est le nombre de portes, J est le nombre d'événements de base et S est le nombre d'événements maison.

$$GD = \bigcup_{i=1}^{n} MCS_i \tag{2.2}$$

où GD est l'événement de tête et MCS_i est la coupe minimale i.

$$MCS_i = \bigcap_{j=1}^{m} B_j \tag{2.3}$$

Le détail des calculs est indiqué dans l'article de Cepin and Mavko [2002]. Dans le cas où les événements de base sont mutuellement indépendants, la probabilité d'occurence Q_{MCS_i} est estimée par la relation:

$$Q_{MCS_i} = \prod_{j=1}^{m} Q_{B_j} \qquad Q_{B_j} = Q_{B_j}(T_j,\, \lambda_j,\, q_j) \tag{2.4}$$

où T_j est l'intervalle de temps considéré, λ_j est le taux de défaillance et q_j est la probabilité de défaillance de l'équipement modélisé dans l'événement de base j.
La probabilité Q_{GD} de l'événement de tête est en fait souvent approximée par la relation simplifiée:

$$Q_{GD} = \sum_{i=1}^{n} Q_{MCS_i} \tag{2.5}$$

Pour des valeurs de Q_{MCS_i} inférieures à $0,1$, la précision du résultat est de l'ordre de 10%, soit une valeur conservative avec une probabilité de défaillance légèrement plus élevée.

2.2.1.2 Prise en compte des éléments maison

La saisie de l'état des événements maison se fait par l'intermédiaire de la matrice des événements maison.

$$||MH_{ST}|| = \begin{Vmatrix} H_{11} & H_{12} & ... & H_{1T} \\ H_{21} & ... & ... & ... \\ ... & H_{st} & ... & ... \\ H_{S1} & ... & ... & H_{ST} \end{Vmatrix} \tag{2.6}$$

Le nombre de rangées représente le nombre d'événements maison dans le modèle, qui modélisent le comportement d'une certaine configuration du système en fonction du temps. Le nombre de colonnes représente le nombre de périodes de temps au cours desquelles des configurations mutuellement différentes existent.
La figure 2.1 illustre deux exemples simples d'utilisation de la matrice des événements maison dans le fonctionnement respectif des portes ET et OU.

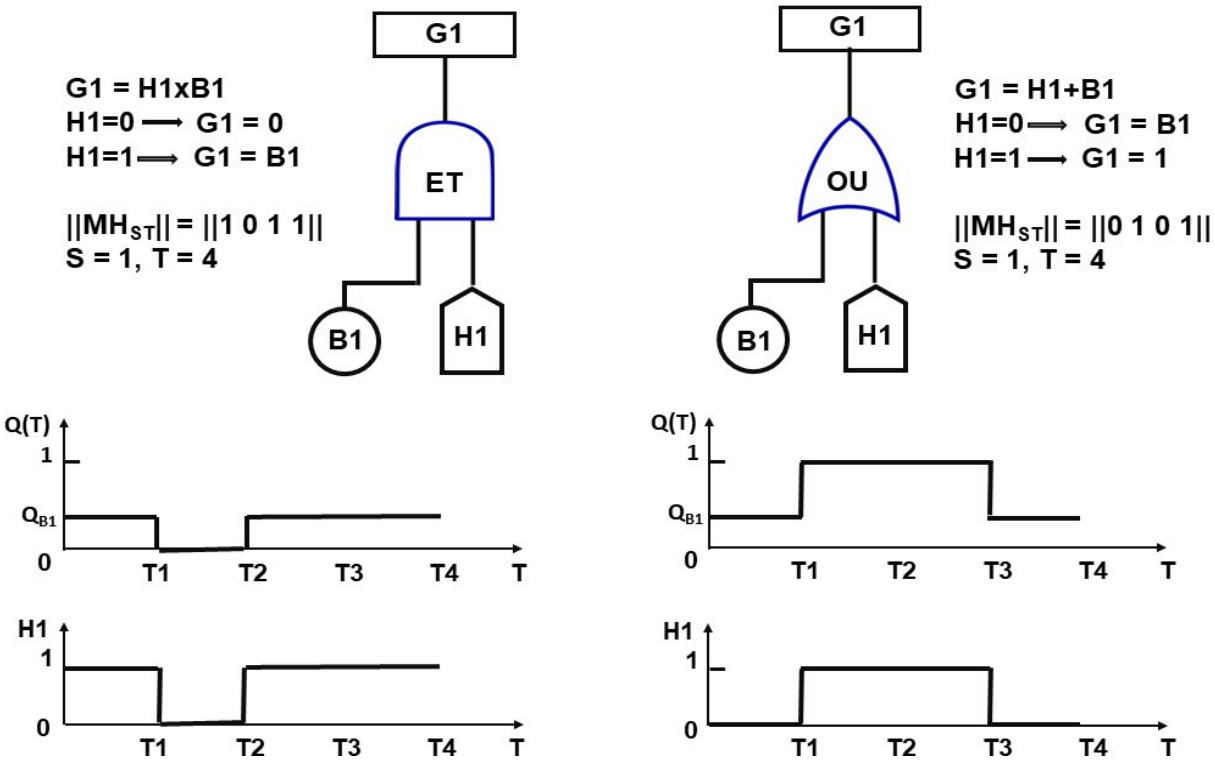

Figure 2.1: Exemples d'utilisation de la matrice des événements maison dans le fonctionnement respectif d'une porte ET (partie gauche) et d'une porte OU (partie droite) - adapté d'après Cepin and Mavko [2002].

Evénement maison et porte OU

L'événement maison H1, sous la porte OU, sert à modéliser une panne de l'équipement modélisé dans la porte ou l'événement de base sous la porte OU mentionnée. Lorsque l'événement maison H1 est réglé sur 0 (faux), la porte G1 dépend de l'événement de base B1. Lorsque l'événement maison H1 est réglé sur 1 (vrai), la porte G1 est à 1 (vrai) indépendamment de l'événement de base B1. Lorsque l'événement maison H1 est réglé sur 1 (vrai), la panne de l'équipement modélisé dans l'événement de base B1 est simulée. Le diagramme temporel explique la matrice de l'événement maison qui, pour les points temporels T2 et T3, simule la panne de l'équipement modélisé dans l'événement de base B1.

Evénement maison et porte ET

L'événement maison H1 sous la porte ET sert soit à modéliser plus de modes opérationnels de l'équipement modélisé dans la porte ou l'événement de base sous la porte ET mentionnée, soit à modéliser plus de critères de réussite de l'équipement modélisé dans la porte ou l'événement de base sous la porte ET mentionnée. Lorsque l'événement maison H1 est réglé sur 0 (faux), la porte G1 est à 0 (faux). Lorsque l'événement maison H1 est réglé sur 1 (vrai), la porte G1 dépend de l'événement de base B1. Lorsque l'événement maison H1 est réglé sur 0 (faux), le deuxième mode opérationnel du système modélisé dans la porte G1 est modélisé, mais l'équipement modélisé dans l'événement de base B1 n'est pas pris en compte dans le modèle. Le diagramme temporel explique la matrice des événements maison qui, pour le point temporel T2, simule le deuxième mode opérationnel du système modélisé à la porte G1. Au point temporel T2, l'équipement modélisé dans l'événement de base B1 n'est pas pris en compte dans le modèle. Le premier mode opérationnel du système modélisé dans la porte G1 aux points temporels T1, T3 et T4 exige que l'équipement modélisé dans l'événement de base B1 soit pris en compte dans le modèle et puisse contribuer à la porte G1.
En résumé, l'arbre de défaillance dynamique permet de modéliser les exigences temporelles de deux manières :

- en introduisant des modèles dépendant du temps pour les probabilités de défaillance des composants (représentant les indisponibilités des événements de base);
- par l'introduction de la matrice des événements maison, qui définit l'activation et la désactivation en temps voulu des parties de l'arbre de défaillance (représentant les parties du système).

2.2.1.3 Arbre dynamique des défaillances

En reprenant et en étendant les équations 2.1, 2.2 et 2.3, Cepin and Mavko [2002] ont établi les équations d'un arbre dynamique des défaillances:

$$G_i(t) = f(G_p, B_j, H_{st}) \qquad i, p \in (1...P), j \in (1...J), s \in (1...S), t \in (1...T) \tag{2.7}$$

où $G_i(t)$ est la porte i au temps t, H_{st} est la valeur d'un élément maison au temps t et T est le nombre de points temporels.

$$GD(t) = \bigcup_{i=1}^{n} MCS_i(H_{1t}, H_{2t}, ..., H_{st}, ..., H_{St}) \tag{2.8}$$

où $GD(t)$ est l'événement de tête au temps t et MCS_i est la coupe minimale i au temps t.

$$MCS_i(H_{1t}, H_{2t}, ..., H_{st}, ..., H_{St}) = \bigcap_{j=1}^{m} B_j \tag{2.9}$$

Le détail des calculs est indiqué dans l'article de Cepin and Mavko [2002]. Dans le cas où les événements de base sont mutuellement indépendants, la probabilité d'occurence Q_{MCS_i} est estimée par la relation:

$$Q_{MCS_i}(H_{1t}, H_{2t}, ..., H_{st}, ..., H_{St}) = \prod_{j=1}^{m} Q_{B_j}(t) \tag{2.10}$$

avec

$$Q_{B_j}(t) = Q_{B_j}(\lambda_j,\, q_j,\, T_{ij},\, T_{tj},\, T_{rj},\, T_{pj...t}) \tag{2.11}$$

où T_{ij} est l'intervalle d'essai de l'équipement modélisé dans l'événement de base j, T_{tj} est la durée d'indisponibilité de l'équipement modélisé dans l'événement de base j, T_{rj} est le délai de remise en état (délai moyen de réparation) de l'équipement modélisé dans l'événement de base j et T_{pj} est le temps de localisation de la panne pour l'équipement modélisé dans l'événement de base j.
La probabilité $Q_{GD}(t)$ de l'événement de tête est en fait souvent approximée par la relation simplifiée:

$$Q_{GD}(t) = \sum_{i=1}^{n} Q_{MCS_i}(H_{1t}, H_{2t}, ..., H_{st}, ..., H_{St}) \tag{2.12}$$

L'arbre de défaillance dynamique est utilisé pour la modélisation et l'évaluation d'une entité étudiée, car l'arbre de défaillance classique n'est pas en mesure de déterminer la probabilité de l'événement de tête en fonction du temps pour suivre les changements de la configuration du système. Pour chacun des points temporels discrets sélectionnés dans l'intervalle de temps choisi, une configuration d'équipement appropriée est déterminée et notée dans la colonne correspondante de la matrice des événements maison. L'indisponibilité du système, qui sert de mesure du risque au niveau du système, est calculée pour tous les points temporels sélectionnés. L'indisponibilité moyenne du système sur l'intervalle de temps retenu est calculée à partir des indisponibilités dépendantes du temps. La disposition optimale des composants défaillants est déterminée sur la base de la minimisation de l'indisponibilité moyenne en tant que fonction ou disposition de la configuration de l'équipement. Une méthode d'optimisation basée sur un algorithme de simulation a été développée afin de déterminer le calendrier optimal des entretiens et arrêts des équipements de sécurité d'un système [Cepin, 2002].

2.3 Application d'un réseau bayésien à l'analyse de l'arbre des défaillances d'un système d'arrosage automatique par sprinkler

2.3.1 Description du système d'extinction automatique d'incendie

La figure 2.2 présente le schéma de principe de l'installation d'extinction automatique d'incendie.

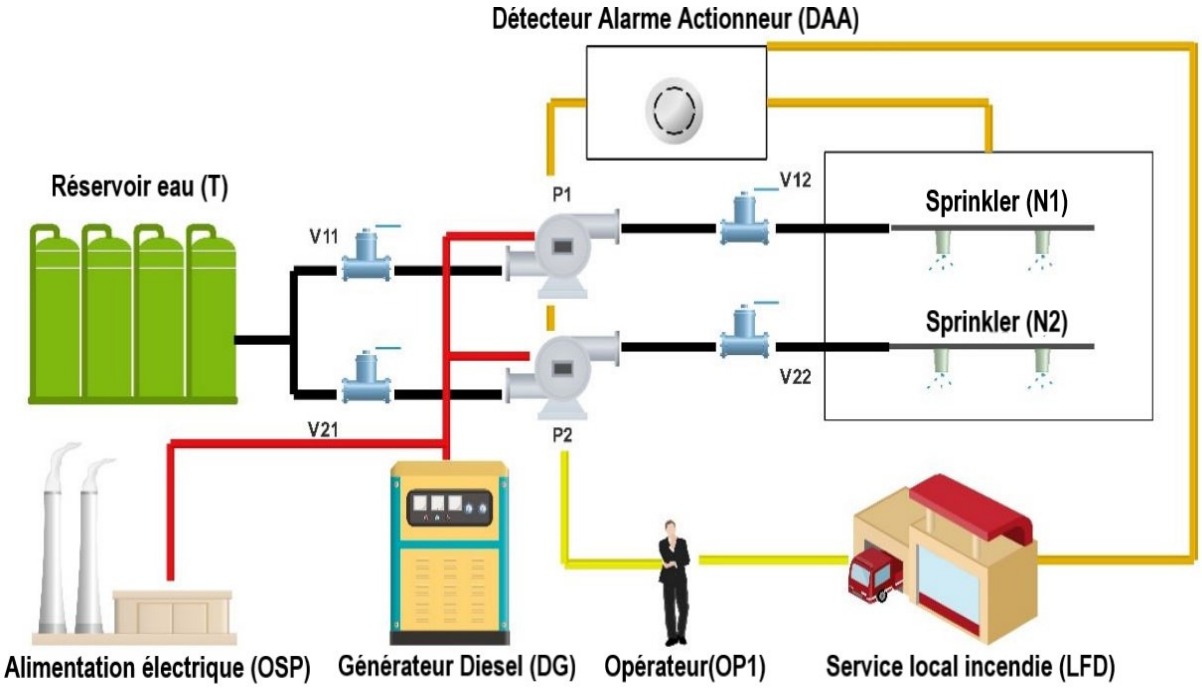

Figure 2.2: Schéma de principe de l'installation d'extinction automatique d'incendie par sprinkler - adapté d'après Givehchi and Heidari [2018].

Deux buses N1 et N2, qui éteignent physiquement le feu avec de l'eau, ont été conçues de manière à ce que chacune d'entre elles puisse contrôler toutes les conditions d'incendie dans l'environnement de l'installation. La buse N1 est le premier mode de pulvérisation d'eau. Dès qu'un signal est reçu du détecteur de l'alarme DAA ou de l'opérateur OP1, la pompe P1 commence à fonctionner automatiquement et extrait l'eau du réservoir T pour la pulvériser dans la zone d'incendie. Si le système de pulvérisation N1 n'est pas déclenchée correctement, l' opérateur local OP1 peut activer manuellement la deuxième rampe de pulvérisation N2 Si la deuxième voie N2 n'est pas disponible, l'opérateur demande de l'aide à la caserne de pompiers locale LFD, bien que le détecteur de l'alarme DAA envoie automatiquement un signal directement au service d'incendie LFD. Cependant, dans ce cas, il faut beaucoup de temps par rapport au moment où les buses sont disponibles et éteignent l'incendie et les dégâts sont plus importants. Dans ces conditions, si l'alimentation électrique externe OSP n'est pas disponible en raison de l'incendie ou pour toute autre raison, un générateur diesel local DG fournira l'énergie nécessaire aux pompes. En outre, le système de détection alarme DAA est alimenté par plusieurs batteries préalablement en charge permanente par l'alimentation électrique externe. Même si l'alimentation en courant alternatif est coupée, l'alimentation en courant continu est fournie par les batteries toujours disponibles. Les vannes manuelles V11, V12, V21 et V22 situées de part et d'autre des pompes P1 et P2 sont normalement ouvertes et ne sont fermées que lorsqu'elles sont en cours de réparation. L'alimentation électrique OSP et le générateur diesel DG sont situés à l'extérieur de l'aire du réacteur à protéger par arrosage et ne sont donc pas soumis à un incendie interne.

2.3.2 Arbre des défaillances du système d'arrosage

La description du système d'extinction automatique d'incendie par sprinkler a permis d'identifier trois phases de fonctionnement du système.
Dans la première phase, l'incendie est d'abord détecté par le détecteur d'alarme DAA et un signal est envoyé à la pompe P1 jusqu'à ce que l'eau du réservoir T entre dans la pompe P1 par la canalisation comportant la vanne V11, puis l'eau est pompée par la canalisation repérée par la vanne V22 vers la buse N1. Si l'un des composants T, V11, P1, V12 et N1 tombe en panne, la première phase sera complètement affectée. La pompe P1 ne fonctionnera pas correctement lorsqu'elle est elle-même défaillante, ou lorsque le détecteur d'alarme DAA n'envoie pas de signal à la pompe P1, ou lorsque les systèmes du générateur diesel DG et l'alimentation électrique du site OSP ne fonctionnent pas simultanément.
Si la première phase ne répond pas, la deuxième phase est normalement activée par l'opérateur OP1 qui démarre le système de pompe P2. Le déroulement du processus restant et les modes de défaillance du système sont les mêmes que ceux de la première phase.
Dans le cas où les deux premières phases sont défaillantes, une troisième phase sera considérée comme l'option finale avec le déclenchement de l'alarme DAA ou l'initiative de l'opérateur OP1 informant le service LFD de lutte contre l'incendie de la survenue de la défaillance totale du système. En retenant ces trois phases de fonctionnement, l'arbre de défaillance du système est illustré par la figure 2.3.

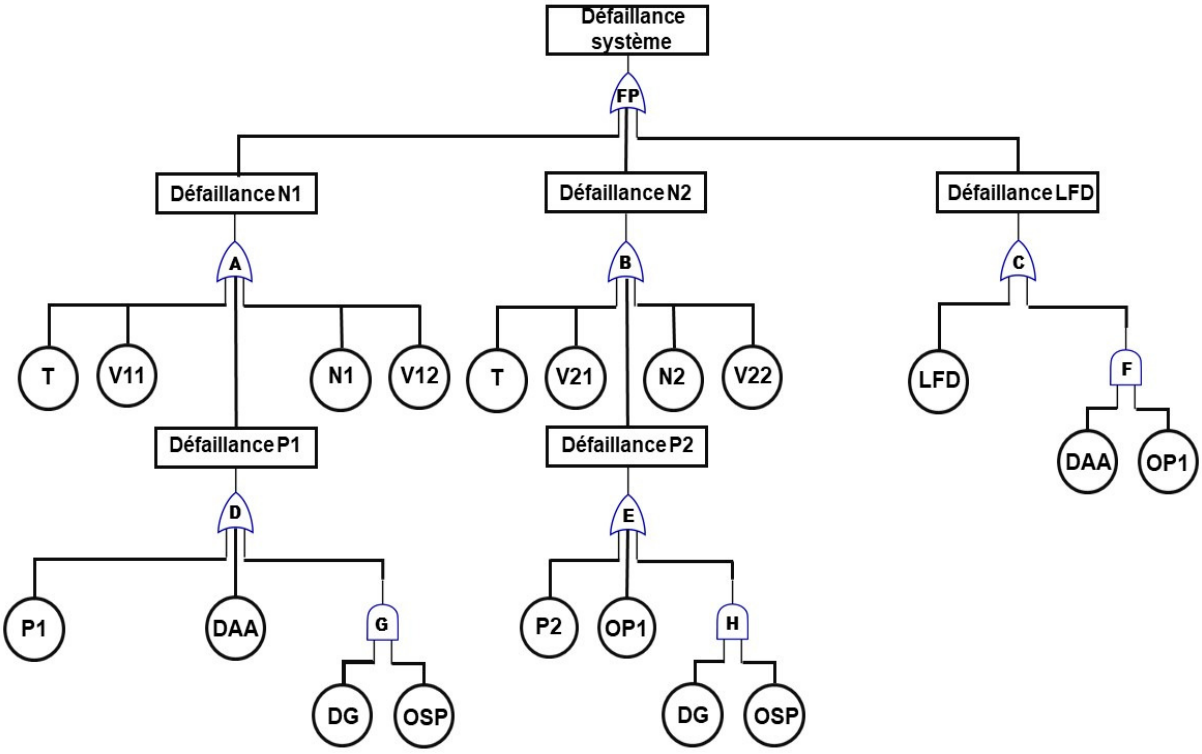

Figure 2.3: Arbre des défaillances de l'installation d'extinction automatique d'incendie par sprinkler - adapté d'après Givehchi and Heidari [2018].

Le tableau 2.1 regroupe les valeurs des probabilités des défaillances des divers éléments de l'installation d'arrosage, valeurs extraites des banques de données et des dires d'experts.

Repère	Composant	Probabilité de défaillance
OSP	Alimentation électrique	$1,1 \times 10^{-4}$
DG	Générateur diesel	$5,5 \times 10^{-2}$
DAA	Détecteur d'alarme	$1,0 \times 10^{-4}$
P1, P2	Pompes 1 et 2	$1,7 \times 10^{-2}$
OP1	Opérateur	$1,0 \times 10^{-2}$
T	Réservoir	$1,0 \times 10^{-5}$
V(ij)	Vannes	$4,2 \times 10^{-3}$
N1, N2	Buse de pulvérisation	$1,0 \times 10^{-5}$
LFD	Local lutte incendie	$1,0 \times 10^{-4}$

Tableau 2.1: Probabilités de défaillances des composants du système d'extinction automatique par arrosage sprinkler - adapté d'après Givehchi and Heidari [2018]

La quantification de l'arbre des défaillances est réalisée à l'aide de la série d'équations relatives aux probabilités des différents composants.

$$
\begin{aligned}
p(FP) &= p(A) + p(B) + p(C) && (2.13)\\
p(A) &= p(T) + p(V11) + p(N1) + p(V12) + p(D) && (2.14)\\
p(B) &= p(T) + p(V21) + p(N2) + p(V22) + p(E) && (2.15)\\
p(C) &= P(LFD) + p(F) && (2.16)\\
p(D) &= p(P1) + p(DAA) + p(G) && (2.17)\\
p(E) &= p(P2) + p(OP1) + p(H) && (2.18)\\
p(F) &= p(DAA) \times p(OP1) && (2.19)\\
p(G) &= p(DG) \times p(OSP) && (2.20)\\
p(H) &= p(DG) \times p(OSP) && (2.21)
\end{aligned}
$$

Givehchi and Heidari [2018] ont ainsi évalué la probabilité de défaillance globale du système d'arrosage et retenu la valeur de $0,071$.

2.3.3 Réseau bayésien de l'arbre des défaillances du système d'arrosage

2.3.3.1 Notion de réseaux bayésiens

Le fondement des réseaux bayésiens s'appuie sur le théorème de Bayes, qui peut s'exprimer par les équations suivantes :

$$P(A|B)\,P(B) = P(A \cap B) = P(B|A)\,P(A] \tag{2.22}$$

où

- le terme P(A) est la probabilité a priori de A, appelée aussi probabilité marginale de A; elle est antérieure au sens qu'elle précède toute information sur B;
- le terme P(A|B) est appelée la probabilité a posteriori de A sachant B (ou encore de A sachant B). Elle est postérieure, au sens qu'elle dépend directement de B;
- le terme P(B|A), pour un B connu, est appelée la fonction de vraisemblance de A;
- le terme P(B) est appelé la probabilité marginale ou a priori de B.

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)} \tag{2.23}$$

Un réseau bayésien est un système représentant la connaissance et permettant de calculer des probabilités conditionnelles apportant des solutions à différentes sortes de problématiques. La structure de ce type de réseau est simple et comprend:

- un graphe acyclique orienté dans lequel les nœuds représentent des variables aléatoires et les arcs reliant ces dernières qui traduisent les relations entre variables qui sont soit déterministes, soit probabilistes. Ainsi, l'observation d'une ou plusieurs causes n'entraîne pas systématiquement l'effet ou les effets qui en dépendent, mais modifie seulement la probabilité de les observer;
- des tables des probabilités conditionnelless de chaque variable, chacune des variables dispose d'une table de probabilités conditionnelles relatives aux variables causales dont elle dépend.

L'inférence bayésienne est basée sur l'utilisation d'énoncés probabilistes, qui dans le cas général sont proposés par des experts étudiant le système. La clarté et la précision des dires d'experts sont importantes, afin d'éviter toute confusion dans les relations de dépendance qui en découleront. Les méthodes bayésiennes se distinguent des méthodes dites standard par l'application systématique de règles formelles de transformation des probabilités. On cherche à induire sur un système bayésien aussi bien par le haut que par le bas, aussi bien les conséquences que les causes, du graphe de dépendance. Les règles d'addition et de multiplication de la logique des probabilités utilisées sont respectivement les suivantes:

$$P(A \cup B|C) = P(A|C) + P(B|C) - P(A \cap B|C) \tag{2.24}$$

$$P(A \cap B) = P(A|B)\,P(B) = P(B|A)\,P(B) \tag{2.25}$$

Le théorème de Bayes peut être retrouvé simplement en mettant à profit la symétrie de la règle de multiplication

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)} \tag{2.26}$$

La puissance du théorème de Bayes permet d'inverser les probabilités. C'est-à-dire que si l'on connaît les conséquences d'une cause, l'observation des effets permet de remonter aux

causes, c'est l'effet d'induction du bas vers le haut. Une lecture littérale du théorème de Bayes permet aussi une induction du haut vers le bas, c'est à dire à partir des causes en déduire les conséquences. Mais il est aussi possible d'envisager de réfuter une cause en en constatant une autre, autrement dit partir d'une conséquence pour remonter aux causes, constater laquelle est vraie et réfuter les conséquences sous jacentes des autres causes. En résumé, pour induire sur un réseau bayésien, il faut en premier lieu trouver les probabilités conditionnelles de chaque variable aléatoire avec lesquelles elles sont directement dépendantes. Ce que les experts font à partir des statistiques étudiées sur le système voulu. Puis partir de faits produits auxquels on appliquera une probabilité de 1 ou 0 sur le réseau bayésien suivant qu'ils identifient une variable vraie ou fausse dans celui ci. Et enfin par le biais de calcul respectant la règle d'addition et ou de multiplication précédemment décrite, on modifie les probabilités causales et ou conséquentes. La nouvelle probabilité obtenue est l'induction que l'on peut faire sur un réseau bayésien. A titre d'exemple pédagogique, la partie droite de la figure 2.4 illustre le schéma de principe d'une procédure digitalisée d'inférence bayésienne. Il existe des logiciels pour traiter les algorithmes d'inférence comme par exemple Matlab `http://www.mathworks.fr/`, Bayesia `http://www.bayesia.fr` ou Hugin `http://www.hugin.com`.

2.3.3.2 Transposition d'un arbre des défaillances en réseau bayésien

Il est nécessaire de convertir l'arbre des défaillances en réseau bayésien. La partie gauche de la figure 2.4 montre la conversion d'une porte OU et d'une porte ET en nœuds équivalents dans la topologie bayésienne. Les nœuds parents A et B se voient attribuer des probabilités préalables coïncidant avec les valeurs de probabilité attribuées aux nœuds de base correspondants dans l'arbre des défaillancess et le nœud enfant C se voit attribuer sa table de probabilités conditionnelles. Étant donné que les portes OU et ET représentent des relations causales déterministes, toutes les entrées correspondantes de la table sont des valeurs 0 ou 1.

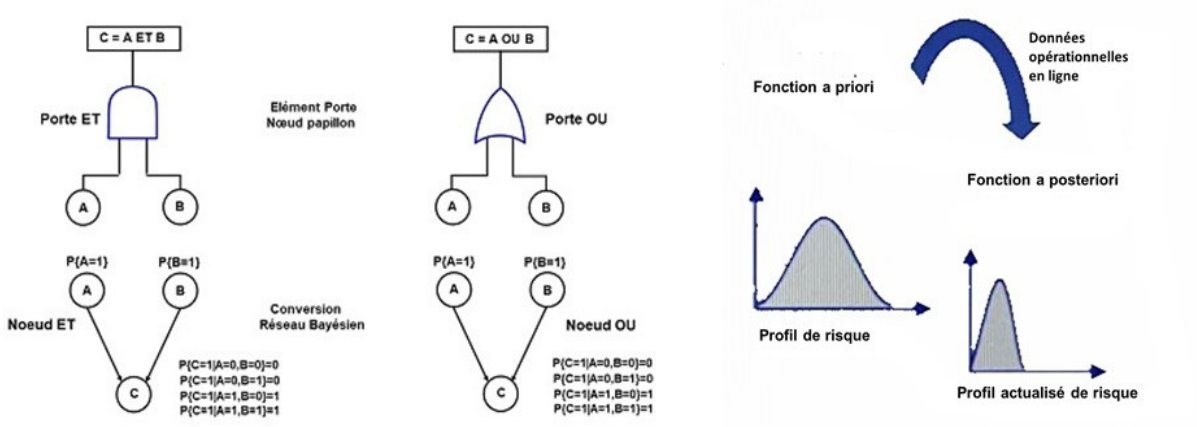

Figure 2.4: Représentations respectives des portes OU et ET dans l'arbre des défaillances et du réseau bayésien (partie gauche) et schéma de principe de l'inférence bayésienne (partie droite) - adapté d'après Bobbio et al. [2001] et Li et al. [2022] .

2.3.3.3 Analyse du réseau bayésien du système d'arrosage

Nous avons vu que la méthode du réseau bayésien, intégrant des informations sur la relation entre différents nœuds, peut créer une inférence bilatérale et générer des situations conditionnelles entre les nœuds d'entrée et de sortie. Il existe également des systèmes avec plusieurs modes de fonctionnement dans des exemples réels. Dans ce cas les données ne sont pas binaires (zéro et un) et l'arbre de défaillance n'est pas en mesure de traiter ces systèmes de fiabilité. Le réseau bayésien peut fournir des fonctions permettant de surmonter cette contrainte de l'arbre de défaillances. La structure de l'arbre des défaillances de la figure 2.3 est convertie en réseau de Bayes sur la figure 2.5.

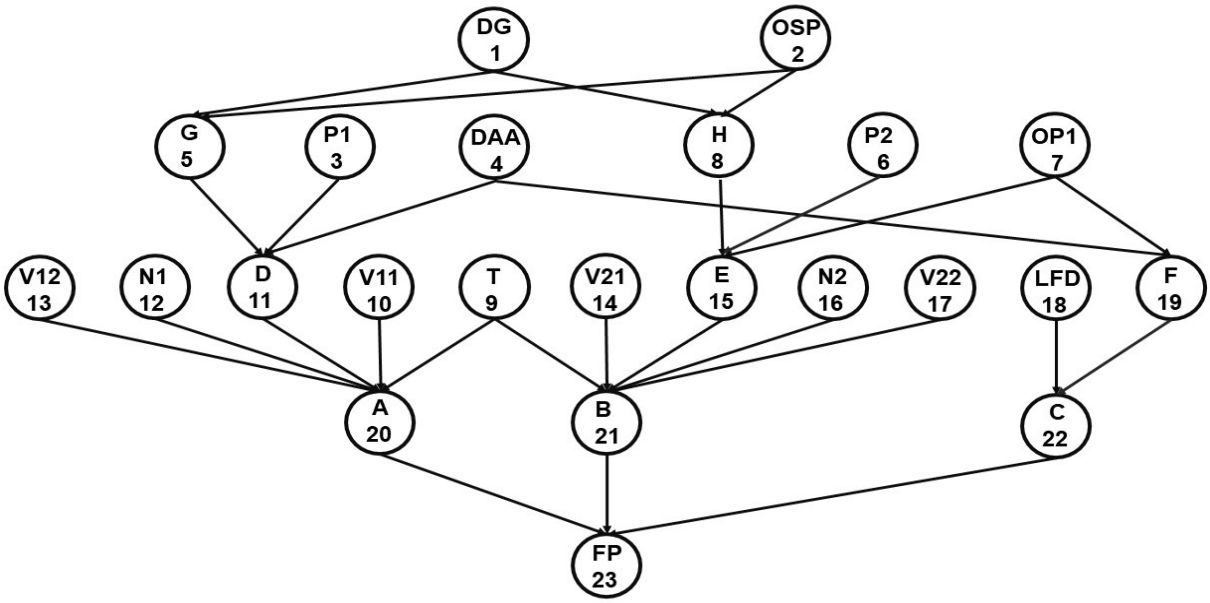

Figure 2.5: Réseau bayésien de l'installation d'extinction automatique d'incendie par sprinkler - adapté d'après Givehchi and Heidari [2018].

Le réseau bayésien obtenu comprend cinq couches:

- La première couche contient les nœuds 1 et 2, respectivement liés aux événements DG et OSP;
- La deuxième couche contient les nœuds 3 à 8; les nœuds 3, 4, 6 et 7 correspondent respectivement aux événements P1, DAA, P2 et OP1 et les nœuds 5 et 8 sont respectivement liés aux nœuds G et H;
- La troisième couche contient les nœuds 9 à 19, qui indiquent respectivement les événements T, V11, D, N1, V12, V21, E, N2, V22, LFD et F;
- La quatrième couche est liée aux événements A, B et C correspondant respectivement aux nœuds 20, 21 et 22;

- La cinquième couche est également liée à l'événement final FP, qui est repéré par le numéro 23.

Chacun des nœuds reliés les uns aux autres de la figure 2.5 possède ses propres informations de fiabilité. Pour mémoire, dans un arbre des défaillances les événements n'ont que deux états (succès et échec). Toutefois, dans la méthode du réseau bayésien pour certains événements, en plus des deux états mentionnés, il est possible de considérer un autre état, qui par exemple est lié au fait que le système fonctionne lentement. Il est évident que plus le nombre de nœuds éligibles est élevé, donc en conséquence le nombre d'états, plus les résultats seront précis. Ici quatre événements des états de fonctionnement lent ont également été ajoutés au système examiné. Ces événements sont liés aux pompes du système (P1 et P2), qui peuvent pomper l'eau vers les buses avec une pression inférieure à la pression standard en raison de problèmes de dysfonctionnement. De même, l'opérateur (OP1) et le service de lutte contre l'incendie (LFD) peuvent également avoir des retards dans l'envoi de messages ou d'actions pour éteindre l'incendie, puisqu'il s'agit de ressources humaines. Il n'est pas évident de trouver des valeurs des probabilités des défaillances pour ces événements. Par conséquent, certaines valeurs ont été supposées pour ces probabilités. Les relations entre les événements seront repérées par les états respectifs 1, 2 et 3. L'état 1 correspond à un moment où le système ne fonctionne pas. L'état 2 indique la condition dans laquelle le système fonctionne correctement. L'état 3 correspond au moment où le système fonctionne lentement (perturbation). Les tableaux 2.2 et 2.3 indiquent les valeurs des probabilités des défaillances des événements comportant respectivements deux et trois états de fonctionnement.

DG	p(DG)	OSP	p(OSP)	DAA	p(DAA)
1	$5,5 \times 10^{-2}$	1	$1,0 \times 10^{-4}$	1	$1,0 \times 10^{-4}$
2	$0,945$	2	$0,9999$	2	$0,9999$
T	p(T)	Nij	p(Nij)	Vij	p(Vij)
1	$1,0 \times 10^{-5}$	1	$1,0 \times 10^{-5}$	1	$4,2 \times 10^{-3}$
2	$0,99999$	2	$0,99999$	2	$0,9958$

Tableau 2.2: Probabilités de défaillances des événements comportant deux états du système d'extinction automatique par arrosage sprinkler - adapté d'après Givehchi and Heidari [2018]

P1, P2	p(P1,P2)	OP1	p(OP1)	LFD	p(LFD)
1	$0,017$	1	$1,0 \times 10^{-2}$	1	$1,0 \times 10^{-4}$
2	$0,6553$	2	$0,66$	2	$0,6666$
3	$0,3277$	3	$0,33$	3	$0,3333$

Tableau 2.3: Probabilités de défaillances des événements comportant trois états du système d'extinction automatique par arrosage sprinkler - adapté d'après Givehchi and Heidari [2018]

Pour mémoire, un nœud parent est un nœud qui a plusieurs arcs en direction d'autres nœuds. Un nœud enfant est un nœud connecté à d'autres nœuds par des arcs entrants. Un nœud sans parent

est désigné nœud racine. Pour chaque nœud racine, il existe une distribution de probabilité marginale, qui présente toutes les conditions possibles pour ce nœud et ses probabilités. Il existe une distribution de probabilité conditionnelle pour les autres nœuds enfants, utilisée pour décrire la distribution des probabilités en fonction des nœuds parents. Givehchi and Heidari [2018] ont utilisé un logiciel spécifique d'outil bayésien développé dans MATLAB pour créer le réseau de Bayes du système d'extinction automatique d'incendie. Ici les principales fonctions ont été utilisées à l'aide des algorithmes dédiés pour créer le graphique du réseau de Bayes, attribuer la distribution de probabilité conditionnelle et calculer les inférences du réseau de Bayes. Ces auteurs rapportent une valeur de la probabilité de défaillance du système global de $0,11$ plus pénalisante que le résultat de la méthode classique de l'arbre des défaillances. L'apport du réseau bayésien intègre de façon plus représentative les dysfonctionnements des divers composants, en particulier celui très prépondérant du générateur diesel (DG).

2.4 Application de la logique floue à l'analyse d'un arbre des défaillances d'une station GPL de rechargement

L'objectif de la section 2.4 est de présenter d'abord l'essentiel d'une revue du concept et de l'application d'un arbre flou des défaillances. La méthodologie du cadre d'analyse d'un arbre flou des défaillances est ensuite discutée. Après la description d'une station GPL de rechargement, la procédure des étapes de l'analyse de l'arbre flou des défaillances est appliquée et commentée.

2.4.1 Quelques principes fondamentaux de la théorie floue

La logique floue facilite la modélisation d'un raisonnement logique opéré sur des propositions vagues ou imprécises. Contrairement à la logique classique opérant sur deux valeurs de vérité (vrai et faux), la logique floue permet d'effectuer des inférences à partir de prémisses n'étant ni vraies, ni fausses, mais possédant un certain degré de vérité. La logique floue permet ainsi de faire le lien entre la modélisation numérique et la modélisation symbolique à partir d'algorithmes de traduction des connaissances et d'informations subjectives, imprécises, vagues ou incertaines, ce qui rend possible entre autres le traitement original de l'incertitude.
Mahmood et al. [2013] ont présenté une revue de la théorie floue appliquée à l'analyse de l'arbre flou des défaillances, en faisant le point sur l'état actuel des méthodologies d'analyse d'un arbre flou des défaillances, leurs forces, leurs faiblesses et leurs potentialités application. Il est utile de reprendre, pour la compréhension du cas traité, quelques principes fondamentaux de la logique floue.

2.4.1.1 Notion de nombre flou

Un nombre flou décrit la relation entre une quantité incertaine x (par exemple, la probabilité d'un événement) et une fonction d'appartenance $\mu_m(x)$, qui varie entre 0 et 1. Un ensemble flou dans l'espace de probabilité représente un nombre flou entre zéro et un, qui peut être attribué

à la probabilité d'un événement. Il existe de nombreuses formes de nombres flous. Le nombre flou triangulaire (TFN) et le nombre flou trapézoïdal (TZFN) sont couramment utilisés.
La partie (a) de la figure 2.6 illustre respectivement les fonctions d'appartenance des nombres flous triangulaire et trapézoïdal.

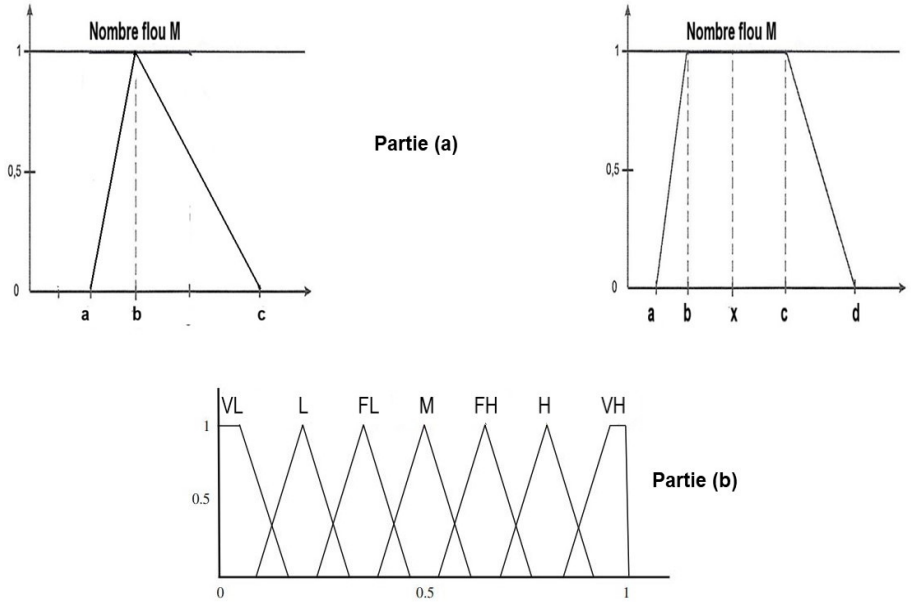

Figure 2.6: Fonctions d'appartenance des nombres flous triangulaire et trapézoïdal (partie a) et exemple d'expression de variables linguistiques (partie b) - adapté d'après Mahmood et al. [2013].

La fonction d'appartenance d'un nombre flou triangulaire m(a,b,c) est définie par l'équation:

$$\mu_m(x) = \begin{vmatrix} \frac{(x-a)}{(b-a)} & a \leq x \leq b \\ \frac{(c-x)}{(c-b)} & a \leq x \leq b \\ 0 & - \end{vmatrix}$$

La fonction d'appartenance d'un nombre flou trapézoïdal m(a,b,c,d) est définie par l'équation:

$$\mu_m(x) = \begin{vmatrix} \frac{(x-a)}{(b-a)} & a \leq x \leq b \\ 1 & b \leq x \leq c \\ \frac{(c-x)}{(c-b)} & c \leq x \leq d \\ 0 & - \end{vmatrix}$$

2.4.1.2 Expressions de variables linguistiques

Le concept de variable linguistique est très utile pour traiter des situations qui sont trop complexes ou trop mal définies pour être raisonnablement décrites par des expressions quantitatives conventionnelles. En effet, les méthodes mathématiques conventionnelles ne peuvent pas

traiter efficacement les expressions linguistiques naturelles. L'introduction de la théorie des ensembles flous permet d'y faire face en transformant ces termes linguistiques en représentations graphiques ou mathématiques. Il a été proposé de combiner l'élicitation d'experts et les théories des ensembles flous afin d'évaluer la probabilité des événements à l'aide de variables linguistiques.
Les variables linguistiques sont des variables dont les valeurs sont décrites par des mots ou des phrases dans une langue naturelle ou synthétique. Par exemple, la probabilité des défaillances d'un procédé peut être une variable linguistique dont les valeurs résultent de l'ensemble de termes: très faible (VL), faible (L), assez faible (FL), moyenne (M), assez élevée (FH), élevée (H) et très élevée (VH). La partie (b) de la figure 2.6 montre un exemple d'ensemble flou dont les membres sont les probabilités de défaillance en tant que variables linguistiques.

2.4.1.3 Opérateurs de logique floue

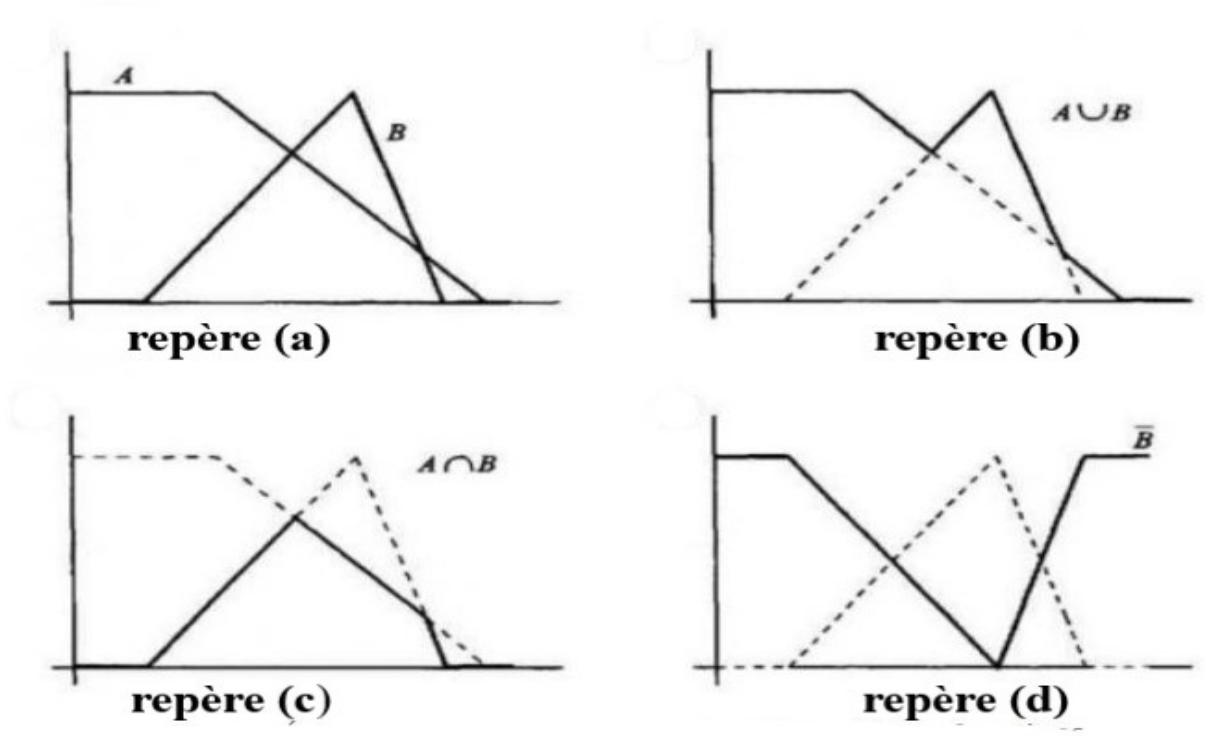

Figure 2.7: Illustration schématique des opérations d'union, d'intersection et de complément des fonctions d'appartenance de deux ensembles flous.

Les opérateurs de logique floue permettent d'écrire des combinaisons logiques entre des notions floues, c'est-à-dire d'effectuer des calculs sur des degrés de vérité.
L'opérateur logique correspondant à l'intersection de deux ensembles M_1 et M_2 est

$$M_1 \cap M_2$$

. Considérons par exemple les deux nombres flous triangulaires exprimés respectivement par (a_1, b_1, c_1) et (a_2, b_2, c_2). Si les événements sont indépendants, l'opérateur flou d'intersection s'écrit:

$$M_1 \cap M_2 = \prod_{i=1}^{n} M_i = \left[\prod_{i=1}^{n} a_i, \prod_{i=1}^{n} b_i, \prod_{i=1}^{n} c_i\right] \tag{2.27}$$

Si les événements sont dépendants, comme c'est souvent le cas, l'expression de l'opérateur est:

$$M_1 \cap M_2 = min\left[M_1, M_2, ..., M_n\right] \tag{2.28}$$

$$\mu\left[M_1 \cap M_2\right] = min\left[\mu(M_1), \mu(M_2)\right] \tag{2.29}$$

L'opérateur logique correspondant à l'union de deux ensembles M_1 et M_2 est

$$M_1 \cup M_2$$

s'écrit pour l'exemple précédent:

$$M_1 \cup M_2 = 1 - \prod_{i=1}^{n} (1 - M_i) = \left[1 - \prod_{i=1}^{n} (1 - a_i), \prod_{i=1}^{n} (1 - b_i), \prod_{i=1}^{n} (1 - c_i)\right] \tag{2.30}$$

$$M_1 \cup M_2 = max\left[M_1, M_2, ..., M_n\right] \tag{2.31}$$

$$\mu\left[M_1 \cup M_2\right] = max\left[\mu(M_1), \mu(M_2)\right] \tag{2.32}$$

La figure 2.7 illustre schématiquement, à partir de fonctions d'appartenance des ensembles flous A et B (repère a), les opérations d'union (repère b), d'intersection (repère c) et de complément $\overline{B}$ (repère d).

2.4.2 Cadre d'analyse de l'arbre flou des défaillances

La figure 2.8 présente le cadre d'analyse d'un arbre flou des défaillances proposé par Rajakarunakaran et al. [2015]. Le logigramme proposé dans cette figure comporte les neuf étapes différentes suivantes:

- Etape 1: Élaboration de l'arbre des défaillances par l'analyse systématique de la logique et des causes fondamentales;
- Etape 2: Évaluation par des experts du domaine des événements de base en termes linguistiques;
- Etape 3: Fuzzification des jugements des experts du domaine, c'est-à-dire conversion en nombres flous;
- Etape 4: Elicitation et agrégation des jugements du groupe d'experts en un résultat de consensus;

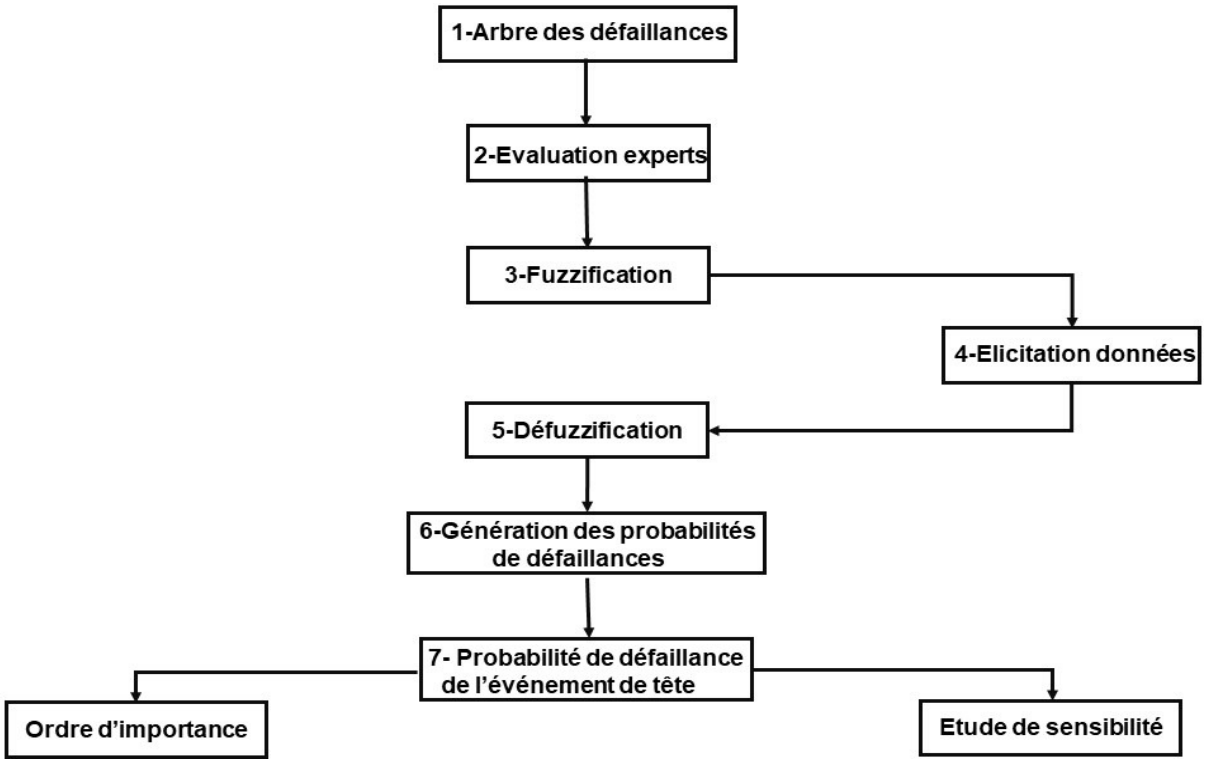

Figure 2.8: Cadre d'analyse d'un arbre flou des défaillances - adapté d'après Rajakarunakaran et al. [2015].

- Etape 5: Défuzzification des jugements flous des experts, c'est-à-dire conversion des résultats flous en un score net;
- Etape 6: Génération de la probabilité de défaillance des événements par transformation du score net en probabilité;
- Etape 7: Calcul de la probabilité de défaillance des coupes et de la probabilité de défaillance de l'événement de tête;
- Etape 8: Classement de l'importance pour obtenir l'ordre d'importance des jeux de coupe;
- Etape 9: Analyse de sensibilité pour identifier la sensibilité de l'événement de tête.

Le descriptif de chacune des étapes est détaillé dans l'article de Rajakarunakaran et al. [2015]. Nous limiterons l'application du logigramme dans l'étude de cas proposée aux étapes 1 à 7.

2.4.3 Description de la station GPL de rechargement

La figure 2.9 présente le réservoir horizontal aérien de stockage de GPL avec le système de distributeur de la station service implantée en milieu urbain.

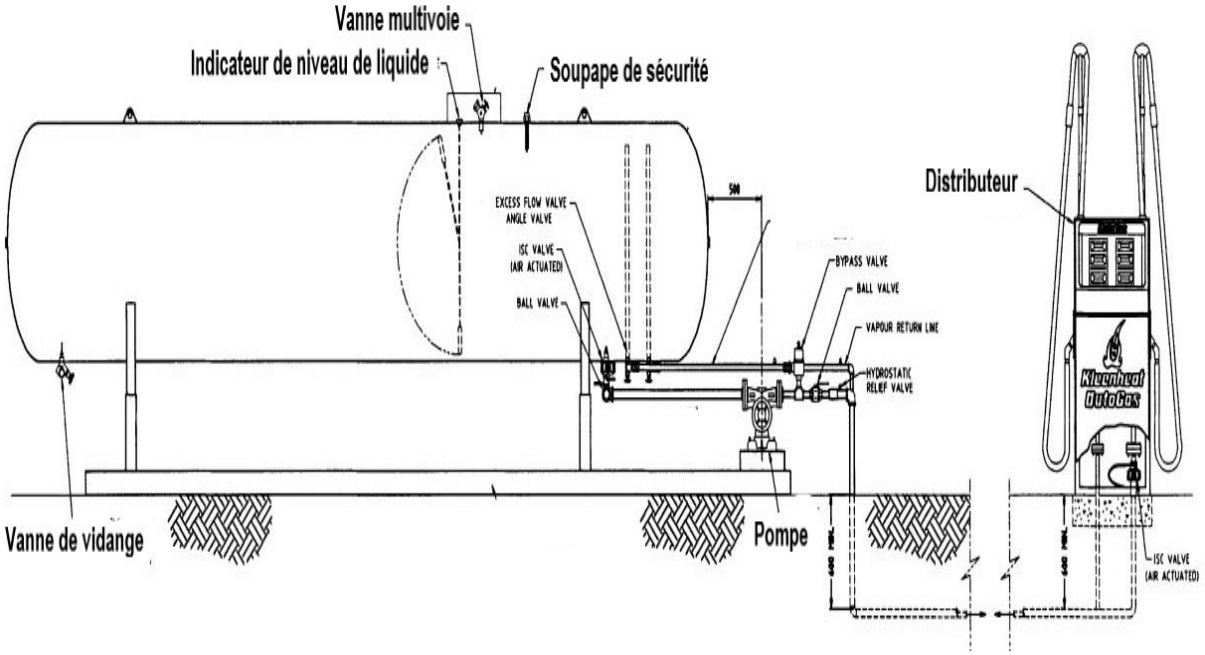

Figure 2.9: Schéma du réservoir de stockage de GPL et du système de distributeur - adapté d'après Melchers and Feutrill [2001].

Le réservoir est alimenté par des camions citernes. Le réservoir est rempli régulièrement, généralement environ 120 fois par an, mais avec des variations considérables. Compte tenu du rythme des prélèvements et des remplissages, le risque de rupture par fatigue de la paroi du réservoir est négligeable. Le dépotage est effectué par des flexibles en caoutchouc de haute qualité. Cette opération comporte un risque connu, considéré comme faible, lié à la réalisation et à l'entretien de l'accouplement, au débrayage de la pompe et au protocole approprié de désaccouplement. Un système d'arrêt d'urgence peut être activé depuis la console de l'opérateur pour couper l'alimentation électrique de la pompe et libérer la vanne d'arrêt automatique interrompant l'approvisionnement en GPL. Au cours d'une opération normale, le contenu du réservoir est progressivement vidé au fur et à mesure que le carburant est vendu. L'expérience opérationnelle montre que le réservoir reste dans un état interne très propre pendant de nombreuses années et que la corrosion interne est négligeable. Pour éviter qu'un camion citerne redémarre après dépotage avant que les flexibles soient débranchés, un dispositif de verrouillage est monté en série sur chaque camion citerne. La présence et l'emplacement d'un camion citerne sur le site de la station service en milieu urbain constituent un élément perturbateur et présentent un danger, à la fois en termes d'impact du camion citerne avec d'autres véhicules que pour l'installation et son équipement.

2.4.4 Application de la procédure des étapes de l'analyse de l'arbre flou des défaillances

2.4.4.1 Développement de l'arbre classique des défaillances

Les principaux scénarios de l'analyse des risques d'une station de stockage et de distribution de GPL sont classiquement:

- le BLEVE (Boiling Liquid Expanding Vapour Explosion);
- l'explosion non confinée d'un nuage de vapeurs;
- le feu flash;
- le feu torche.

Les événements initiateurs de ces scénarios dangereux dans l'étude de cas considérée peuvent être:

- la défaillance de la structure métallique du réservoir de stockage du GPL;
- l'implication de la présence d'une flamme;
- l'impact avec des véhicules;
- l'absence de prudence des conducteurs des camions citernes et de l'opérateur lors des opérations de dépotage;
- le vandalisme.

Rajakarunakaran et al. [2015] ont ainsi recensé 16 événements initiateurs comportant les diverses défaillances potentielles, comme celles du flexible de transfert du GPL, de l'enrouleur du flexible, du réservoir de stockage, de la vanne de vidange, de la soupape de sécurité, de la ligne de retour des vapeurs, de la ligne de sortie du liquide, de la buse du distributeur, de l'impact des véhicules et de l'action négligente des conducteurs et de l'opérateur. Le tableau 2.4 récapitule les événements de base et leurs probabilités suggérées par les dires d'experts.
La figure 2.10 présente l'arbre classique des défaillances du système de stockage et distribution GPL.

2.4.4.2 Evaluation des experts

Les probabilités des événements initiateurs de base ont été estimées à partir des dires d'experts de deux groupes d'experts comportant chacun six experts. Un groupe est composé d'experts qualifiés du domaine des hydrocarbures combustibles. L'autre groupe est formé d'experts sélectionnés dans des domaines variés, tels que la conception, l'installation, la maintenance, l'exploitation et la gestion des procédés. Ce choix volontaire de deux groupes très différents est guidé par le souci de Rajakarunakaran et al. [2015] de déterminer si l'approche proposée

Repère	Descriptif (défaillance)	Probabilité de défaillance
B1	Raccord flexible (faible)	$0,024$
B2	Enrouleur flexible (moyen)	$3,46 \times 10^{-6}$
B3	Remplissage excessif, surpression camion citerne	$1,0 \times 10^{-4}$
B4	Soupape de sécurité camion citerne	$0,19 \times 10^{-6}$
B5	Vanne de vidange (faible)	$1,7 \times 10^{-4}$
B6	Remplissage excessif, surpression réservoir de stockage	$1,0 \times 10^{-4}$
B7	Soupape de sécurité du réservoir	$0,53 \times 10^{-6}$
B8	Ligne retour vapeur (faible)	$1,0 \times 10^{-3}$
B9	Fuite ligne sortie liquide (faible)	$5,0 \times 10^{-6}$
B10	Fuite ligne sortie liquide (moyen)	$2,3 \times 10^{-6}$
B11	Fuite ligne sortie liquide (fort)	$0,56 \times 10^{-6}$
B12	Impact véhicule (faible)	$4,5 \times 10^{-6}$
B13	Impact véhicule (fort)	$2,43 \times 10^{-6}$
B14	Buse distributeur (faible)	$2,0 \times 10^{-4}$
B15	Camion citerne en démarrage (faible)	$6,67 \times 10^{-4}$
B16	Impact véhicule (tuyau ou distributeur)	$6,67 \times 10^{-4}$

Tableau 2.4: Récapitulatif descriptif des événements initiateurs et de leurs probabilités de défaillances du système de stockage et de distribution du GPL - adapté d'après Rajakarunakaran et al. [2015]

permettrait de tenir compte des opinions très variées des experts. Les données ainsi obtenues nécessitent une élicitation pondérant la qualité relative de chaque expert en fonction de sa position professionnelle, de son expérience et de sa qualification universitaire initiale et conciliant les termes linguistiques qualitatifs.

2.4.4.3 Fuzzification

L'opération de fuzzification permet de passer du domaine réel au domaine flou. Elle consiste à transformer une valeur numérique précise (crisp) en degré d'appartenance flou (ou degré de vérité) par évaluation d'une fonction d'appartenance.
Rajakarunakaran et al. [2015] ont montré que les fonctions d'appartenance des nombres flous triangulaires et trapézoïdaux permettaient bien de représenter des événements à faible probabilité de défaillance (par exemple 10^{-7}) et à forte probabilité de défaillance (par exemple 10^{-2}). A titre d'exemple, le tableau 2.5 indique que les fonctions d'appartenance des nombres flous triangulaires décrivent correctement les potentialités des défaillances linguistiques qualitatives.

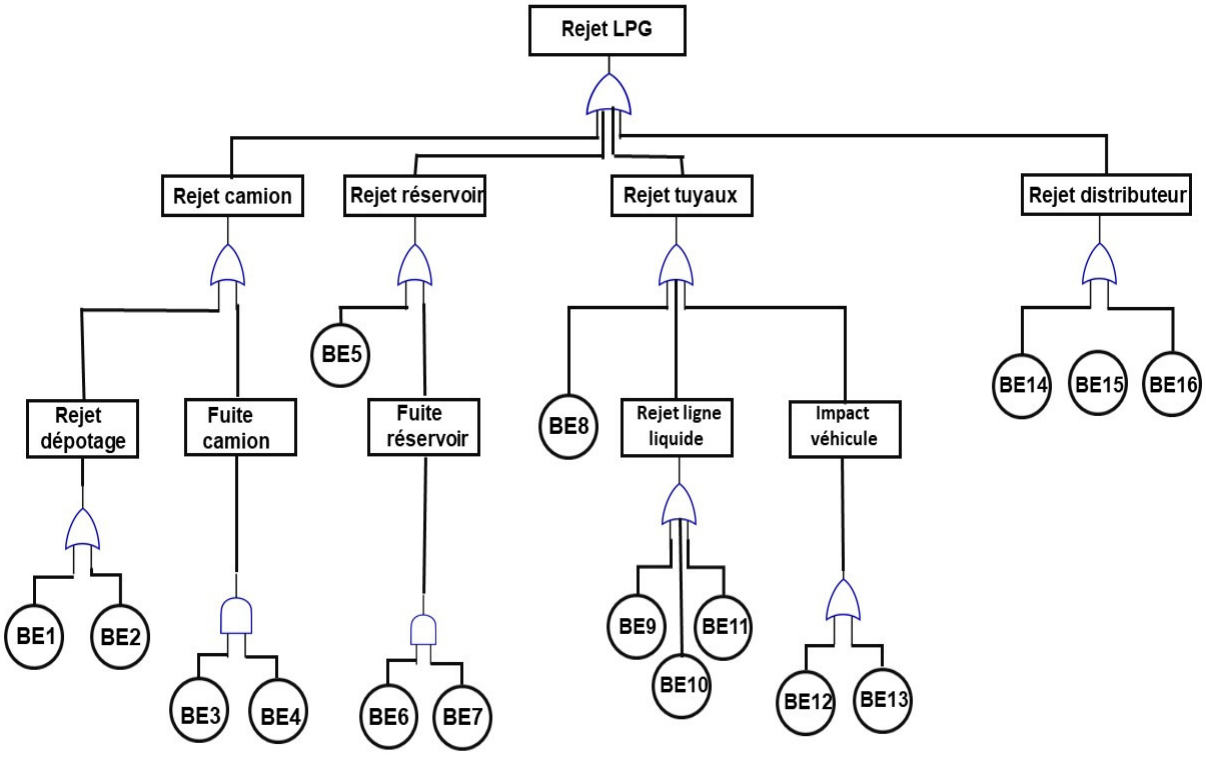

Figure 2.10: Arbre classique des défaillances du système GPL de stockage et distribtion - adapté d'après Rajakarunakaran et al. [2015].

2.4.4.4 Agrégation des données

L'étape d'agrégation élicitation a pour objet de générer à l'aide d'algorithmes dédiés un consensus pour chaque événement de base sur une valeur finale à partir des évaluations subjectives des experts.

2.4.4.5 Défuzzification

La défuzzification consiste à transformer, après inférence, un ensemble flou d'une variable de sortie en une valeur numérique pertinente (crisp). Afin de déterminer la relation entre les deux, le nombre flou doit être converti en un score précis, appelé score de possibilité floue (FPS). Les scores flous de possibilité de défaillance d'un événement de base sont générés à partir de leur fonction d'appartenance finale obtenue lors de l'étape d'agrégation des avis d'experts. Le score de possibilité floue représente la probabilité la plus élevée qu'un expert croit en l'occurrence d'un événement de base. Il est très important de choisir une technique de défuzzification adaptée à une application spécifique. Rajakarunakaran et al. [2015] ont sélectionné ici la technique de défuzzification du centre de gravité pour ce travail. Pour une représentation par un nombre flou

Echelle linguistique	Nombre flou triangulaire		
	a	b	c
VL	0	$0,04$	$0,08$
L	$0,07$	$0,13$	$0,19$
FL	$0,17$	$0,27$	$0,37$
M	$0,35$	$0,5$	$0,65$
FH	$0,63$	$0,73$	$0,83$
H	$0,81$	$0,87$	$0,93$
VH	$0,92$	$0,96$	1

Tableau 2.5: Exemple de conversion des variables linguistiques qualitatives en nombres flous triangulaires (a, b, c) - adapté d'après Rajakarunakaran et al. [2015].

triangulaire, le score de possibilité floue FPS s'écrit:

$$FPS = \frac{\int \mu_i(x) x dx}{\int \mu_i(x)} = \frac{1}{3}(a+b+c) \tag{2.33}$$

2.4.4.6 Génération des probabilités des défaillances

Cette étape génère des probabilités de défaillance d'événements de base à partir de leurs scores de possibilité de défaillance correspondants, issus du processus de défuzzification.

2.4.4.7 Probabilité de défaillance de l'événement de tête

Les probabilités d'occurrence de la défaillance de l'événement de tête indésirable évaluées séparément, classiquement et par logique floue, sont comparées dans le tableau 2.6.

Evaluation	Experts	Probabilité
classique	-	$2,7 \times 10^{-2}$
floue	Groupe I	$4,8 \times 10^{-2}$
floue	Groupe II	$2,3 \times 10^{-2}$

Tableau 2.6: Comparaison des probabilités de défaillance de l'élément de tête - adapté d'après Rajakarunakaran et al. [2015].

L'augmentation observée de la probabilité de défaillance de l'événement de tête par le groupe I illustre l'impact des incertitudes prises en compte par l'évaluation qualitative des experts par le biais de la logique floue impliquée dans ce processus. Il s'avère que la différence importante de valeur de la probabilité de l'événement de tête résultant de l'évaluation du groupe II peut s'expliquer par le défaut d'expertise de l'équipe. Bien qu'en terme d'ordre de grandeur la différence des résultats ne soit pas très prononcée, la capacité de l'approche par logique floue

à gérer les incertitudes et la précision reste intéressante en raison du manque de qualité des données génériques d'entrée.

Pour aller plus loin
- Evaluation du risque d'une unité de filtration par charbon actif d'effluents VOC et VX (agent inervant organophosphoré) par arbre conventionnel et par approche floue des défaillances.
Documentation: Wang et al. [2005] - Ferdous [2006]

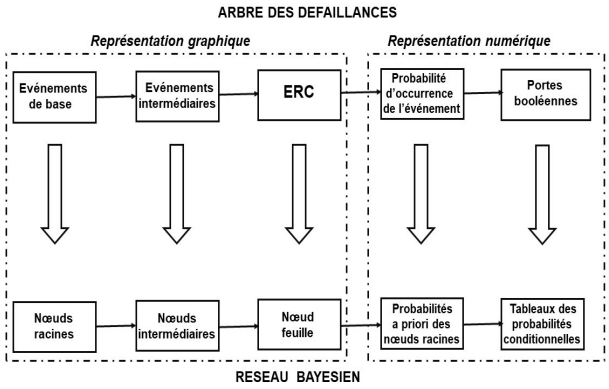

Figure 2.11: Transposition d'un arbre des défaillances en réseau bayésien - adapté d'après Khakzad et al. [2011].

- Approches comparatives d'un arbre des défaillances et de sa transposition en réseau bayésien - Application au contrôle du débit d'alimentation d'une colonne d'abattement de propane gazeux.
Documentation: Khakzad et al. [2011]
- Approche dynamique de l'analyse d'un arbre des défaillance par un réseau bayésien: application à un stockage côtier pétrochimique.
Documentation: Vairo et al. [2019]

Chapitre 3

Approche dynamique quantifiée de la méthode de l'arbre des événements

3.1 Rappel de la méthode classique de l'arbre des événements

La méthode de l'arbre des événements a pour objet d'analyser l'évolution d'un système en décrivant les différentes conséquences résultant d'un événement initiateur fixé a priori. Cette méthode procède d'une démarche inductive en progressant des causes vers les effets, c'est-à-dire dans le sens de déroulement du temps.
Le principe de la méthode de l'arbre des événements consiste d'abord à définir un événement initiateur comme une défaillance d'un élément, d'un composant ou d'un sous-système, comme une perturbation de l'environnement (foudre, gel, tremblement de terre...) ou comme une intervention humaine non prévue. On étudie ensuite la propagation et la combinaison des événements consécutifs ultérieurs, en particulier celles des défaillances du système, pouvant conduire à des conséquences indésirables. Cette phase d'analyse de l'évolution du système doit prendre en compte le fonctionnement ou non des moyens de prévention, de compensation, d'alarme et de sécurité incluant les dispositifs automatiques, le rôle des opérateurs, l'application des procédures et l'intervention des secours [Laurent, 2011]. La méthode se traduit par la construction d'un arbre séquentiel des événements susceptibles de se produire dans le système en aval de l'événement inititiateur ou cause initiale.
L'application de la méthode conduit à l'élaboration d'un arbre logique dont les arborescences se développent à chaque étape en deux cheminements possibles. Habituellement l'événement initiateur (cause) est placé à gauche. L'arbre est ensuite développé de la gauche vers la droite avec la convention de considérer la branche supérieure de chaque alternative comme représentant la réussite de fonctionnement et donc le cheminement inférieur comme l'échec de fonctionnement du dispositif ou de la procédure examiné. A priori, l'arbre des événements présente donc un développement symétrique, c'est-à-dire que le fonctionnement et le non-fonctionnement des dispositifs respectivement présents à chaque étape doivent être systématiquement considérés dans chacune des branches de l'arbre. Théoriquement, pour un système donné, la présence de n dispositifs ou procédures ayant pour objet de s'opposer à la propagation de la défaillance initiale vers l'accident (conséquence) conduit à l'élaboration d'un arbre comportant au maximum

2^n cheminements (ou aussi en considérant m séquences avec la séquence initiale au maximum 2^{m-1} cheminements). En pratique, certaines branches ne demandent pas à être développées parce que les conséquences bonnes ou mauvaise ne dépendent plus de la réussite ou de l'échec de fonctionnement des autres dispositifs.
L'examen qualitatif de la structure d'un arbre des événements permet une première appréciation de la robustesse de la sécurité du système. En effet, un arbre des événements, qui présente des cheminements traduisant la non réussite de fonctionnement et ne passant que par une branche inférieure, constitue un indicateur de la fragilité du système étudié.
Il est possible de quantifier l'arbre des événements en affectant à chacun des événements pris en compte une probabilité. Comme chaque étape de l'arbre comporte deux alternatives possibles respectives de succès et d'échec, il est recommandé d'adopter les notations i pour la probabilité de succès de l'événement I (branche supérieure) et $\bar{i}$ pour la probalité d'échec du même événement I en remarquant que $\bar{i} = 1 - i$. La quantification effective dépend alors beaucoup de la nature des dépendances entre les événements constitués par l'événement initiateur et les événements génériques des conséquences. Dans le cas simple où tous les événements sont indépendants entre eux, la probabilité de la conséquence d'une extrémité de branche de chaque séquence est alors égale de manière approchée au produit des probabilités des cheminements alternatifs suivis pour y parvenir.
Pour faciliter la construction d'un arbre des événements, Vilchez et al. [2011] ont proposé de manière systématique une série d'arbres génériques quantifiés pour les principaux scénarios de perte de confinement impliquant différents types de substances dangereuses. A titre d'exemple, la figure 3.1 présente l'arbre des événements d'un rejet diphasique continu d'un gaz liquéfié sous pression et extrêmement inflammable.

3.2 Application d'un arbre quantifié dynamique des événements à la conduite d'un réacteur discontinu

Plusieurs outils d'arbres dynamiques des événements (DET) sont recensés dans la littérature [Karanki et al., 2018]. Quelques différences existent entre ces outils DET, qui sont apparues lors de l'examen des complexités de la quantification du risque, comme par exemple avec les variables continues, les dépendances du système de gestion, etc. Selon la manière dont les variables aléatoires continues sont traitées dans les simulations DET les méthodologies/outils DET peuvent être classés en deux méthodes distinctes, à savoir l'approche DET discrète et l'approche DET par échantillonnage. La principale différence réside dans le fait que les variables aléatoires continues (par exemple, le temps de récupération, le temps de réponse de l'opérateur, le temps de défaillance de l'équipement, etc.) sont discrétisées dans l'approche DET discrète, tandis que les mêmes variables sont échantillonnées dans l'approche par simulation de Monte Carlo.
L'exemple proposé compare ces approches DET dans l'analyse d'un problème de réacteur chimique discontinu en montrant l'impact sur la précision des résultats finaux, lorsque de nombreuses variables continues sont présentes dans les séquences d'accidents, tant en termes de fréquence de défaillance du procédé que de contributions de divers événements initiateurs au risque d'emballement du procédé.

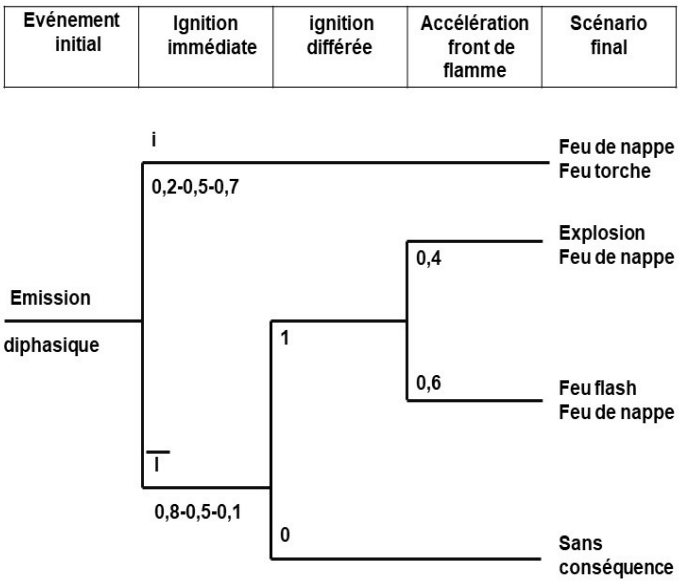

Figure 3.1: Exemple d'arbre générique quantifié des événements - d'après Vilchez et al. [2011].

3.2.1 Description du réacteur fermé discontinu (batch)

Le réacteur fermé discontinu, de 2 m^3 de volume avec un taux de remplissage par charge de 80%, est schématisé sur la figure 3.2. La partie (a) de la figure 3.2 présente un schéma simplifié du système de réacteur chimique discontinu avec jaquette. Le système chimique réactionnel exothermique, mis en œuvre pendant une durée de 240 minutes, est constitué par deux réactions parallèles très exothermiques :

$$\mathrm{A} + \mathrm{B} \xrightarrow{k_1} \mathrm{C} \tag{3.1}$$

$$\mathrm{A} + \mathrm{C} \xrightarrow{k_2} \mathrm{D} \tag{3.2}$$

où A et B sont les réactifs, C le produit désiré, D le produit parasite indésirable, k_1 et k_2 les constantes cinétiques respectives.
D'une part le réacteur est équipé d'un système de contrôle de la température (TCS), dont la fonction est d'agir comme un dissipateur de chaleur via la jaquette du réacteur en maintenant la masse réactionnelle à une température constante de 71° C. D'autre part, un système de refroidissement d'urgence (ECS) permet en cas de défaillance due à la perte totale de débit de refroidissement ou de divergence par rapport aux conditions opératoires normales du réacteur d'éviter un emballement thermique par perte de contrôle de la température du réacteur.
La partie (b) de la figure 3.2 regroupe schématiquement les différents éléments de protection du réacteur instrumenté.

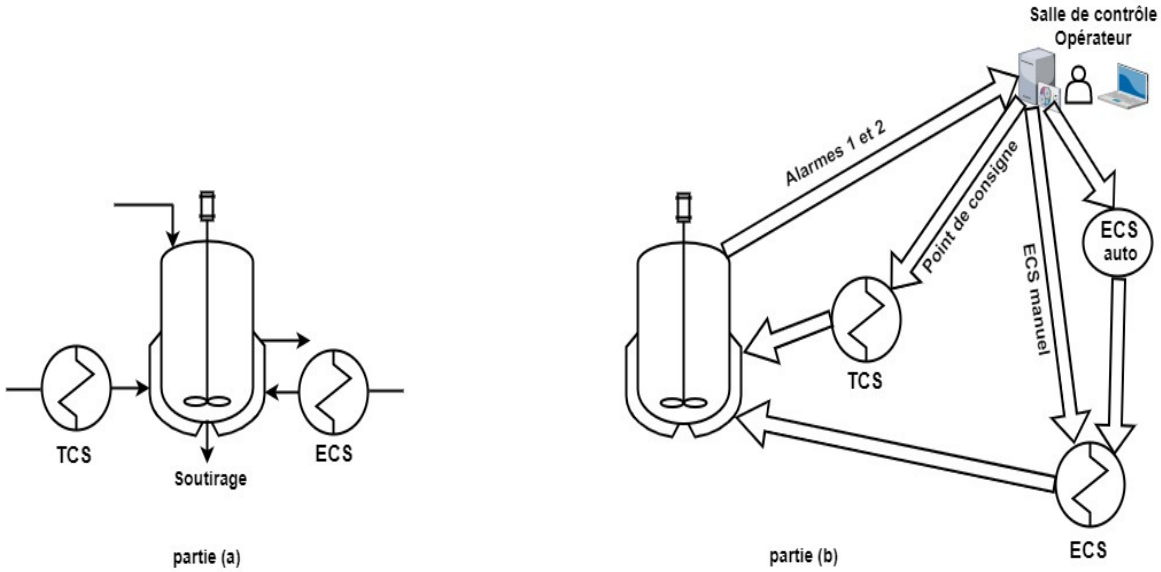

Figure 3.2: Schéma de principe du réacteur fermé discontinu - adapté d'après Podofillini and Dang [2012].

En fonctionnement normal du réacteur, le TCS commence par transférer la chaleur au réacteur par l'intermédiaire de la jaquette à l'aide d'un échangeur de chaleur, ce qui déclenche l'allumage de la réaction exothermique. Ensuite durant la phase de refroidissement, le TCS refroidit le réacteur lorsque la température de l'enveloppe atteint 71° C. En fonctionnement dégradé du réacteur, les différentes mesures de sécurité comportent deux alarmes 1 et 2, le système de refroidissement d'urgence ECS et la présence de l'opérateur de quart en salle de contrôle. Deux scénarios types ont été examinés :

- évolution transitoire due à une variation de la température initiale T dans le réacteur sans perte du fluide de refroidissement;
- évolution de la température T simultanément à la perte totale du fluide de refroidissement.

La figure 3.3 illustre les arbres des événements de deux scénarios étudiés.
Par exemple, pour l'arbre repéré (a), l'alarme 1 est activée lorsque la température T de la masse réactionnelle atteint 90° C dans les premières 70 minutes. La bonne pratique de l'opérateur consiste à réduire la température de consigne du système TCS à la valeur de 40° C. En cas d'échec, pour une température $T \geq 105^\circ$ C, le système de refroidissement d'urgence ECS devrait démarrer automatiquement pour alimenter la jaquette du réacteur avec de l'eau à 20° C. En cas d'échec, l'alarme 2 est activée. L'opérateur a pour consigne de démarrer manuellement

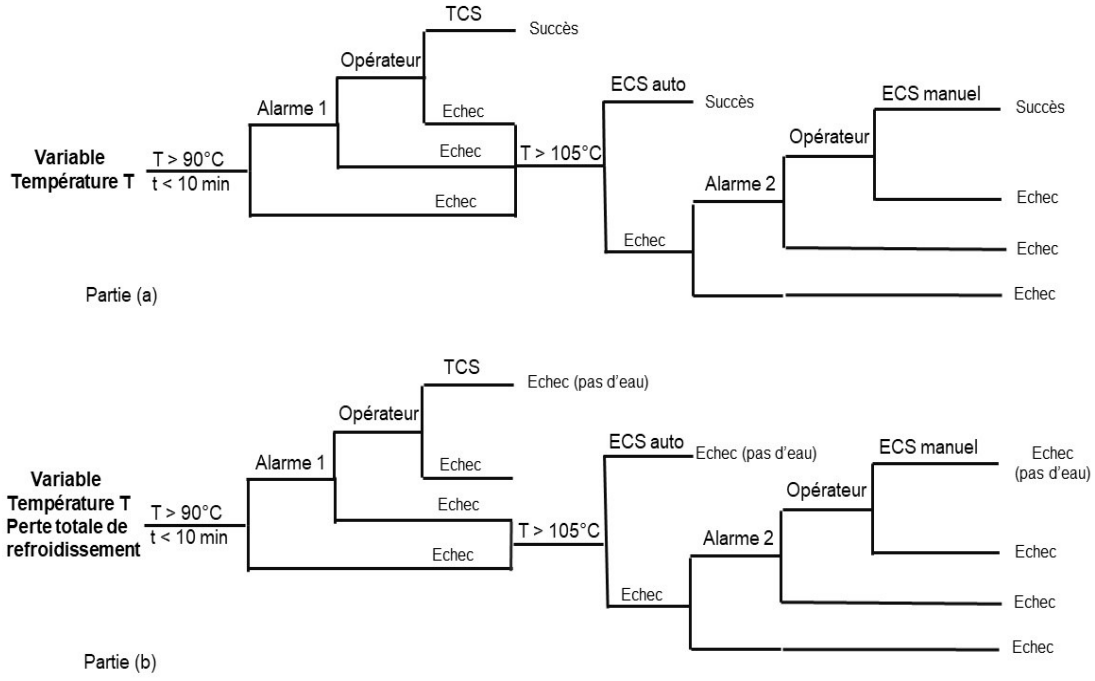

Figure 3.3: Arbre des évéments des scénarios accidentels du réacteur discontinu - adapté d'après Karanki et al. [2018].

le système d'urgence ECS. Il a été considéré, à la suite de l'alarme, que le comportement de l'intervention effective de l'opérateur intégrait sa décision d'agir et celle de son exécution.

3.2.2 Etude de la dynamique du comportement d'une charge du réacteur discontinu

3.2.2.1 Conditions de l'étude

Le tableau 3.1 récapitule les caractéristiques des distributions gaussiennes (moyenne et écart type) des paramètres initiaux du procédé batch, tels que les charges molaires respectives des réactifs A et B, la température de la masse réactionnelle, le débit volumique de refroidissement dans la jaquette et la température de consigne de fonctionnement du réacteur.
Les événements initiateurs de base identifiés et leurs fréquences ou probabilités issues des tables de donnés ou des dires d'experts sont listés dans le tableau 3.2.
La quantification de la fréquence / probabilité des événements du procédé implique de quantifier la fréquence / probabilité des combinaisons des valeurs des paramètres qui conduisent aux événements finaux étudiés. La méthode des distributions de probabilités discrètes est d'abord adoptée. L'idée est d'approximer la fonction de densité de probabilité continue de chaque paramètre incertain par une distribution de probabilité discrète, identifiée par un ensemble de

Paramètre	Valeur nominale	Déviation standard
Réactif A (kmole)	12	1.0
Réactif B (kmole)	12	1.0
Température réacteur (° C)	20	2.0
Débit jaquette ($m^3.min^{-1}$)	0.35	0.05
Consigne réacteur (° C)	71	1.5

Tableau 3.1: Caractéristiques des paramètres initiaux du procédé - d'après Podofillini and Dang [2012]

points d'évaluation x_i et les probabilités correspondantes p_i. Chaque point x_i est la moyenne prise sur chaque intervalle de discrétisation identifié par les p_i. Les intervalles peuvent être sélectionnés pour explorer les régions les plus intéressantes des valeurs des paramètres.
La simulation de Monte Carlo (MC) pour l'analyse de la sécurité et de la fiabilité des systèmes implique la génération de nombreuses histoires de vie du système (appelées "essais MC" dans ce qui suit) en échantillonnant les temps de transition et les états des composants du système ainsi que les résultats des actions des opérateurs. Les caractéristiques dynamiques de l'évolution du système sont intégrées dans la simulation stochastique en introduisant les modèles physiques de l'évolution du processus (c'est-à-dire les équations des bilans de matière et d'énergie pour la présente application). Au début de chaque simulation, les valeurs des paramètres du procédé sont échantillonnées à partir des distributions gaussiennes, dont les caractéristiques sont indiquées dans le tableau 3.1.
Les détails de chacune des procédures discrètes (PSA) et échantillonées (MC) sont décrits dans l'article [Podofillini and Dang, 2012].

3.2.2.2 Résultats et discussion

Les résultats des procédures (PSA) et (MC) sont indiqués et comparés en termes de fréquence globale de défaillance du système et de contributeur de risques.
Le tableau 3.3 permet de comparer les valeurs de la fréquence globale de défaillance du réacteur fermé.
En considérant la valeur de la procédure (MC) comme référence, selon les hypothèses de l'expert A, le résultat de $4.4 \times 10^{-5}.(jour)^{-1}$ est environ d'un facteur de $1,5$ plus important que le résultat de l'analyse dynamique (MC), tandis que, selon les hypothèses de l'expert B, le résultat de la procédure (PSA) de $1.0 \times 10^{-4}.(jour)^{-1}$ est d'un facteur 4 supérieur à celui de l'analyse dynamique (MC). En termes d'ordre de grandeur, les résultats sont cohérents avec le choix initial des scénarios de référence. Le scénario choisi par l'expert A est plus représentatif des scénarios d'emballement thermiques. Le scénario plus difficile à contrôler retenu par l'expert B est un choix plus conservateur, ce qui conduit à des résultats plus défavorables.
La figure 3.4 permet de comparer le poids respectif de chaque évément initiateur dans sa contribution à des défaillances du réacteur fermé. L'ordonné FV est le facteur d'importance de diagnostic de Fussel-Vesely, qui indique la probabilité pour qu'un composant soit en panne, sachant

Repère	Description	Fréquence ou probabilité
IE-DEV	Valeurs divergentes des paramètres du procédé (déclenchement d'un transitoire dangereux)	$2.7 \times 10^{-2}.(jour)^{-1}$
IE-TCS	Transitoires dangereux déclenchés par la perte de débit de la jaquette	$9.0 \times 10^{-5}.(jour)^{-1}$
PP-EX	Valeurs divergentes des paramètres du procédé telles que le transitoire est incontrôlable	1.1×10^{-3}
A1-BYPASS	Valeurs des paramètres du processus telles que la condition d'activation de l'alarme 1 est contournée	1.0×10^{-1}
A1	Défaillance de l'alarme 1	1.0×10^{-2}
HFE-A1-DIAG	Défaut de diagnostic de l'opérateur (réponse à A1)	1.0×10^{-1} (expert A) 1.7×10^{-1} (expert B)
ECS-FS	Le système de refroidissement d'urgence ne démarre pas	1.0×10^{-2}
A2	Défaillance de l'alarme 2	1.0×10^{-2}

Tableau 3.2: Liste des événements initiateurs et de leurs fréquences - d'après Podofillini and Dang [2012]

Procédure	Fréquence globale de défaillance
(PSA) expert A	$4.4 \times 10^{-5}.(jour)^{-1}$
(PSA) expert B	$1.0 \times 10^{-4}.(jour)^{-1}$
(MC)	$2.7 \times 10^{-5} \pm 1.2 \times 10^{-6}.(jour)^{-1}$

Tableau 3.3: Comparaison des valeurs de la fréquence de défaillance globale du réacteur fermé.

que le système est en panne. Ce facteur représente la probabilité qu'une coupe minimale contenant l'événement initiateur provoque la défaillance du système, sachant que le système est défaillant.

Les approches (MC) et (PSA) aboutissent à la même conclusion quant aux événements qui contribuent le plus aux risques. Ceux-ci sont liés à la présence de scénarios de conditions "extrêmes", tels que le non-démarrage ECS, l'absence de réponse de l'opérateur aux alarmes A1 et A2 et le contournement des conditions d'activation de l'alarme A1. La figure 3.4 montre également une correspondance étroite entre les résultats de l'approche (MC) et ceux de l'approche (PSA) obtenus avec les hypothèses de l'expert A. Cela suggère que le scénario limitatif choisi par l'expert A représente bien la réalité du comportement des transitoires conduisant à des conditions dangereuses pour le réacteur discontinu. Il est aussi possible de constater que les importances relatives obtenues avec les hypothèses de l'expert B sont très différentes des autres observations. Comme cela a déjà été indiqué lors de la comparaison des valeurs de la fréquence de défaillance globale du réacteur fermé, c'est le résultat des scénarios conservateurs choisis

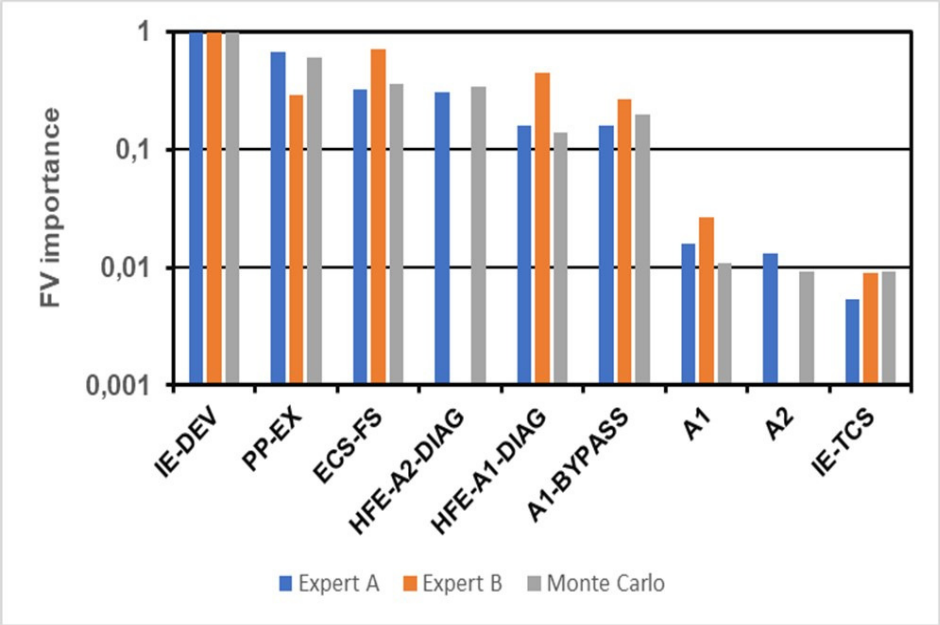

Figure 3.4: Comparaison des procédures (MC) et (PSA) en termes de contributeurs de risques - adapté d'après Podofillini and Dang [2012].

par l'expert B pour la définition des mesures de protection lors de ces conditions extrêmes.

3.2.3 Prise en compte des incertitudes épistémiques

Pour mémoire, Yazdi et al. [2022] ont souligné les nombreux paramètres intervenant dans l'évaluation des risques, tels entre autres, les taux de défaillance des différents composants et des différents modes de défaillance, les temps de réparation et d'arrêt des différents composants, les taux de défaillance de cause commune, les probabilités d'erreur humaine, les paramètres d'usure et de détérioration des composants, les probabilités d'inflammation des rejets de gaz, les fréquences des événements naturels, les données d'exposition, les données d'activité et les actions sur les données des procédés. Les incertitudes de ces paramètres indiquent le large spectre de données pouvant être utilisées dans le processus d'évaluation des risques. Les principales raisons pour lesquelles la disponibilité des données est incertaine sont:

- le recours à des jugements d'experts;
- la pertinence des données;
- la qualité des données et de leur collecte;
- la quantité de données.

3.2.3.1 Conditions initiales des incertitudes

Karanki et al. [2018] ont complété les travaux de Podofillini and Dang [2012] en étudiant l'influence des incertiutdes épistémiques sur la dynamique du comportement du réacteur discontinu. Le tableau 3.4 récapitule les types de distributions épistémiques utilisées pour les paramètres physiques et de sécurité du procédé chimique du réacteur discontinu.

Système	Paramètres	Distribution épistémique	Paramétres
Sécurité procédé	Défaillance jaquette (J)	Lognormale	6×10^{-5} (h^{-1}); $3,7$
	Défaillance alarme (A)	Lognormale	$0,01$; $5,1$
	Défaillance start urgence (ECSA)	Lognormale	$0,01$; 7
	Défaillance hardware urgence (ECSH)	Lognormale	3×10^{-5} (h^{-1}); $3,7$
Données procédé	Constantes cinétiques (k1;k2)	Normale	1; $0,25$
	Facteur d'entartrage	Uniforme	$1,75 \times 10^{-4}$; $3,5 \times 10^{-4}$

Tableau 3.4: Distributions des incertitudes épistémiques dans le modèle du réacteur discontinu - d'après Karanki et al. [2018].

3.2.3.2 Résultats et discussion

Le profil de risque est fonction de paramètres épistémiques retenus. Lorsque les paramètres épistémiques sont modifiés, la mesure du facteur d'importance obtenue peut changer et, par conséquent, l'ordre des contributeurs de risque peut également varier. Compte tenu des incertitudes liées aux paramètres épistémiques du modèle de risque, les mesures du facteur d'importance des événements de base ont été calculées. L'incertitude de chaque mesure d'importance des événements de base est obtenue à partir de ces résultats. La figure 3.5 montre les distributions de probabilités cumulées des facteurs d'importance des événements de base. Les moyennes de ces distributions sont utilisées pour classer les facteurs de risque.
Les facteurs de risque sont presque identiques dans les deux approches échantillonnée et discrète, sauf que la discrétisation a surestimé la contribution de IE-1 et PPEX (conditions d' emballement). A la lumière des incertitudes épistémiques, les initiateurs d'accidents IE-1 et IE-2 et les conditions d'emballement PPEX sont apparus comme des contributeurs critiques, suivis par les événements associés aux fonctions de sécurité. En ce qui concerne ces derniers, après le déclenchement de l'accident, le système automatique ECSA et la réponse de l'opérateur à l'alarme 2 (A2OAR) sont des facteurs importants. Il faut aussi curieusement remarquer que la contribution de l'événement IE-TCS, qui avait été considéré comme pratiquement négligeable dans le cas purement aléatoire (voir figure 3.4), devient notoire en tenant compte des incertitudes épistémiques.
Karanki et al. [2018] ont aussi examiné la gestion de l'incertitude, qui nécessite l'identification des principaux facteurs d'incertitude. Le tableau 3.4 avait considéré les deux systèmes Procédé et Sécurité comportant respectivement trois paramètres physiques et quatre paramètres sécu-

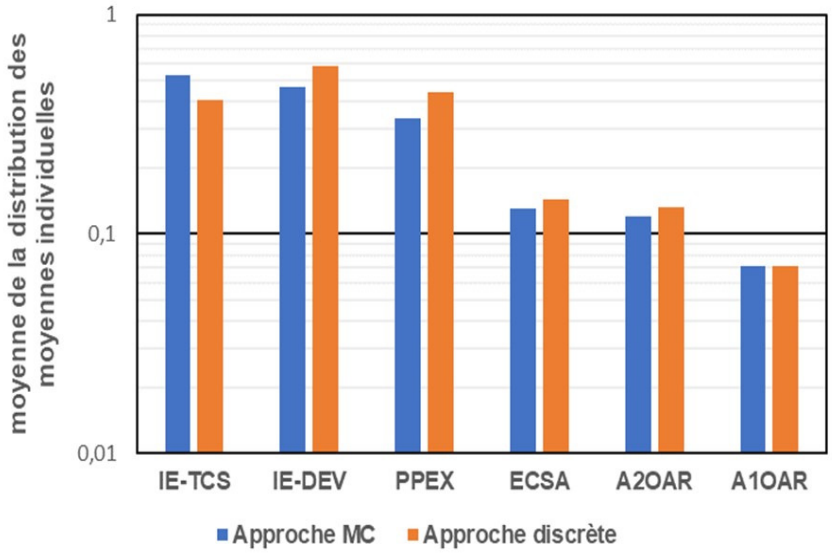

Figure 3.5: Comparaison des contributeurs de risques en considérant les incertitudes épistémiques - adapté d'après Karanki et al. [2018].

rité. La figure 3.6 illustre la hiérarchie d'incertitude de classement du facteur d'importance des paramètres.

Les deux approches présentent une hiérarchie similaire de l'importance des paramètres. Il est intéressant de noter que les poids des constantes cinétiques de la réaction chimique (k1-k2) et du coefficient global de transfert de chaleur de la jaquette (U) contribuent de manière significative à l'incertitude de la stabilité de fonctionnement du réacteur fermé. Cette contribution au classement est ensuite complétée par les paramètres relatifs aux équipements de sécurité. La conséquence importante du constat de l'influence des paramètres physicochimiques du procédé résulte de la compétition entre la forte exothermie réactionnelle et l'évacuation de la chaleur par la jaquette de refroidissement. Ceci se traduit par l'évolution de la température du réacteur entrainant la probabilité que le système entre dans un état transitoire incontrôlable menant à une défaillance du système (emballement). Par conséquent, ces paramètres devraient être au centre des efforts visant à réduire l'incertitude de l'estimation du risque.

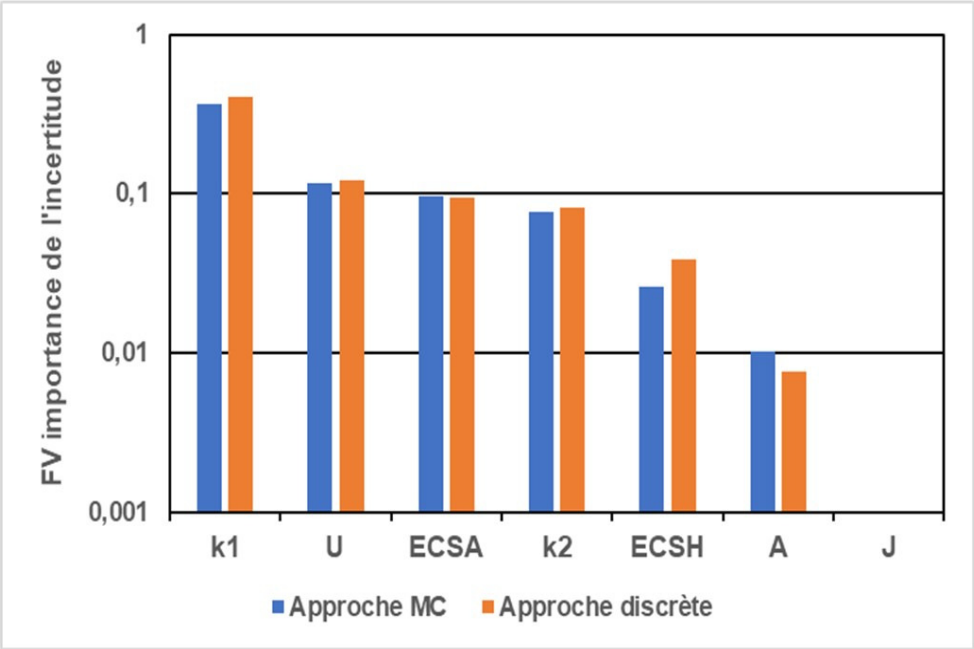

Figure 3.6: Classement de l'importance de l'incertitude des paramètres épistémiques - adapté d'après Karanki et al. [2018].

3.3 Application d'un arbre quantifié dynamique des événements au comportement d'un réservoir de stockage

L'objectif du contenu de cet exemple consiste à présenter une méthodologie d'évaluation dynamique du risque d'un procédé avec inférence bayésienne. En s'inspirant des travaux de Meel and Seider [2006] et Meel et al. [2007], Kalantarnia et al. [2009] ont proposé l'organigramme de la figure 3.7 pour mettre en œuvre la procédure d'analyse dynamique des risques. L'évaluation des défaillances est initiée par la détermination des scénarios d'accidents potentiels par l'analyse de l'arbre des événements. La probabilité d'occurrence de chaque conséquence finale est estimée simultanément par l'approche déterministe conventionnelle et par une approche probabiliste. Notons qu'à ce stade des étapes, l'évaluation relève des méthodes classiques des risques. Dans l'étape suivante, l'approche bayésienne est utilisée pour actualiser la probabilité de l'occurrence de l'événement et celle du système. L'inférence bayésienne permet de calculer la probabilité finale, dite postérieure ou a posteriori, de chaque conséquence finale, en considérant que les données initiales, ainsi que celles des précurseurs d'accidents se produisant au cours du fonctionnement du procédé, sont représentées ici par les valeurs, dites a priori, obtenues dans les étapes précédentes. Notons que l'acquisition en temps réel peut à tout moment enrichir les valeurs a priori des données.

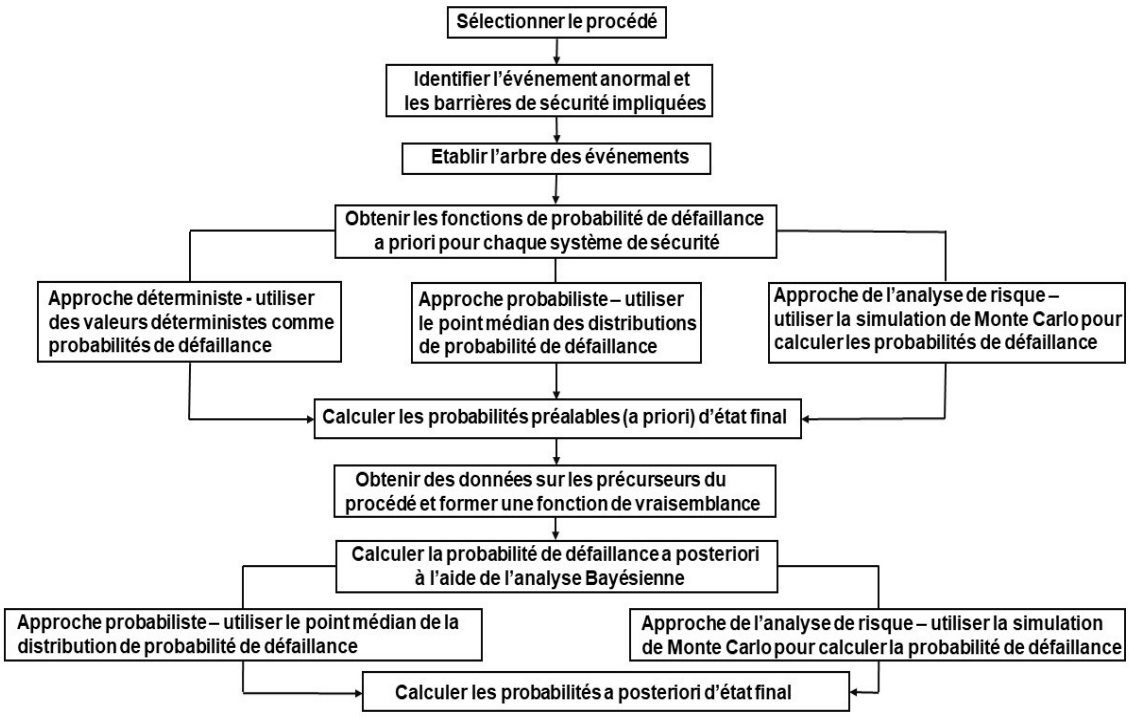

Figure 3.7: Organigramme de la procédure d'analyse dynamique des risques d'un procédé - adapté d'après Kalantarnia et al. [2009].

Remarquons ici que dans le calcul de la probabilité a priori, une étape de l'organigramme de la figure 3.7 propose l'approche de l'analyse du risque via la simulation de Monte Carlo. Cette méthode d'évaluation des caractéristiques de risque d'un procédé incertain, dans lequel les hypothèèses sont échantillonnées de manière itérative sur la base de distributions de probabilité prédéfinies, génère une distribution correspondante de probabilité de sortie. Son intérêt permet de répondre à des questions quantitatives en termes de probabilités plutôt qu'en termes déterministes uniques.

3.3.1 Description du réservoir tampon de stockage

Le procédé considéré est constitué par un réservoir tampon fonctionnant en système ouvert et contenant des produits chimiques dangereux. Le principal risque potentiel de ce procédé réside dans le sur-remplissage avec débordement généré par un débit d'alimentation excessif. La figure 3.8 indique le schéma de principe du procédé. Pour en assurer la sécurité, les barrières de sécurité suivantes ont été mises en place :

- Contrôle du processus de base (BPCS);
- Bypass de la ligne de dérivation;
- Alarme de seuil haut (LSH);

- Soupape de sécurité (PSV),
- Vanne manuelle

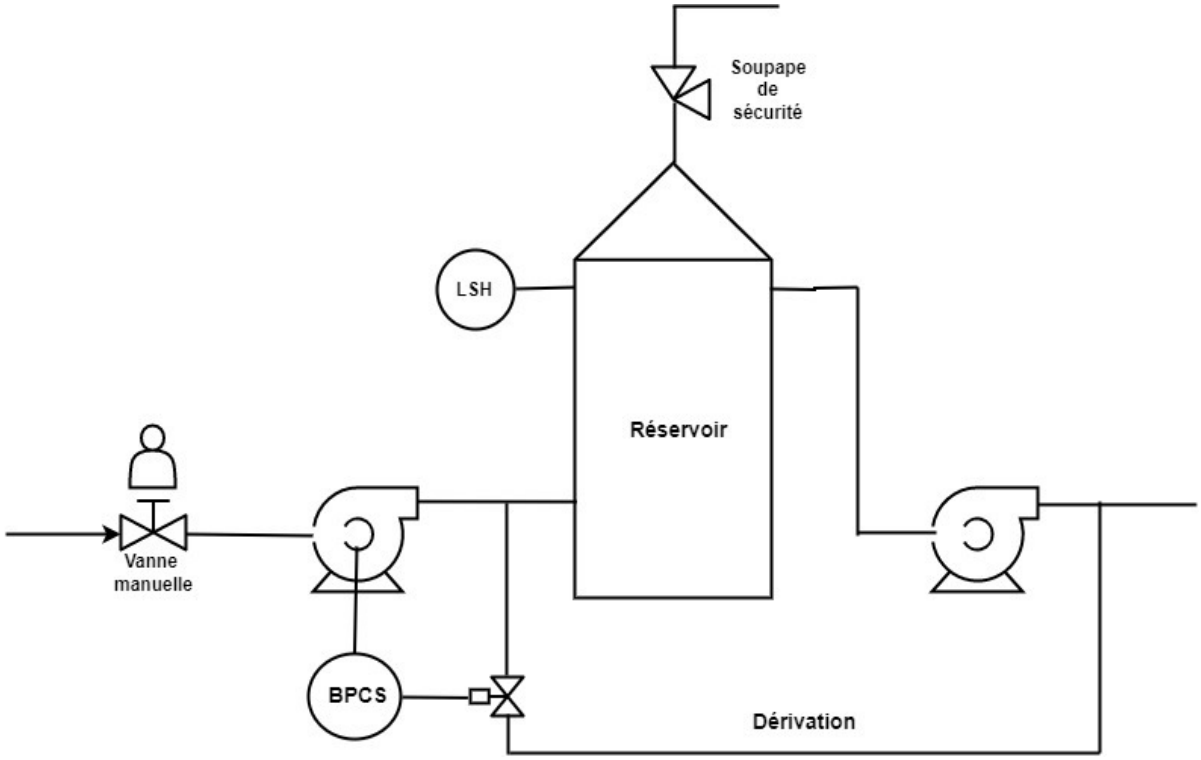

Figure 3.8: Schéma de principe du réservoir équipé des barrières de sécurité - adapté d'après Kalantarnia et al. [2009].

L'excès de débit entrant dans le réservoir doit être détecté par le système de contrôle du processus de base (BPCS), qui ouvre la vanne de dérivation. Le débit excédentaire quitte alors le système par la conduite de dérivation . Si le BPCS ne fonctionne pas, l'alarme de seuil haut se déclenche, signalant à l'opérateur de fermer la vanne manuelle afin d'empêcher l'entrée d'un débit supplémentaire dans le réservoir. Si, pour une raison quelconque, l'opérateur ne ferme pas la vanne, la soupape de sécurité est activée et l'excès de fluide est relâché.
La figure 3.9 présente l'arbre des événements, qui relie l'événement anormal d'un débit entrant excessif à toutes ses conséquences connues. Les états finaux sont identifiés par un repère alpha-numérique, où la lettre décrit une des trois situations:

- A état de sécurié;
- B rejet de liquide;
- C surpression.

Il faut noter ici que la lettre x_i représente les probabilités successives de défaillance dans chaque branche de l'arbre.

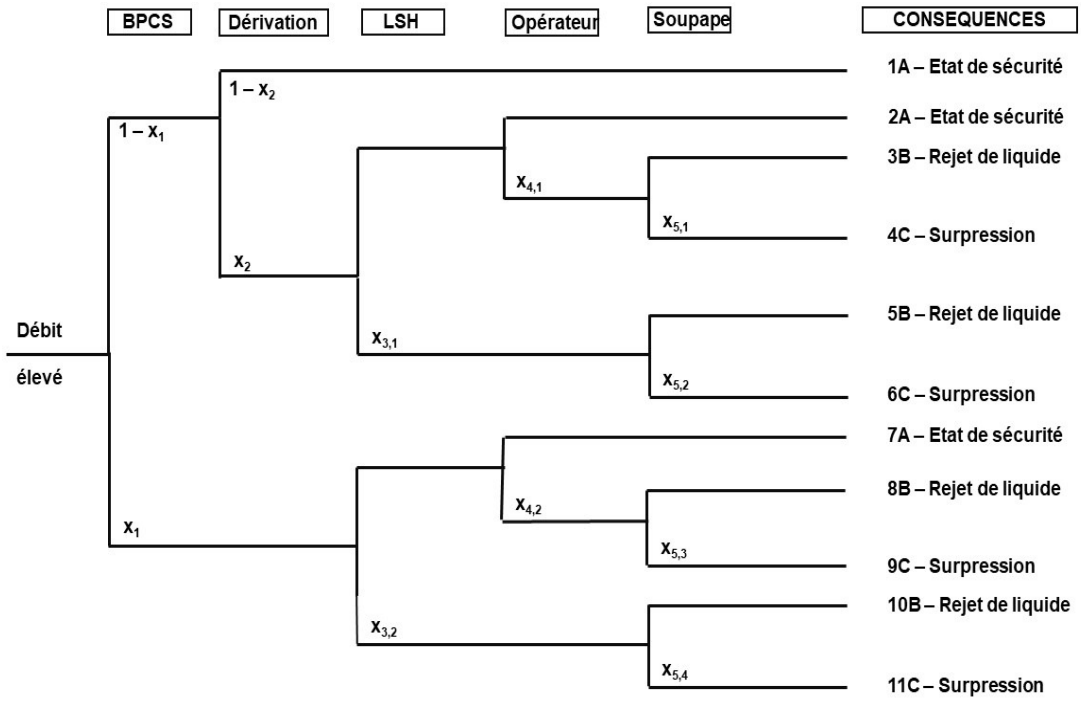

Figure 3.9: Arbre des événements du réservoir généré par un débit entrant excessif - adapté d'après Kalantarnia et al. [2009].

Les conditions respectives initiales des valeurs déterministes des probabilités de défaillance et des paramètres de la fonction de distribution Beta des barrières sont récapitulées dans les tableaux 3.5 et 3.6. Les valeurs indiquées proviennent des banques de données et des dires d'experts.

Barrière de sécurité	Probabilité de défaillance
BPCS système de contrôle de base du procédé	0,025
Bypass de recirculation	0,015
LSH seuil haut de niveau	0,150
Opérateur vanne manuelle	0,200
PSV soupape de sécurité	0,045

Tableau 3.5: Probabilités déterministes de défaillance des barrières.

Barrière de sécurité	α	β
BPCS système de contrôle de base du procédé	0,25	2,10
Bypass de recirculation	0,15	0,76
LSH seuil haut de niveau	1,50	7,00
Opérateur vanne manuelle	1,00	3,00
PSV soupape de sécurité	0,40	3,40

Tableau 3.6: Paramètres α et β de la fonction de distribution Beta des barrières de sécurité.

3.3.2 Etude comparative des approches déterministe, probabiliste et bayésienne

3.3.2.1 Approche déterministe

Dans cette approche, une probabilité de défaillance déterministe est attribuée à chaque système. La probabilité d'un état final est calculée en suivant les branches de l'arbre des événements jusqu'à cet état particulier. La valeur déterministe de chaque état final est obtenue simplement en multipliant les probabilités de chaque branche liée à l'état à l'aide des valeurs du tableau 3.5. Par exemple, la probabilité de l'état final de sécurité 1A est calculée par la relation:

$$p(1A) = (1 - x_1)(1 - x_2) = (1 - 0,025)(1 - 0,015) = 0,96 \tag{3.3}$$

Toutes les autres probabilités d'état final sont obtenues de la même manière.

3.3.2.2 Approche probabiliste

Dans l'approche probabiliste, chaque probabilité d'état final est estimée en utilisant des fonctions de densité de probabilité pour chaque système suivant les distributions Beta du tableau 3.6. Dans une première estimation, en raison du logiciel simple mais limité utilisé, les probabilités de défaillance sont établies à partir du point médian de la distribution Beta. Le résultat pour chaque état final est calculé en multipliant les points médians de la distribution de probabilité de défaillance des systèmes dans chaque branche.
Il est possible d'améliorer cette première approche probabiliste en une approche dite analyse de risque. Cette fois l'analyse est effectuée à l'aide du logiciel @Risk (Palisade Corporation), qui a la capacité de générer l'ensemble de la distribution Beta pour chaque système. Les probabilités d'état final sont obtenues par simulation de Monte Carlo.

La synthèse de trois approches fournit les probabilités d'occurrence de chaque état final, qui seront considérées dans la suite de la démarche de l'analyse dynamique des risques comme les valeurs préalables ou a priori (Tableau 3.7).

Etat final	Approche déterministe	Approche probabiliste	Approche analyse de risque
1A	$9,60 \times 10^{-1}$	$9,61 \times 10^{-1}$	$8,64 \times 10^{-1}$
2A	$9,95 \times 10^{-3}$	$9,90 \times 10^{-3}$	$7,59 \times 10^{-3}$
3B	$2,37 \times 10^{-3}$	$2,46 \times 10^{-3}$	$1,31 \times 10^{-3}$
4C	$1,12 \times 10^{-4}$	$1,17 \times 10^{-4}$	$2,66 \times 10^{-5}$
5B	$2,10 \times 10^{-3}$	$2,11 \times 10^{-3}$	$1,38 \times 10^{-3}$
6C	$9,87 \times 10^{-5}$	$1,01 \times 10^{-4}$	$2,74 \times 10^{-5}$
7A	$1,70 \times 10^{-2}$	$1,66 \times 10^{-2}$	$1,44 \times 10^{-2}$
8B	$4,06 \times 10^{-3}$	$4,13 \times 10^{-3}$	$2,48 \times 10^{-3}$
9C	$1,91 \times 10^{-4}$	$1,97 \times 10^{-4}$	$6,39 \times 10^{-5}$
10B	$3,58 \times 10^{-3}$	$3,55 \times 10^{-3}$	$2,59 \times 10^{-3}$
11C	$1,69 \times 10^{-4}$	$1,69 \times 10^{-4}$	$6,59 \times 10^{-5}$

Tableau 3.7: Comparaison des résultats des probabilités d'occurrence a priori en fonction du type d'approche.

3.3.2.3 Approche bayésienne

Soit x la probabilité de défaillance du système et $f(x)$ la fonction de distribution de probabilité (distribution a priori), $f(x|Data)$ représentera la distribution a posteriori à l'aide de l'équation :

$$f(x|Data) \propto g(Data|x).f(x) \tag{3.4}$$

où $g(Data|x)$ est la fonction de vraisemblance.
En considérant la fonction a priori Beta de distribution de paramètres a et b et la fonction binomiale de vraisemblance, la fonction de distribution a posteriori s'écrit à l'aide de la théorie de Bayes:

$$f(x) \propto x^{a-1}\,(1-x)^{b-1} \tag{3.5}$$

$$g(Data|x) \propto x^{s}\,(1-x)^{f} \tag{3.6}$$

$$f(x|Data) \propto g(Data|x)\,f(x) \propto x^{a-1} \times (1-x)^{b-1}\,x^{s}\,(1-x)^{f} \propto x^{a+s-1}\,(1-x)^{b+f-1} \tag{3.7}$$

Kalantarnia et al. [2009] ont publié les résultats des probabilités d'occurrence a posteriori sur une période de dix années et montré que les valeurs obtenues sont très proches pour les deux approches examinées. Ils ont noté que les résultats des probabilités des conséquences finales changent drastiquement sur la période décennale lorsque les nouvelles valeurs a priori sont introduites dans les analyses. Le tableau 3.8 illustre clairement de dernier constat pour les trois conséquences A, B et C en indiquant simultanément sur la durée de dix années les valeurs a posteriori et initiale de base (repère 0).

Année Type	1	2	3	4	5	6	7	8	9	10	0
A	0,604	0,431	0,341	0,294	0,280	0,274	0,278	0,297	0,298	0,309	0,987
B	0,170	0,244	0,283	0,278	0,270	0,283	0,312	0,346	0,351	0,346	0,012
C	0,225	0,324	0,376	0,428	0,450	0,442	0,411	0,357	0,351	0,346	0,001

Tableau 3.8: Comparaison des probabilités a posteriori sur dix années pour les trois types de conséquences.

3.4 Traitement par logique floue des incertitudes des données dans l'analyse des arbres d'événements

L'objectif principal de cette section est de prendre en compte les différents types d'incertitudes dans l'arbre des événements en utilisant des approches telles que la théorie des ensembles flous et la théorie de la preuve. La première est utilisée pour traiter les incertitudes linguistiques/subjectives des probabilités d'événements, alors que la seconde permet de gérer l' ignorance incomplète ou partielle des connaissances des experts. L'applicabilité de ces approches est illustrée par l'étude de cas d'un rejet de GPL dans une usine.

La logique floue est une approche issue d'une théorie mathématique qui a été développée dans les années 60 par le mathématicien Lotfi Zadeh. C'est une méthode de traitement de l'information également connue sous le nom de logique incertaine ou « fuzzy logic », permettant de traiter des informations imprécises ou incertaines. Contrairement à la logique classique, qui énonce que toute proposition est soit vraie, soit fausse, la logique floue permet d'exprimer une proposition avec un certain degré de certitude ou d'incertitude. Pour résumer, la logique floue est une méthode de traitement de l'information et de mise en qualité qui permet de gérer des informations approchantes ou imprécises. Elle est utilisée dans de nombreux domaines pour modéliser des systèmes complexes et est capable de représenter des nuances et des degrés de corrélation entre des données approchantes.

Les approches fondées sur la notion de flou permettent de remédier aux lacunes inhérentes à la logique binaire. Elles traitent efficacement l'imprécision due à la subjectivité et à l'imprécision et sont utiles pour propager les incertitudes tout au long de l'analyse et de l'évaluation des risques. Les approches floues sont une forme généralisée d'analyse des intervalles utilisée pour traiter les informations incertaines ou imprécises. Un nombre flou décrit la relation entre une quantité incertaine p (par exemple, la probabilité d'un événement) et une fonction d'appartenance, qui varie entre 0 et 1. Un ensemble flou est une extension de la théorie traditionnelle des ensembles (dans laquelle p est soit membre de l'ensemble P, soit non membre), de sorte que p peut être membre de l'ensemble P avec un certain degré d'appartenance. Toute forme de nombre flou est possible, mais la forme choisie doit être justifiée par les informations disponibles. En général, les nombres flous triangulaires (TFN) ou trapézoïdaux (ZFN) sont utilisés pour représenter les variables.

3.4.1 Cadre de l'étude des incertitudes dans un arbre des événements

Ferdous et al. [2009] ont examiné l'analyse des incertitudes d'un arbre des événements à l'aide de la théorie des ensembles flous. Le jugement subjectif de la probabilité d'un événement est supposé décrit à l'aide d'un profil de nombre flou triangulaire (TFN). Les probabilités floues d'initiation sont ensuite utilisées pour estimer la probabilité de l'événement, qui est également exprimé sous la forme d'un nombre flou. L'approche floue utilisée pour l'arbre des événements comprend les trois étapes suivantes:

- définir la probabilité de l'événement à l'aide des TFN;
- déterminer la probabilité de l'événement résultant en tant que TFN;
- défuzzifier la fréquence de l'événement de résultat sous forme d'un nombre précis.

3.4.1.1 Définir la probabilité d'un événement à l'aide de nombres flous

Les experts utilisent habituellement des appréciations, telles par exemple que probable, vraisemblable, improbable plutôt que des expressions numériques pour justifier la probabilité d'un événement. Il est possible d'attribuer un profil triangulaire de nombre flou (TFN) pour remplacer l'évaluation linguistique d'un expert. Un TFN typique pour une quantité incertaine, comme par exemple la probabilité d'un événement, est illustré sur la partie (a) de la figure 3.10.
Le TFN est un vecteur (p_L, p_m, p_R) qui représente les valeurs minimales, les valeurs les plus probables et les valeurs maximales de la probabilité de l'événement, tandis que le niveau de coupe $\alpha - cut$ traduit une fonction d'appartenance μ_P. Pour un TFN déterminé, les intervalles imbriqués $\tilde{P}_\alpha$ peuvent être générés en modifiant progressivement les niveaux de coupe $\alpha - cut$ comme suit:

$$\tilde{P}_\alpha = (\alpha_i, p_{Li}, p_{Ri}) \qquad \text{pour } i = 1, 2, ..., n \tag{3.8}$$

La présente étude a utilisé huit grades qualitatifs représentés par des TFN pour exprimer les probabilités linguistiques des experts. Les huit degrés sont les suivants : hautement improbable (HI), très improbable (VI), plutôt improbable (RI), assez improbable (RI), très improbable (RI), improbable (I), probable (P), assez probable (RP), très probable (VP). La partie (b) de la figure 3.10 indique la correspondance dans une échelle floue.

3.4.1.2 Déterminer la probabilité d'un événement conséquence en tant que nombre flou

La fonction d'appartenance μ_P représente l'incertitude de la probabilité d'un événement. Les niveaux de coupe $\alpha - cut$ sont utilisés pour déterminer les intervalles flous (c'est-à-dire les intervalles imbriqués dans un nombre flou) dont le degré d'appartenance est supérieur ou égal à la valeur du niveau de la coupe. Dans un nombre flou trianglaire, la fonction d'appartenance utilise la relation (3.9) pour déterminer l'intervalle à la valeur du niveau de coupe

$$\tilde{P}_\alpha = p_L + \alpha(p_m - p_L),\ p_R + \alpha(p_R - p_m) \tag{3.9}$$

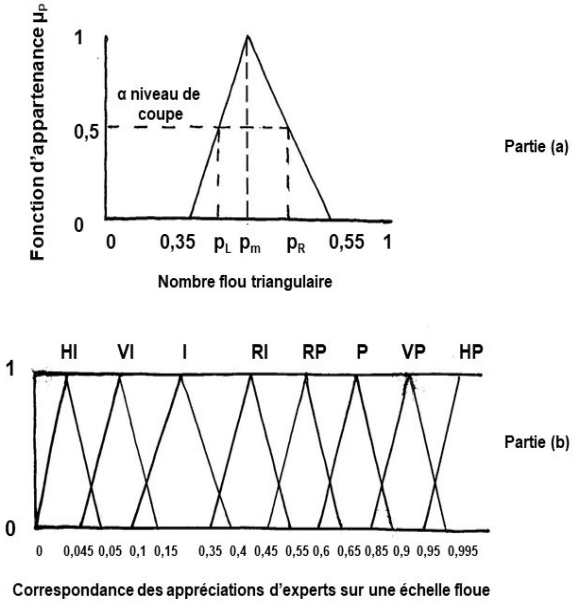

Figure 3.10: Exemples d'un nombre flou triangulaire (a) et de correspondance des avis d'experts dans une échelle floue (b) - adapté d'après Ferdous et al. [2009].

Pour simplifier l'analyse, Ferdous et al. [2009] ont entre autres utilisé la formulation de la méthode du niveau de coupe $\alpha - cut$ en arithmétique floue pour estimer la probabilité de l'événement conséquence. Le tableau 3.9 récapitule les opérations et équations recommandées:

Opération	Equations
$\tilde{P}_{1\alpha} \times \tilde{P}_{2\alpha}$	$p_{1L} \times p_{2L},\ \ p_{1R} \times p_{2R}$
$\tilde{P}_{1\alpha} + \tilde{P}_{2\alpha}$	$p_{1L} + p_{2L},\ \ p_{1R} + p_{2R}$

Tableau 3.9: Formulation des opérations et équations de la méthode du niveau de coupe en arithmétique floue - adapté d'après Ferdous et al. [2009].

3.4.1.3 Défuzzifier la fréquence de l'événement en tant que nombre précis (estimation ponctuelle)

La défuzzification transforme un nombre flou en une valeur exacte. La méthode de la moyenne pondérée est efficace en termes de calcul. L'équation (3.10) est utilisée pour la défuzzification

de la probabilité ou de la fréquence de l'événement de résultat.

$$p_{out} = \frac{\sum \mu_P(\tilde{P}) \times \tilde{P}}{\sum \mu_P(\tilde{P})} \tag{3.10}$$

3.4.2 Etude de cas sur le rejet de GPL dans une usine d'alkylate de détergent

Il est proposé d'appliquer la démarche de logique floue à l'analyse d'un arbre des événements représentant un rejet important de GPL à proximité d'une usine de fabrication d'un alkylate de détergent. La figure 3.11 illustre l'exemple de l'arbre des événements extrait de l'ouvrage de Lees [1996].

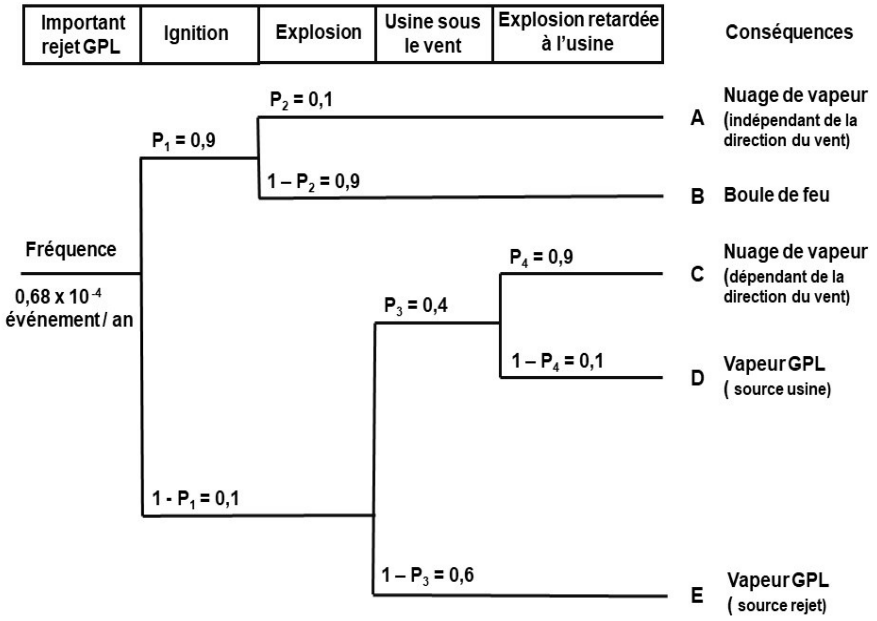

Figure 3.11: Arbre des événements d'un rejet important de GPL - adapté d'après Lees [1996].

L'événement initiateur est constitué par une importante fuite de GPL. L'inflammation de l' hydrocarbure peut provoquer une explosion ou une boule de feu dans le voisinage de la source de rejet. L'explosion génère un nuage de vapeur. En l'absence d'ignition, le nuage de rejet dérive alors vers l'usine et peut provoquer une explosion retardée, qui provoque également un autre nuage de vapeur en fonction de la direction du vent. A partir du point de rejet du GPL, les vapeurs peuvent dériver dans une autre direction s'il n'y a pas d'explosion au voisinage de l'usine. Quatre événements sont identifiés : l'ignition, l'explosion, l'usine sous le vent et l'explosion retardée au niveau de l'usine. Les cinq conséquences potentielles sont les suivantes:

- A - Nuage de vapeur (indépendant de la direction du vent);
- B - Boule de feu;
- C - Nuage de vapeur (dépendant de la direction du vent);
- D - Vapeur GPL (source usine);
- E - Vapeur GPL (source rejet).

3.4.2.1 Approche déterministe

L'évaluation quantitative classique des fréquences respectives des conséquence A - B- C - D et E est estimée à l'aide de la relation 3.11.

$$\lambda_i = \lambda \times \prod_{i=1}^{n} P_i \tag{3.11}$$

où λ est la fréquence de l'événement initiateur du rejet de GPL, λ_i est la fréquence de la conséquence i et P_i la probabilité de chaque événement rencontré sur un chemin de l'arbre.
Le calcul est effectué en suivant les différentes branches de l'arbre des événements de la figure 3.11 avec les valeurs numériques repérées.
Le tableau 3.10 regroupe les valeurs des fréquences des cinq conséquences.

Conséquences	Fréquence (événement par an)
A	$6,1 \times 10^{-6}$
B	$5,5 \times 10^{-5}$
C	$2,4 \times 10^{-6}$
D	$2,7 \times 10^{-7}$
E	$4,1 \times 10^{-6}$

Tableau 3.10: Fréquence des conséquences de l'arbre des événements par approche déterministe classique - adapté d'après Ferdous et al. [2009].

3.4.2.2 Approche floue

La figure 3.11 de l'arbre des événements du rejet inflammable est d'abord transformée en un arbre des événements, intégrant les appréciations linguistiques floues, illustré sur la figure 3.12. La méthode de l'approche, dite du niveau de coupe $\alpha - cut$ donné, a été retenue pour les opérations d'arithmétique floue. Dans cette méthode, un niveau de coupe $\alpha - cut$ est choisi (ce qui revient à fixer une fonction d'appartenance). Comme un arbre des événements implique de discriminer à chaque instant parmi deux états, l'arithmétique floue nécessite deux opérations de multiplication et ou d'addition pour calculer la probabilité d'une conséquence pour deux nombres flous triangulaires. Le tableau 3.9 en a préalablement déjà détaillé la formulation des

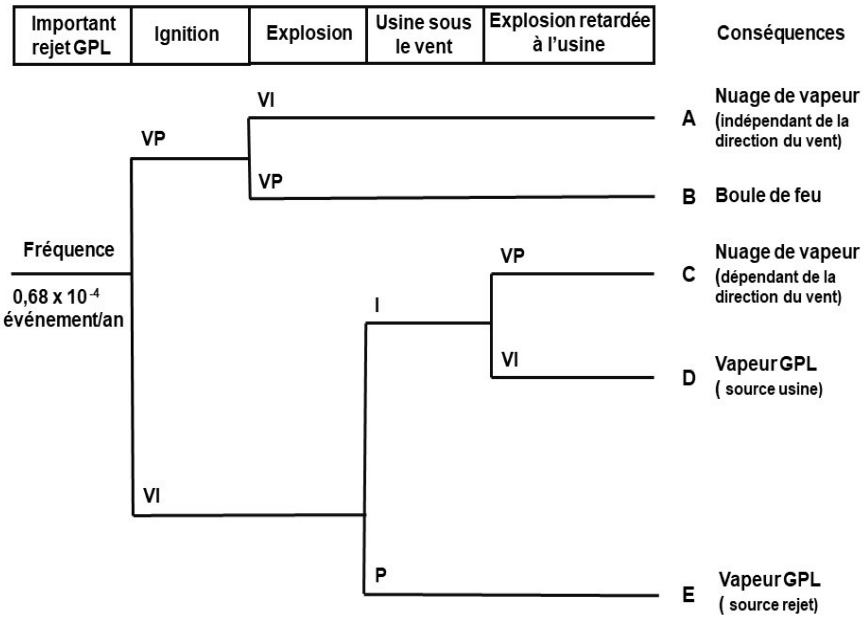

Figure 3.12: Arbre des événements avec les variables d'appréciation floue - adapté d'après Ferdous et al. [2009].

expressions. Par exemple, le chemin menant à la conséquence A est accompagné par deux événements. Les probabilités de ces deux événements sont exprimées par les appréciations VP (très probable) et VI (très improbable). Deux nombres flous triangulaires sont attribués à ces deux variables, puis le nombre flou triangulaire de la conséquence est calculé. Pour une valeur donnée du niveau de coupe $\alpha - cut$, le nombre flou de la fréquence de la conséquence est défuzzifié. Le tableau 3.11 regroupe les fréquences des cinq conséquences ainsi obtenues.
Cet exemple a été volontairement traité en se limitant au type d'incertitude linguistique en utilisant une approche floue. Une approche globale plus complète est traitée en détail dans l'article de [Ferdous et al., 2009].

Pour aller plus loin
- Analyse des différentes barrières de sécurité d'un terminal de vaporisation de GNL par approche bayésienne.
Documentation: Mithun et al. [2023] - Kujath et al. [2010].
- Etude quantitative dynamique de la combinaison d'un arbre des événements et d'un réseau bayésien pour estimer les probabilités des presqu'accidents d'une unité automatisée de production de styrène.
Documentation: Chen et al. [2020].

$\alpha - cut$	A	B	C	D	E
$0,20$	$5,20 \times 10^{-6}$	$3,86 \times 10^{-5}$	$1,57 \times 10^{-6}$	$2,32 \times 10^{-7}$	$4,21 \times 10^{-6}$
$0,40$	$5,10 \times 10^{-6}$	$3,85 \times 10^{-5}$	$1,45 \times 10^{-6}$	$2,05 \times 10^{-7}$	$4,11 \times 10^{-6}$
$0,50$	$5,06 \times 10^{-6}$	$3,84 \times 10^{-5}$	$1,36 \times 10^{-6}$	$1,93 \times 10^{-7}$	$4,07 \times 10^{-6}$
$0,60$	$5,03 \times 10^{-6}$	$3,83 \times 10^{-5}$	$1,33 \times 10^{-6}$	$1,82 \times 10^{-7}$	$4,04 \times 10^{-6}$
$0,80$	$4,99 \times 10^{-6}$	$3,83 \times 10^{-5}$	$1,22 \times 10^{-6}$	$1,62 \times 10^{-7}$	$3,99 \times 10^{-6}$
$1,00$	$4,97 \times 10^{-6}$	$3,82 \times 10^{-5}$	$1,12 \times 10^{-6}$	$1,45 \times 10^{-7}$	$3,98 \times 10^{-6}$

Tableau 3.11: Fréquence des conséquences de l'arbre des événements par approche floue - adapté d'après Ferdous et al. [2009].

Chapitre 4

Approche dynamique du graphe du nœud papillon

Dans cette présentation, l'objectif recherché consiste à promouvoir la prise en compte dynamique du graphe du nœud papillon, d'une part par approche bayésienne et d'autre part par application de la logique floue.

4.1 La méthode conventionnelle du graphe du nœud papillon

4.1.1 Principe de la méthode

La méthode du nœud papillon a pour objet d'analyser l'évolution globale des défaillances d'un système, via des scénarios d'accidents, depuis leurs causes initiales et leurs combinaisons jusqu'à la nature et l'ampleur des conséquences et d'en traduire graphiquement la représentation. Schématiquement la méthode du nœud papillon centré sur un Evénement Redouté Central (ERC) établit un lien entre les causes et les conséquences de cet événement. Plus précisément la méthode du nœud papillon a pour principe de combiner un arbre de défaillances et un arbre d'événements respectivement disposés en amont et en aval d'un Evénement Redouté Central. Comme l'arbre des défaillances relève d'une méthode déductive inverse alors que l'arbre des événements résulte d'une méthode inductive directe, la méthode du noeud papillon allie les deux approches déductive et inductive. La figure 4.1 illustre une représentation d'un scénario d'accident selon le diagramme générique du noeud papillon.
Le point central du nœud papillon, soit l'Evénement Redouté Central (ERC), désigne soit une perte de confinement pour un fluide, soit une perte d'intégrité physique pour un solide (par exemple une décomposition). La partie gauche du nœud papillon est un arbre des défaillances permettant d'identifier les causes générant l'Evénement Redouté Central. La partie droite est un arbre d'événements déterminant les conséquences de l'Evénement Redouté Central. Les barrières de sécurité illustrent leur rôle d'opposition au déroulement des scénarios d'accidents. Il est ainsi possible de visualiser chaque chemin potentiel d'un scénario d'accident de ses causes initiales à ses conséquences finales sur les cibles.

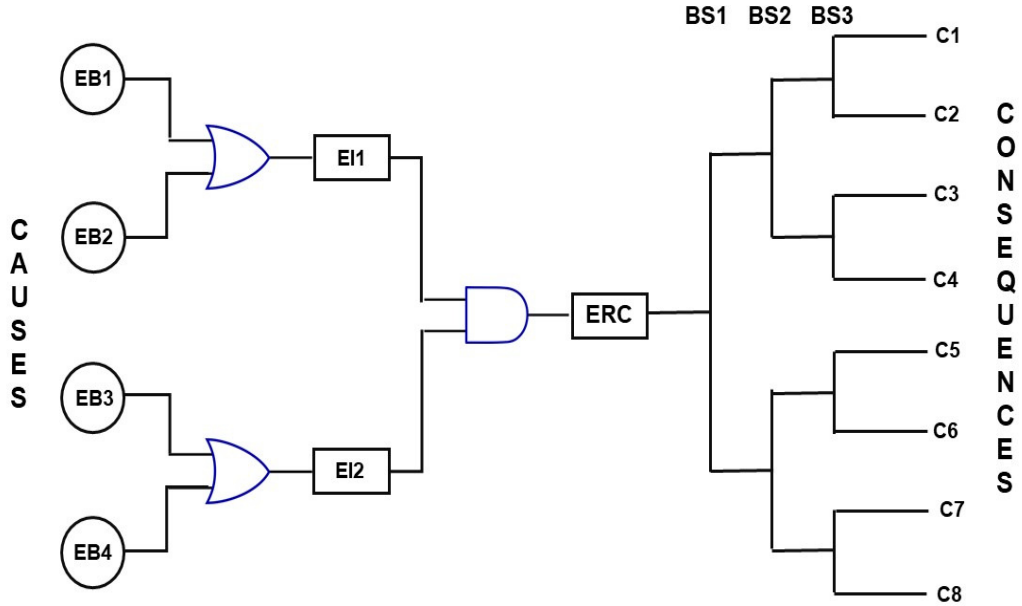

Figure 4.1: Graphe du modèle générique du nœud papillon - adapté d'après Khakzad et al. [2013].

4.1.2 Application de la méthode du nœud papillon

La méthode du nœud papillon peut être appliquée soit qualitativement, soit quantitativement.

4.1.2.1 Application qualitative

Son utilisation qualitative est maintenant courante. Elle permet de visualiser très simplement les divers scénarios d'accidents. Elle illustre clairement la place et le rôle des différentes barrières en aidant ainsi à la formalisation de la démarche de maîtrise des risques. La méthode du nœud papillon est appliquée classiquement, du point de vue qualitatif, a priori pour identifier et analyser les scénarios d'accidents majeurs. Mais son emploi a posteriori lors du retour d'expérience est également intéressante.

4.1.2.2 Application quantitative

Son utilisation quantitative est très utile dans l'approche probabiliste de la maîtrise des risques, malgré sa mise en oeuvre plus délicate, détaillée et coûteuse. D'après Iddir [2008] la quantification de la méthode du nœud papillon, dont l'objectif consiste à estimer les probabilités d'occurrence des dommages et conséquences (décès, blessés, dégâts matériels et pollutions...), nécessite préalablement d'évaluer celles de l'Evénement Redouté Central. Il est ensuite néces-

saire de recenser et d'affecter les probabilités de défaillances des barrières d'atténuation et de protection de l'arbre des événements avant d'en déduire les probabilités des dommages. L'auteur indique que les trois étapes de la quantification de la méthode du nœud papillon sont:

- évaluation de l'occurrence de l'Evénement Redouté Central;
  - soit de manière directe en se référant aux banques de donnés d'accidentologie quantifiée;
  - soit de manière estimée par le calcul à partir de la connaissance des probabilités des événements initiaux constitutifs de l'arbre des défaillances et des règles de calcul associées aux portes logiques présentes.
- estimation des probabilités des défaillances des barrières de détection et de protection prévues pour limiter les conséquences de l'Evénement Redouté Central;
- évaluation des probabilités des dommages à partir des deux étapes précédentes.

Iddir [2008] a discuté les incertitudes et erreurs liées à la quantification pour les données d'entrée et lors de la propagation des erreurs en amont et en aval de l'Evénement Redouté Central. Il a aussi précisé les précautions et les limites d'utilisation des banques de données.
Cette approche d'évaluation quantitative reste cependant insuffisante. En effet, comme le graphe du nœud papillon est constitué d'un arbre de défaillances et d'un arbre d'événements, il souffre des limitations des deux constituants d'événements. Par exemple, les arbres de défaillance standard ne conviennent pas aux scénarios d'accident dans lesquels des défaillances redondantes, de cause commune ou dépendantes se produisent. Les arbres de défaillance sont également incapables d'incorporer des variables multi-états, qui sont fréquemment rencontrées dans la modélisation des systèmes de procédés. Mais aussi de façon plus pénalisante, en raison de leurs structures statiques, les arbres de défaillance et les arbres d'événements ne peuvent pas s'adapter à la dynamique des accidents. En d'autres termes, ces techniques ne peuvent pas utiliser les informations en temps réel directement obtenues de l'installation pour mettre à jour les données antérieures, comme les probabilités de défaillance antérieures des événements primaires et des barrières de sécurité. Pour améliorer les limites de cette approche, il est possible d'utiliser l'inférence bayésienne, dans laquelle la gestion de l'incertitude et la mise à jour des données sont des caractéristiques inhérentes à cette inférence.

4.2 L'approche bayésienne du graphe du nœud papillon

4.2.1 Notion de réseaux bayésiens

Le fondement des réseaux bayésiens s'appuie sur le théorème de Bayes, qui peut s'exprimer par les équations suivantes :

$$P(A|B)\,P(B) = P(A \cap B) = P(B|A)\,P(A] \tag{4.1}$$

où

- le terme P(A) est la probabilité a priori de A, appelée aussi probabilité marginale de A; elle est antérieure au sens qu'elle précède toute information sur B;
- le terme P(A|B) est appelée la probabilité a posteriori de A sachant B (ou encore de A sachant B). Elle est postérieure, au sens qu'elle dépend directement de B;
- le terme P(B|A), pour un B connu, est appelée la fonction de vraisemblance de A;
- le terme P(B) est appelé la probabilité marginale ou a priori de B.

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)} \tag{4.2}$$

Un réseau bayésien est un système représentant la connaissance et permettant de calculer des probabilités conditionnelles apportant des solutions à différentes sortes de problématiques. La structure de ce type de réseau est simple et comprend:

- un graphe acyclique orienté dans lequel les nœuds représentent des variables aléatoires et les arcs reliant ces dernières qui traduisent les relations entre variables qui sont soit déterministes, soit probabilistes. Ainsi, l'observation d'une ou plusieurs causes n'entraîne pas systématiquement l'effet ou les effets qui en dépendent, mais modifie seulement la probabilité de les observer;
- des tables des probabilités conditionnelless de chaque variable, chacune des variables dispose d'une table de probabilités conditionnelles relatives aux variables causales dont elle dépend.

L'inférence bayésienne est basée sur l'utilisation d'énoncés probabilistes, qui dans le cas général sont proposés par des experts étudiant le système. La clarté et la précision des dires d'experts sont importantes, afin d'éviter toute confusion dans les relations de dépendance qui en découleront. Les méthodes bayésiennes se distinguent des méthodes dites standard par l'application systématique de règles formelles de transformation des probabilités. On cherche à induire sur un système bayésien aussi bien par le haut que par le bas, aussi bien les conséquences que les causes, du graphe de dépendance. Les règles d'addition et de multiplication de la logique des probabilités utilisées sont respectivement les suivantes:

$$P(A \cup B|C) = P(A|C) + P(B|C) - P(A \cap B|C) \tag{4.3}$$

$$P(A \cap B) = P(A|B)\,P(B) = P(B|A)\,P(A) \tag{4.4}$$

Le théorème de Bayes peut être retrouvé simplement en mettant à profit la symétrie de la règle de multiplication

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)} \tag{4.5}$$

La puissance du théorème de Bayes permet d'inverser les probabilités. C'est-à-dire que si l'on connaît les conséquences d'une cause, l'observation des effets permet de remonter aux causes,

c'est l'effet d'induction du bas vers le haut. Une lecture littérale du théorème de Bayes permet aussi une induction du haut vers le bas, c'est à dire à partir des causes en déduire les conséquences. Mais il est aussi possible d'envisager de réfuter une cause en en constatant une autre, autrement dit partir d'une conséquence pour remonter aux causes, constater laquelle est vraie et réfuter les conséquences sous jacentes des autres causes. En résumé, pour induire sur un réseau bayésien, il faut en premier lieu trouver les probabilités conditionnelles de chaque variable aléatoire avec lesquelles elles sont directement dépendantes. Ce que les experts font à partir des statistiques étudiées sur le système voulu. Puis partir de faits produits auxquels on appliquera une probabilité de 1 ou 0 sur le réseau bayésien suivant qu'ils identifient une variable vraie ou fausse dans celui ci. Et enfin par le biais de calcul respectant la règle d'addition et ou de multiplication précédemment décrite, on modifie les probabilités causales et ou conséquentes. La nouvelle probabilité obtenue est l'induction que l'on peut faire sur un réseau bayésien. Il existe des logiciels pour traiter les algorithmes d'inférence comme par exemple Matlab `http://www.mathworks.fr/`, Bayesia `http://www.bayesia.fr` ou Hugin `http://www.hugin.com`.

4.2.2 Transposition d'un graphe nœud papillon en réseau bayésien

La transposition d'un graphe nœud papillon en réseau bayésien s'effectue par étapes successives. Khakzad et al. [2013] ont proposé l'algorithme simplifié de transposition d'un graphe nœud papillon en réseau bayésien de la figure 4.2.

Il est d'abord nécessaire de convertir respectivement l'arbre des défaillances et l'arbre des événements.
Pour l'arbre des défaillances, la partie gauche de la figure 4.3 montre la conversion d'une porte OU et d'une porte ET en nœuds équivalents dans la topologie bayésienne. Les nœuds parents A et B se voient attribuer des probabilités préalables coïncidant avec les valeurs de probabilité attribuées aux nœuds de base correspondants dans l'arbre des défaillances et le nœud enfant C se voit attribuer sa table de probabilités conditionnelles. Étant donné que les portes OU et ET représentent des relations causales déterministes, toutes les entrées correspondantes de la table sont des valeurs 0 ou 1.

Pour l'arbre des événements, chaque barrière de sécurité est représentée par un nœud de sécurité ayant deux états, l'un pour l'échec et l'autre pour la réussite de la barrière de sécurité. De même, un nœud de conséquence ayant autant d'états que le nombre de conséquences de l'arbre des événements est ajouté au réseau.

Une fois que les représentations bayésiennes équivalentes de l'arbre de défaillance et de l'arbre des événements sont développées, elles sont connectées l'une à l'autre via l'intermédiaire du nœud pivot, équivalent de l'Evénement Redouté Central. Le nœud pivot est connecté au nœud de conséquence. Un autre état, par exemple l'état de sécurité, est également connecté au nœud de conséquence. La partie droite de la figure 4.3 illustre ainsi le graphe générique du réseau bayésien potentiellement équivalent au graphe du nœud papillon de la figure 4.1.

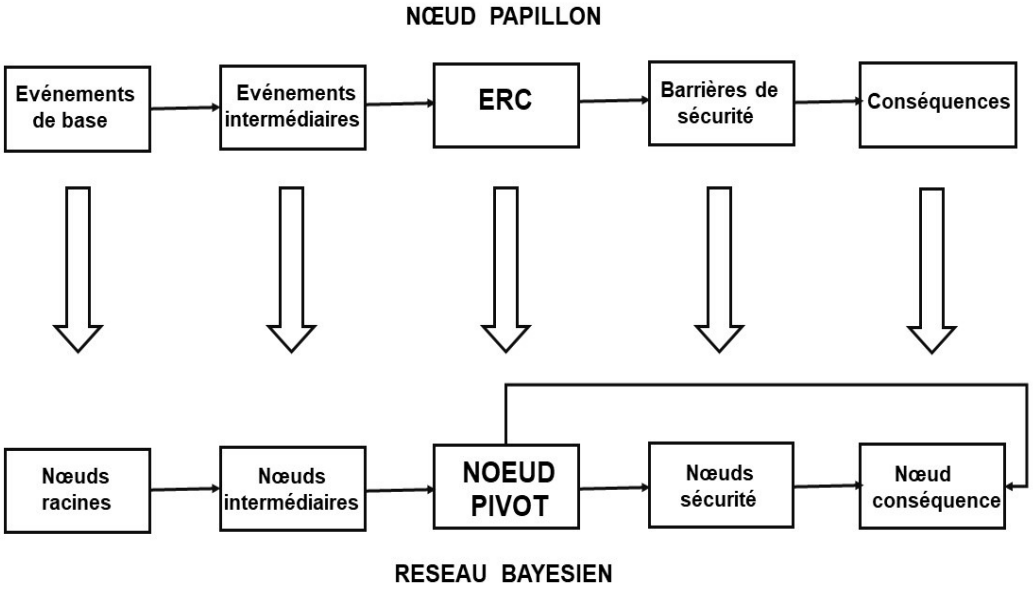

Figure 4.2: Algorithme simplifié de transposition d'un graphe nœud papillon en réseau bayésien - adapté d'après Khakzad et al. [2013].

4.3 Exemple d'application à l'ignition de vapeur inflammable issue d'un réservoir de mélange

Il est proposé d'appliquer les méthodes respectives du graphe du nœud papillon et du réseau bayésien à l'analyse d'un accident, dû à l'allumage d'un nuage de vapeur généré par le mélange et le chauffage d'un liquide inflammable dans un réservoir ouvert, sans dispositifs de sécurité adéquats. Les conséquences ont entrainé le décès d'une personne, les blessures de deux autres personnes, dont une grièvement et une interruption de l'activité de l'installation.

4.3.1 Description de l'accident

L'accident étudié a eu lieu le 16 Juin 2006 dans l'entreprise Universal Clamp Inc à Bellwood, Illinois (USA). Selon le rapport documenté et publié par l'US Chemical Safety Board, le scénario probable d'accident résulte de l'inflammation d'un nuage de vapeur, composé d'heptane et d'essence minérale, qui a débordé d'un réservoir ouvert de mélange et de chauffage [CSB, 2007]. Le réservoir était équipé de serpentins à vapeur, qui lui fournissaient la chaleur nécessaire au processus de mélange. Un régulateur de température composé d'un capteur de température et d'une unité de commande pneumatique a été installé pour actionner les vannes à vapeur

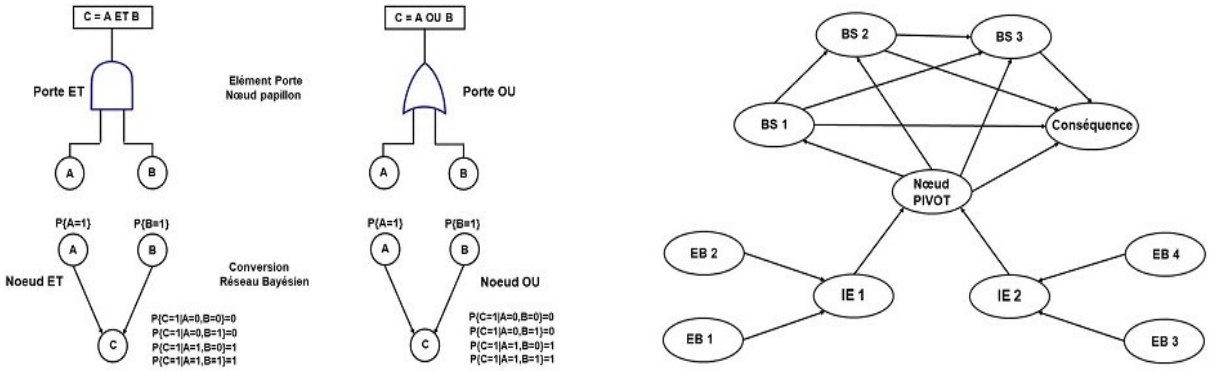

Figure 4.3: Représentations respectives des portes OU et ET dans le graphe du nœud papillon et du réseau bayésien (partie gauche) et Graphe générique du réseau bayésien équivalent au graphe d'un nœud papillon (partie droite) - adapté d'après Bobbio et al. [2001] et Khakzad et al. [2013]
.

en fonction de la température du mélange. En plus de ce système de contrôle, un opérateur était censé vérifier la température à l'aide d'un thermomètre infrarouge et décider des actions éventuelles nécessaires. Le réservoir était également équipé d'une ventilation locale en aspiration par le haut pour éviter l'accumulation des vapeurs. Selon l'enquête post accidentelle, un dysfonctionnement du système de contrôle de la température a permis aux vannes de vapeur de rester ouvertes suffisamment longtemps pour chauffer le mélange jusqu'à son point d'ébullition, générant un volume important de vapeur. En raison d'une rupture de la courroie du ventilateur, la défaillance du système de ventilation locale a conduit à la formation d'un nuage de vapeur, qui s'est échappé du réservoir et s'est finalement enflammé lorsqu'il a été exposé à une source d'inflammation, dont l'identification est restée indéterminée. Il a également été constaté que même si le système de ventilation avait fonctionné, il n'aurait pas eu la capacité suffisante pour collecter un tel volume de vapeur. Les détails complémentaires de l'enquête et leurs illustrations sont consultables dans le rapport CSB [2007].

4.3.2 Application du graphe du nœud papillon

La description détaillée de l'accident et une analyse préliminaire des risques ont permis de construire un graphe du nœud papillon pour examiner les scénarios envisageables et vérifier l'efficacité de différentes mesures de maîtrise des risques. Les différents éléments et événements constitutifs du graphe sont regroupés dans le tableau 4.1. Les valeurs indiquée des différentes probabilités de défaillance résultent des dires d'experts et des banques de données. Il convient de noter que les probabilités de défaillance des barrières de sécurité "Sprinkler" et "Alarme" sont influencées soit par la barrière de sécurité "Ignition", soit par l'ERC Vapeur, ce qui montre la dépendance conditionnelle de la première par rapport à la seconde. L'arrosage et l'alarme sont activés en cas d'inflammation des vapeurs, c'est-à-dire lorsque "ERC Vapeur = Débordement" et "Ignition = Étincelle", mais avec des probabilités d'échec égales à 0,04 et à 0,0013 respectivement. D'autre part, l'alarme peut également être stimulée par une certaine

concentration de vapeur dans l'air, même si elle n'est pas allumée, même si elle n'est pas enflammée, c'est-à-dire lorsque "ERC Vapeur = Débordement" et "Ignition = Pas d'étincelle", mais avec une probabilité de défaillance égale à 0,2250.

Repère	Nature de l'événement	Probabilité de défaillance
EB 1	Sonde capteur	0,0400
EB 2	Unité pnematique	0,2015
IE 1	Système de contrôle de la température	porte OU
EB 3	Opérateur	0,0200
EB 4	Thermomètre infra rouge	0,0468
IE 2	Systéme de mesure de la température	porte OU
EB 5	Vanne manuelle vapeur	0,0243
EB 6	Vanne automatique vapeur	0,0276
IE 3	Systèma automatique de contrôle température	porte OU
IE 4	Système manuel de contrôle température	porte OU
IE 5	Systèle de protection température haute	porte ET
EB 7	Ventilation inadéquate	0,0150
EB 8	Défaillance ventilateur	0,0100
EB 9	Défaillance courroie	0,0500
EB 10	Empoussièrage	0,0010
IE 6	Système de ventilation	porte OU
ERC	Débordement vapeur	porte ET
BS 1	Barrière d'ignition	0,1000
BS 2	Systène de sprinkler eau	0,0400
BS 3	Système d'alarme	0,0013; 0,2250

Tableau 4.1: Eléments, événements et probabilités de défaillance de construction du graphe du nœud papillon - d'après Khakzad et al. [2013].

Le tableau 4.2 récapitule la liste des huit conséquences potentielles du scénario d'accident de débordement de vapeur inflammable, mais non toxique. Il est supposé que même s'il n'y a pas d'incendie (c'est-à-dire qu'il n'y a pas d'étincelle), le fonctionnement de l'arrosage sprinkler conduira à un mode plus sûr que sa défaillance. Cela s'explique par le fait que le fonctionnement du sprinkler peut éventuellement réduire la probabilité d'inflammations ultérieures (inflammations retardées). Ainsi, les conséquences C1 et C2 sont respectivement moins graves que les conséquences C3 et C4.

Repère	Expression de la conséquence
C1	Evacuation en sécurité
C2	Nuage de vapeur humide près du sol
C3	Evacuation en toute sécurité avec possibilité d'inflammation retardée
C4	Nuage de vapeur avec possibilité d'inflammation retardée
C5	Incendie, dégâts matériels modérés, faible nombre de décès
C6	Incendie, dégâts matériels modérés, nombre élevé de décès
C7	Incendie, dégâts matériels importants, faible nombre de décès
C8	Incendie, dégâts matériels importants, nombre élevé de décès

Tableau 4.2: Liste des conséquences du scénario d'accident de débordement de vapeur - adapté d'après Khakzad et al. [2013].

La figure 4.4 présente, à l'aide des repères des tableaux 4.1 et 4.2, le graphe du nœud papillon du scénario d'accident du débordement de vapeur inflammable.

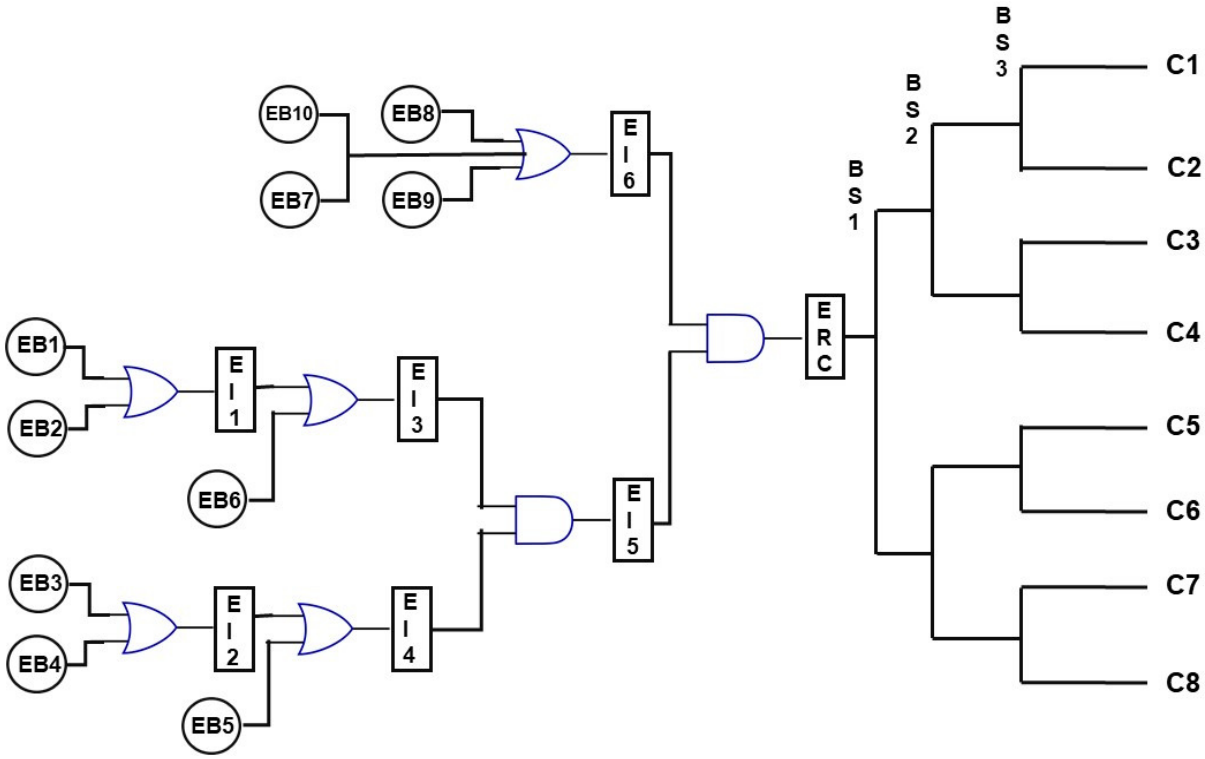

Figure 4.4: Graphe du nœud papillon du scénario d'accident - adapté d'après Khakzad et al. [2013].

L'attribution des probabilités énumérées dans le tableau 4.1 aux événements primaires et aux barrières de sécurité du graphe du nœud papillon permet de calculer classiquement les probabilités de l'Evénement Central Redouté (ERC) et les conséquences de l'accident présentées dans le tableau 4.3.

4.3.3 Analyse du réseau bayésien

La transposition du graphe du noeud papillon de la figure 4.4, à l'aide l'algorithme simplifié indiqué sur la figure 4.2 de la section 4.2.2 en graphe du réseau bayésien est proposée sur la figure 4.5.
Tous les nœuds du réseau bayésien, qui correspondent aux éléments et événements précédemment décrits dans le graphe du nœud papillon, sont présents, à l'exception du nœud "Conséquence", qui est ajouté pour tenir compte des résultats du graphe papillon. En connectant le nœud PIVOT (Vapeur) au nœud "Conséquence", un autre état dit sûr, à savoir "C1 - Evacuation en sécurité" est ajouté à l'ensemble d'états comprenant les conséquences pour tenir compte de la non-occurrence de l'événement PIVOT, c'est-à-dire "Vapeur sous contrôle". Pour montrer la dépendance entre les barrières de sécurité et le nœud PIVOT, des arcs de causalité sont

Repère	Probabilité
ERC	$1,68 \times 10^{-3}$
C1	$0,00$
C2	$0,00$
C3	$1,04 \times 10^{-3}$
C4	$3,03 \times 10^{-4}$
C5	$3,23 \times 10^{-4}$
C6	$4,21 \times 10^{-7}$
C7	$1,35 \times 10^{-5}$
C8	$1,75 \times 10^{-8}$

Tableau 4.3: Résultats quantitatifs de l'analyse par le graphe du nœud papillon du scénario d'accident de débordement de vapeur - adapté d'après Khakzad et al. [2013].

également tracés à partir des nœuds "BS1 - Ignition" et PIVOT (Vapeur) vers les nœuds "BS2 - Sprinkler" et "BS3 - Alarme". A titre d'exemple, la table des probabilités conditionnelles du nœud "BS3 - alarme" est intégrée à la figure 4.5. Etant donné que diverses combinaisons d'échec et de succès des barrières de sécurité séquentielles entraînent des conséquences différentes dans le graphe papillon, il convient de noter que tous les nœuds de sécurité du graphe acyclique du réseau bayésien sont connectés au nœud "Conséquence".
En attribuant les probabilités listées dans le tableau 4.1 en tant que valeurs a priori ou antérieures, le réseau bayésien est analysé à l'aide du logiciel HUGIN 7.4 (`http://www.hugin.com`). Khakzad et al. [2013] ont ainsi obtenu les mêmes probabilités que celles estimées initialement lors de l'analyse quantitative du graphe du nœud papillon et indiquées dans le tableau 4.3. Ce résultat montre le bien fondé de la démarche proposée pour analyser un scénario d'accident.
Khakzad et al. [2013] ont ensuite expliqué l'intérêt d'utiliser en dynamique le réseau bayésien pour mettre à jour les probabilités en tenant compte des preuves, tâche que le graphe du nœud papillon classique n'est pas en mesure d'effectuer. Deux types de mise à jour des probabilités peuvent être réalisées à l'aide du réseau bayésien en fonction de la nature de preuve propagée dans le réseau. La première possibilité, communément appelé mise à jour des probabilités, calcule la probabilité postérieure de l'événement x_i étant donné la présence de l'événement Q, c'est-à-dire la probabilité de l'événement sachant Q, soit $P(x_i|Q)$. Cette procédure est généralement utilisée pour trouver l'explication la plus probable des événements, qui ont conduit à l'accident ou à une conséquence spécifique. La seconde opportunité, appelée adaptation des probabilités, calcule la probabilité postérieure de l'événement x_i, étant donné que l'événement Q s'est produit n fois, soit $P(x_1|Q = n)$. L'expérience antérieure est exploitée pour effectuer la mise à jour des probabilités. Les distributions a priori de probabilités conditionnelles sont adaptées à l'aide des informations cumulées collectées en ligne au cours d'un intervalle de temps comme preuve pour estimer les probabilités dites postérieures. L'article de Khakzad et al. [2013] illustre cette double approche quantitative dynamique à l'aide de l'exemple du scénario de l'accident examiné.

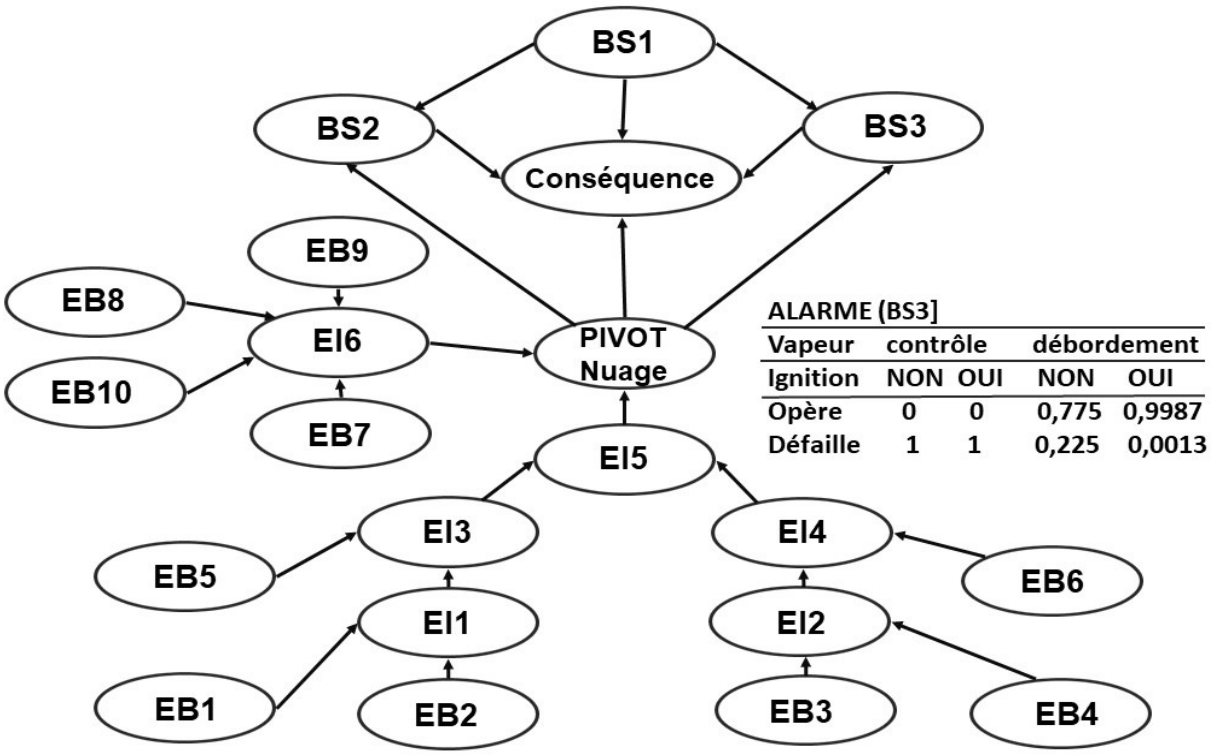

Figure 4.5: Graphe du réseau bayésien du scénario d'accident - adapté d'après Khakzad et al. [2013].

4.4 Application de la logique floue au graphe du nœud papillon

Pour mémoire, l'introduction, l'objectif, l'approche et le traitement par logique floue de la sécurité des procédés ont déjà été présentés dans la section 3.4 lors de l'examen de l'analyse d'un arbre des événements.

4.4.1 Modèle de logique floue d'un nœud papillon

Le modèle, proposé par Markowski et al. [2009] et présenté par le logigramme de la figure 4.6, comprend deux parties:

- la partie traditionnelle centrée sur l'identification du graphe du nœud papillon;
- la partie logique floue liée au calcul de la probabilité de l'événement résultat conséquence.

La première partie réalise l'identification de scénarios d'accidents représentatifs en construisant le graphe du nœud papillon à l'aide de l'arbre des défaillances (FT) et de l'arbre des événements (ET). Compte tenu de la structure des scénarios, les ensembles respectifs des coupes

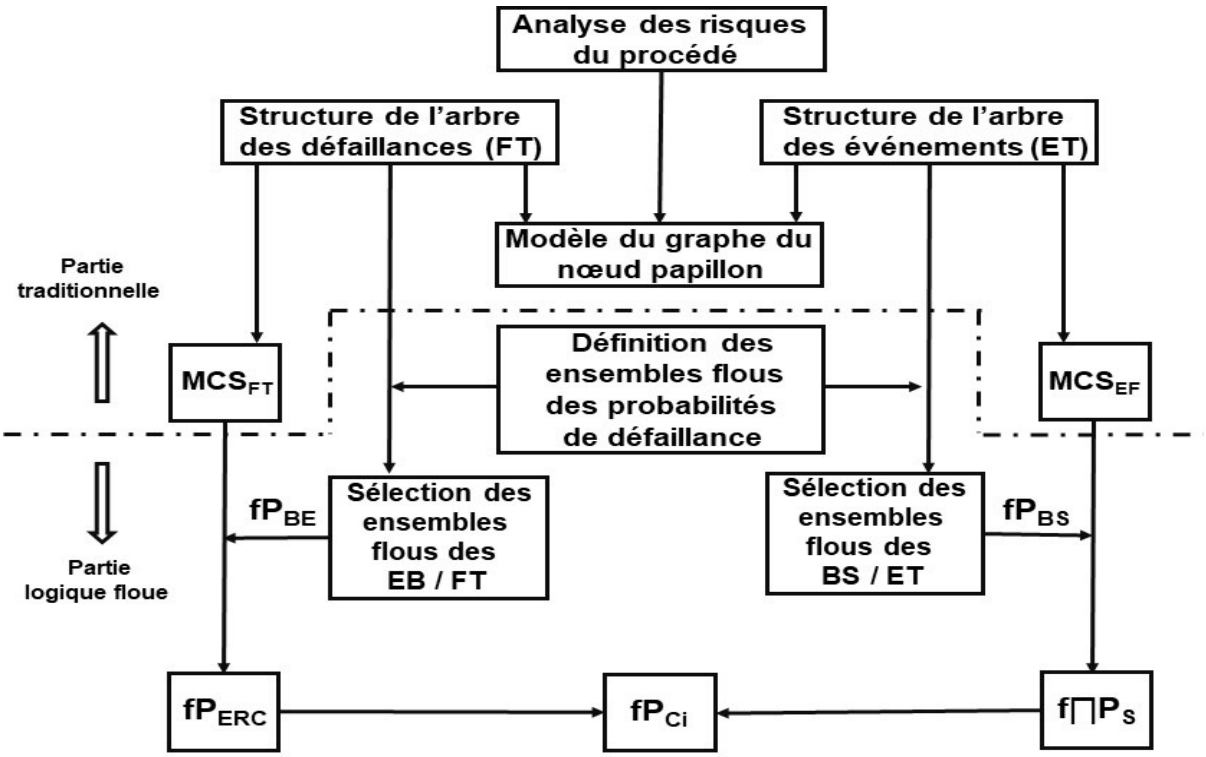

Figure 4.6: Modèle de logique floue d'un graphe nœud papillon - adapté d'après Markowski et al. [2009].

minimales (MCS_{FT}) et (MCS_{ET}) de chacun des arbres peuvent être obtenus par l'algèbre booléenne.
En supposant l'indépendance entre les éléments de base BE_i de l'arbre des défaillances, l'expression quantitative de la coupe MCS_{FT} s'écrit:

$$MCS_{FT} = \sum_{i=1}^{n} \left(\prod_{i=1}^{i} (BE)_i, \prod_{j=1} j(BE)_j, ..., \prod_{k=1}^{k} (BE)_k \right)_n \tag{4.6}$$

La coupe minimale relative aux conséquences MCS_{ET} est estimée en fonction de l'Evénement redouté Central (ERC) et des barrières de sécurité (BS) par la relation:

$$MCS_{EF} = ERC \times \prod_{m=1}^{m} (BS)_m \tag{4.7}$$

L'utilisation des équations 4.6 et 4.7 implique la connaissance des probabilités de défaillances respectives des éléments de base et des barrières.
La deuxième partie de l'analyse prend en compte la théorie des ensembles flou. Elle concerne la quantification de la probabilité de chaque scénario ainsi que l'évaluation de la gravité des conséquences selon les équations 4.6 et 4.7. En conséquence, la probabilité floue de l'événement

de sortie est ainsi obtenue.
Markowski et al. [2009] ont précisé les conditions d'application de la démarche:

- les probabilités des défaillances des événements de base EB_i et des barrières de sécurité BS_i sont exprimées par les termes linguistiques (I) impossible, (VL) très faible, (L) faible, (M) modéré, (FH) assez fort, (H) fort et (VH) très fort;

- chaque terme linguistique est associé à un nombre flou spécifique de type L - R ici de forme trapézoïdale, dont l'écriture symbolique est:

$$M = (x, \underline{m}, \underline{n}, \bar{n}, \bar{m}) \tag{4.8}$$

- la fonction de vraisemblance du nombre flou est donnée par l'équation:

$$\mu_m(x) = \left\{ \begin{array}{cc} 0 & x \leq \underline{m} \\ \frac{x-\underline{m}}{\underline{n}-\underline{m}} & \underline{m} < x \leq \underline{n} \\ 1 & \underline{n} \leq x \leq \bar{n} \\ \frac{\bar{m}-x}{\bar{m}-\bar{n}} & \bar{n} \leq x \leq \bar{m} \\ 0 & \bar{m} \leq x \end{array} \right\} \tag{4.9}$$

- L'ordre de grandeur de référence le plus approprié pour l'éventail des probabilités de taux de défaillance habituellement rencontrées dans l'industrie est compris entre 10^{-6} et 10^{0}.

A titre d'illustration, la figure 4.7 indique le profil trapézoïdal d'un nombre flou (partie gauche) et l'échelle floue normalisée établie par les experts (partie droite).

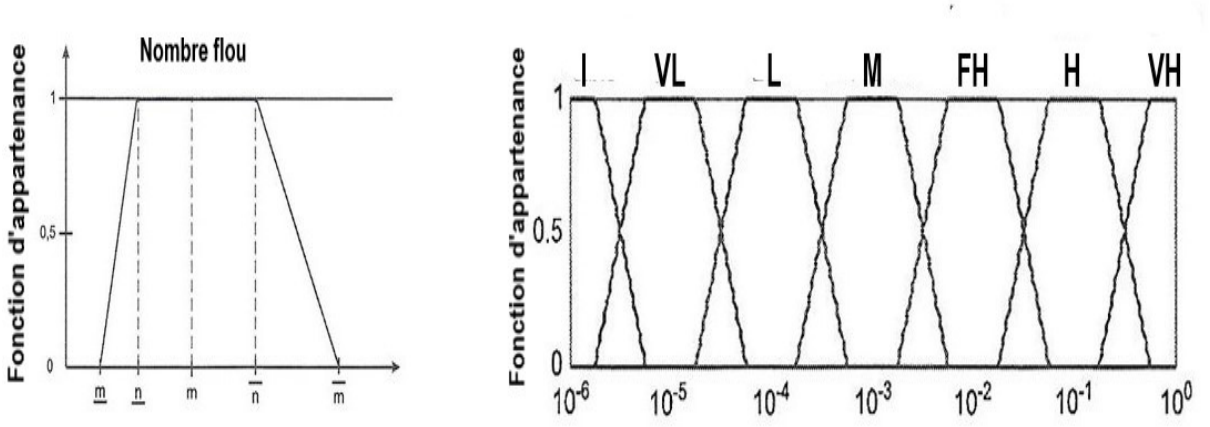

Figure 4.7: Exemples d'un nombre flou trapézoïdal (gauche) et de l'échelle floue normalisée de correspondance (droite) - adapté d'après Markowski et al. [2009].

4.4.2 Application du modèle de logique floue à l'analyse de sécurité d'un réservoir de stockage d'isobutane

La figure 4.8 présente le réservoir sphérique instrumenté de stockage d'isobutane. Le volume, la température et la pression sont respectivement de 300 m^3, 35°C et 3,27 bar. Une analyse des risques du procédé a permis d'identifier une dizaine de scénarios d'accident, dont en particulier celui de la rupture du réservoir par surremplisage et défaillance d'une couche de protection de maîtrise des risques. Les différents conséquences consécutives à ce scénario dépendent de l'inflammation ou non de l'isobutane. En l'absence d'inflammation, la conséquence retenue est la dispersion du nuage. En cas d'ignition les conséquences possibles examinées dans cette étude de cas sont le feu de nappe, l'explosion du nuage de vapeur et le feu flash.

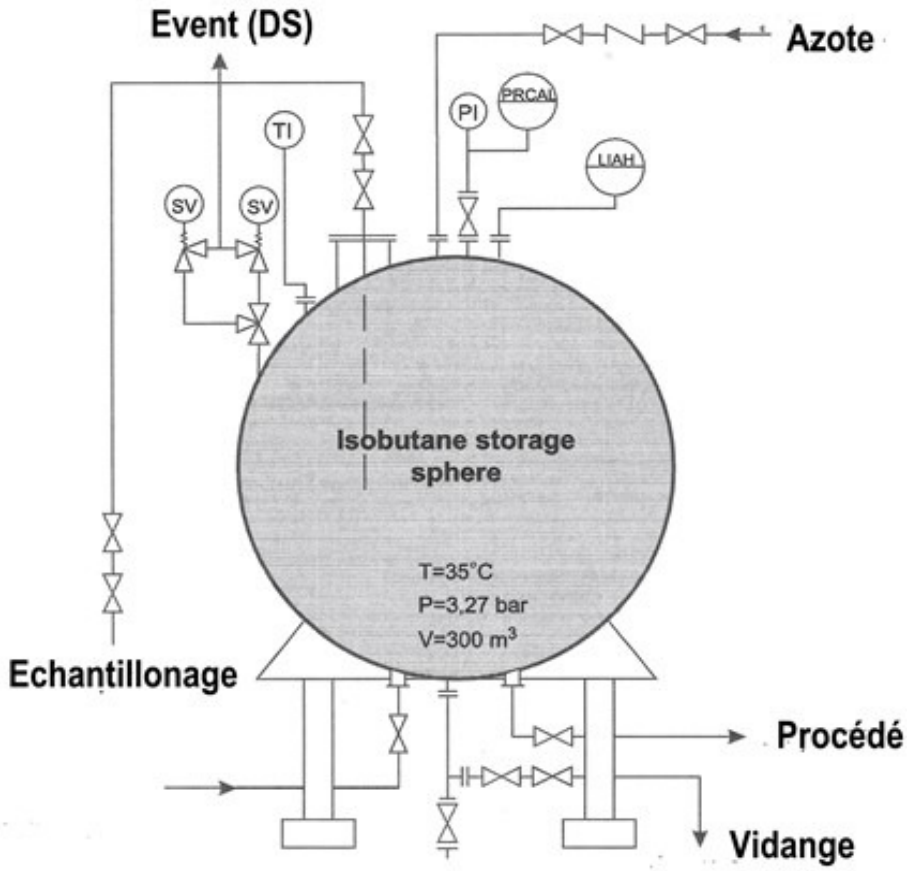

Figure 4.8: Schéma instrumenté du réservoir sphérique de stockage d'isobutane - adapté d'après Markowski et al. [2009].

En considérant les événements de base EB1-défaillance de l'indicateur de niveau alarme haute LIAH, EB2 défaillance de l'indicateur de pression PI, EB3 erreur de l'opérateur, EB4 défaillance de la soupape de sécurité SV et EB5 défaillance de l'évent DS, les éléments intermédiaites EI1 défaillance du système de contrôle de base du procédé BPCS, EI2 surremplissage et EI3 dé-

faillance d'une couche de protection, l'ERC rupture du réservoir, les fonctions de sécurité BS1 ignition immédiate et BS2 ignition retardée et les conséquences C1 feu de nappe, C2 explosion du nuage de vapeur et feu flash et C3 dispersion du nuage, il est possible de construire le graphe du nœud papillon du scénarion de ruptue du réservoir de la figure 4.9.

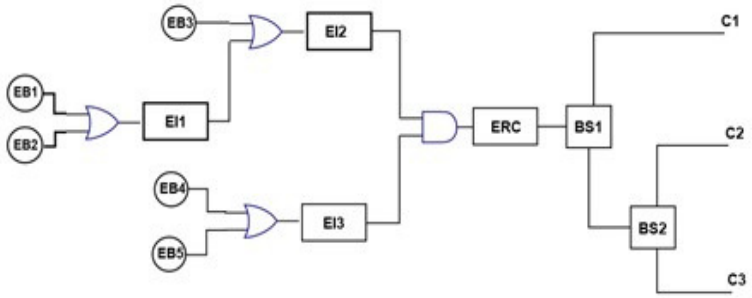

Figure 4.9: Graphe du nœud papillon de la rupture du stockage d'isobutane - adapté d'après Markowski et al. [2009].

Les probabilités floues des éléments de base et des fonctions de sécurité sont choisies arbitrairement par les ingénieurs procédés et les experts sur la base de l'échelle floue normalisée de la figure 4.7. Le détail des calculs de la probabilité floue de résultats utilisent des opérations arithmétiques sur des nombres flous. Le calcul final de la probabilité floue de chaque conséquence suivant l'équation appropriée pour chaque coupe minimale de la branche du modèle du nœud papillon représentant le scénario concerné d'accident est détaillé dans l'article de Markowski et al. [2009].

Evénement	Méthode floue	Méthode classique
	Probabilité	Probabilité
ERC	$4,40 \times 10^{-3}$	
C1	$4,37 \times 10^{-4}$	$3,87 \times 10^{-4}$
C2	$4,98 \times 10^{-5}$	$3,87 \times 10^{-5}$
C3	$5,53 \times 10^{-6}$	$4,20 \times 10^{-6}$

Tableau 4.4: Comparaison des probabilités défuzzifiées et des probabilités classiques du graphe nœud papillon pour les conséquences examinées - adapté d'après Markowski et al. [2009].

Le tableau 4.4 présente pour chacune des conséquences une comparaison des probabilités défuzzifiées précises avec celles de la méthode classique du graphe du nœud papillon. Markowski et al. [2009] estiment que les valeurs calculées par la logique floue sont environ inférieures de 10% à celles de la méthode traditionnelle. Ils considèrent que la méthode de logique floue, qui tient compte des incertitudes des données d'entrée, conduit à des estimations plus précises. Ces auteurs soulignent aussi que la valeur défuzzifiée exacte permet d'afficher le pourcentage de contribution de chaque nombre de probabilité floue dans l'ensemble flou représentant la plage de probabilité floue, ce que ne permet pas la méthode traditionnelle. Par exemple, dans le cas de

la conséquence C2 de l'explosion du nuage de vapeur et du feu flash, la valeur de la probabilité défuzzifiée de $4,98 \times 10^{-5}$ indique que cette probabilité appartient à deux ensembles: Faible (L) avec un degré d'appartenance de 86% et Très faible (VL) dans 14% des cas. La distance de cet ensemble particulier par rapport à l'appartenance 100% est donc clairement mis en évidence. Enfin il ne faut pas oublier que la pertinence du modèle de logique floue d'un nœud papillon dépend évidemment de la qualité des données de défaillance collectées dans le procédé.

Pour aller plus loin

- Modélisation dynamique du risque de sécurité des procédés à l'aide d'un réseau bayésien - Analyse des risques d'un système de stockage de liquides inflammables dans une raffinerie.
Documentation: Zarei et al. [2017].
- Evaluation dynamique de la sécurité des installations urbaines de distribution de gaz naturel à l'aide d'un réseau bayésien.
Documentation: Zarei et al. [2017a].
- Analyse bayésienne comparative des risques de différents systèmes de distribution et de transport d'hydrogène comprimé ou liquéfié.
Documentation: Pasman and Rogers [2012].

Chapitre 5

Approche dynamique de la méthode LOPA

La méthode LOPA fondée sur la notion de couche de protection, décrite dans la norme IEC 61511 relative à la sécurité fonctionnellle et aux systèmes instrumentés de sécurité, est une méthode semi-quantitative d'analyse et d'évaluation des risques, où la fréquence et la gravité d'une conséquence sont exprimées en termes d'ordre de grandeur. Ce modèle simple peut être amélioré en quantifiant l'incertitude des probabilités des défaillances résultant des données génériques des bases, des données spécifiques du procédé et des dires d'experts. L'objectif de l'approche proposée dans cette partie concerne les apports respectifs des réseaux bayésiens et la logique floue pour cette amélioration.

5.1 Principe et structure de la méthode LOPA

La méthode LOPA (Layer Of Protection Analysis) est une méthode intégrée semi quantitative d'analyse probabiliste des risques. Elle a été initiée par le Center for Chemical Process Safety (CCPS) sur la base du modèle des couches de protection [CCPS, 2001]. La méthode LOPA propose d'évaluer les mesures de maîtrise des risques fondées sur l'approche "barrières" en analysant la contribution des différents couches successives. La figure 5.1 illustre les différentes couches successives (IPL) associées à un possible scénario d'accident.
Elle est utilisée pour déterminer entre autres les probabilités de défaillance des différentes mesures de maîtrise des risques mises ou à mettre en place.
Le principe de la méthode LOPA consiste, après le préalable indispensable d'une classique analyse qualitative des risques (HAZOP, arbres...), à quantifier les fréquences d'occurrence des événements initiateurs et les probabilités de défaillances associées à chaque couche de protection pour évaluer le risque de façon probabiliste discrète. La méthode LOPA est structurée en six étapes [Laurent, 2011]:

- L'étape 1 "Identification des conséquences des scénarios" a pour objet de recenser les scénarios dont l'impact est significatif en terme de gravité et des conséquences. Cette étape permet de fait de limiter le nombre de scénarios à étudier et donc de réduire la durée de l'étude LOPA;

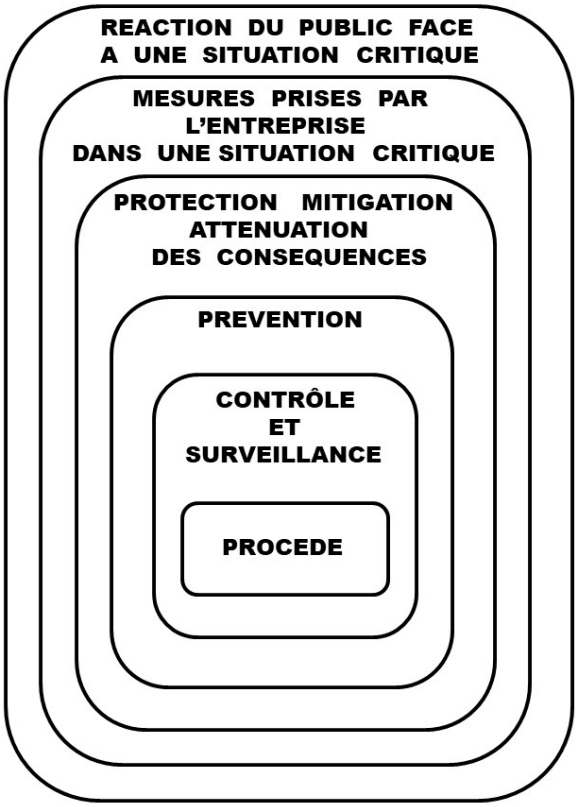

Figure 5.1: Exemple simplifié d'un modèle de couches de protection (IPL) - d'après Laurent [2011].

- L'étape 2 "Sélection et développement des scénarios" consiste, à partir de l'inventaire réalisé précédemment et à l'aide des outils classiques d'analyse qualitative des risques (HAZOP, arbres...), à préciser clairement les étapes des scénarios et à représenter chaque scénario par le schéma du noeud papillon;

- L'étape 3 "Identification de l'ensemble des événements initiateurs et évaluation de leurs fréquences" propose, sur la base de l'analyse détaillée des scénarios retenus, d'identifier l'ensemble des Evénements Initiateurs (EI) dont la réalisation est susceptible de conduire à l'Evénement Redouté Central. L'évaluation de la fréquence des EI est estimée à l'aide des valeurs d'occurrence déduites du retour d'expérience, des données issues de la littérature ou des dires d'experts;

- L'étape 4 "Identification des fonctions et barrières de sécurité et évaluation de leurs probabilités de défaillances" permet pour chaque scénario d'identifier toutes les mesures permettant de prévenir le cheminement du scénario menant à l'ERC en considérant les critères de qualification des dispositifs retenus en particulier celui de couche de protection

indépendante (IPL Independent Protection Layer). Une valeur de la probabilité de défaillance est ensuite associée à chaque barrière de sécurité en remarquant que cette étape de la méthode LOPA fait explicitement référence aux niveaux d'intégrité SIL (Safety Integrity Level) de la norme IEC 61511-3. Stack [2009] a souligné la difficulté d'identifier la véritable indépendance des couches de protection et indiqué une procédure d'évaluation dans le cas où les barrières ne sont pas indépendantes. Il faut aussi remarquer que cette étape permet la prise en compte de l'ensemble des barrières qu'elles soient techniques, humaines ou organisationnelles. Par exemple, Baybutt [2002] a proposé la méthode LOPA-FH pour améliorer l'estimation des probabilités de défaillances des barrières humaines;

- L'étape 5 "Estimation de la probabilité d'occurrence de l'Evénement Redouté Central (ERC)" constitue la synthèse des étapes précédentes. Cette étape permet de calculer la probabilité d'occurrence de l'ERC en combinant les probabilités d'occurrence des EI et les probabilités de défaillances des couches de protection et d'atténuation concernées à l'aide de la relation:

$$f_i^C = f_i^I \times \prod_{j=1}^{j} PFD_{ij} = f_i^I \times PFD_{i1} \times PFD_{i2} \times ... \times PFD_{ij} \tag{5.1}$$

où f_i^C est la fréquence de la conséquence C générée par l'événement initiateur i,
f_i^I est la fréquence initiale de l'événement initiateur i,
PFD_{ij} est la probabilité de défaillance à la sollicitation de la couche IPL j pour l'événement initiateur i.

- L'étape 6 "Evaluation du risque par rapport à des critères de maîtrise des risques" implique de s'assurer que le risque est bien maîtrisé par rapport à des critères préalablement définis.

En raison de sa mise en oeuvre plus simple par rapport aux autres méthodes d'analyse des risques, la méthode LOPA est largement utilisée dans l'industrie. Malgré son évolution progressive vers une version quantitative [Chambers, 2020]-[Iddir, 2023], la méthode LOPA présente toutefois des limites. La restriction la plus courante est relative à la prise en compte d'un scénario résultant strictement d'un simple couple cause-conséquence. La présence de différentes sources d'incertitude est également un facteur limitatif pour une meilleure qualification nécessaire des résultats. La combinaison de la méthode LOPA et d'une approche dynamique du procédé devrait permettre à la fois de surmonter la limite des incertitudes sur les mesures de prévention de sécurité et celle de la nature statique du risque.

5.2 Approche bayésienne dynamique de la méthode LOPA

5.2.1 Apport d'un réseau bayésien à la méthode LOPA

L'objectif de l'application d'un réseau bayésien à la méthode LOPA a pour objet d'améliorer la méthode LOPA par une estimation bayésienne, afin d'obtenir des résultats plus fiables ou

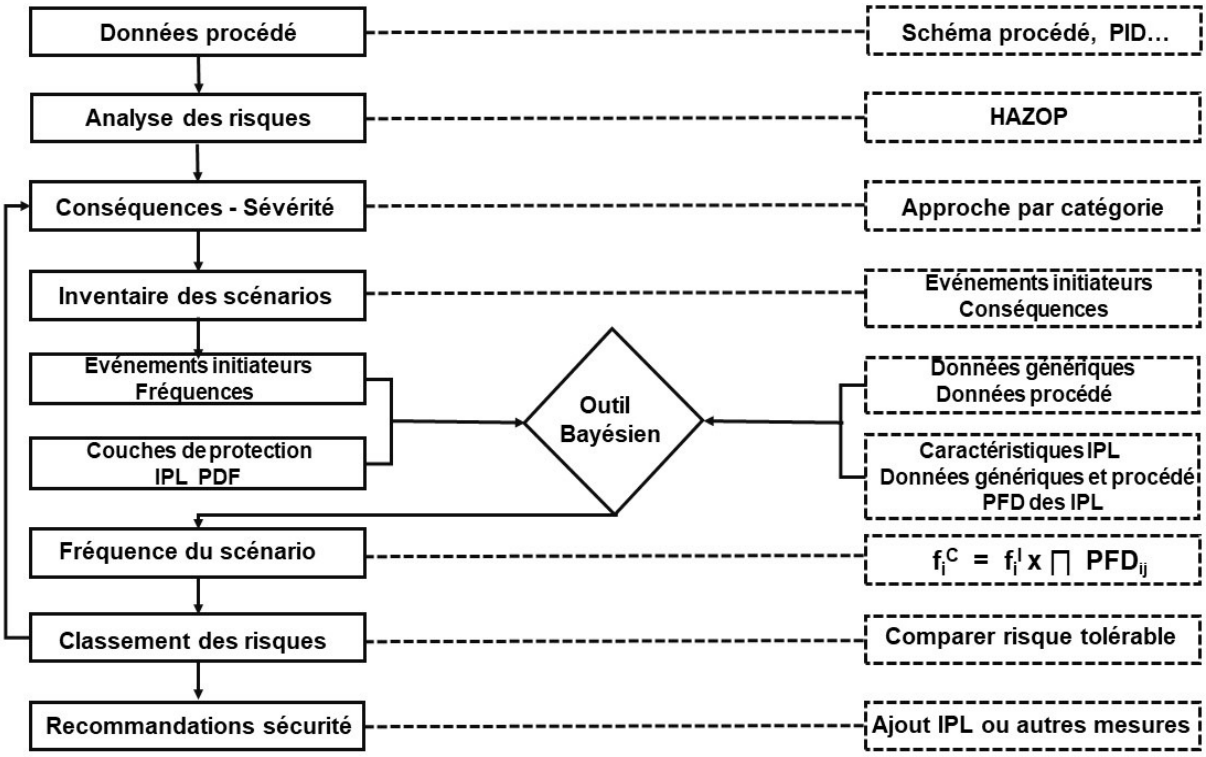

Figure 5.2: Modèle d'application d'un réseau bayésien à l'amélioration de la méthode LOPA - adapté d'après Yun et al. [2009].

plus concrets lors de l'évaluation des risques d'un procédé. La figure 5.2 présente les étapes successives de la méthode proposée par Yun et al. [2009]

- La première étape "Données du procédé" implique de collecter diverses informations actualisées du procédé comme les plans de circulation des fluides avec bilans de matière et d'énergie, les schémas PID et toutes les données;

- La seconde étape "Analyse des risques" propose de mettre en œuvre la méthode HAZOP;

- La troisième étape "Conséquences - Sévérité" consiste à estimer par une approche dite des catégories la sévérité ou gravité des conséquences listées par la méthode HAZOP. La méthode des catégories permet de traiter en fonction de la gravité les conséquences susceptibles d'entraîner des décès et ou des dommages matériels importants;

- La quatrième étape "Inventaire des scénarios" est obtenue en combinant chaque paire cause - conséquence établie dans la méthode HAZOP après estimation de la gravité de chaque conséquence;

- La cinquième étape "Evénements initiateurs - Fréquences" s'attache, à partir des causes, à identifier les événements initiateurs de chaque scénario. La fréquence de défaillance

de chaque événement initiateur est calculée par la méthode LOPA à partir des différentes catégories de données:

  - données historiques provenant des domaines industriels similaires ou proches de celui du procédé analysé;
  - données spécifiques connues de procédés identiques;
  - estimation bayésienne d'actualisation préalable des données de défaillances génériques et spécifiques via le moteur bayésien.

- La sixième étape "Couches de protection IPL PDF" nécessite d'identifier les couches de protection indépendantes (IPL). La liste des mesures de protection établie pour chaque cas d'accident dans le rapport HAZOP permet de choisir une couche IPL. Il convient d'être très attentif lors de ce choix, car la sauvegarde par IPL doit satisfaire à trois caractéristiques d'exigence d'indépendance, d'efficacité et d'auditabilité. Ensuite l'évaluation de la probabilité de défaillance à la demande (PFD) de chaque IPL est calculée par une procédure similaire à celle utilisée via le moteur bayésien pour les événnements initiaux;

- La septième étape "Fréquence du scénario" a pour but de détermier simplement la fréquence d'un scénario d'accident à l'aide de tableurs numériques (Excel);

- La huitième étape "Classement des risques" permet de comparer les résultats des fréquences calculées lors de la démarche approche bayésienne - LOPA aux critères de risque tolérable et de risque impliquant une nécessaire action de correction. Par exemple, l'ouvrage CCPS [2001] recommande d'adopter les valeurs récapitulées dans le tableau 5.1.

Conséquence	Risque tolérable	Risque impliquant une correction
humaine	$< 10^{-5}$	$< 10^{-3}$
matérielle	$< 10^{-5}$	$< 10^{-4}$

Tableau 5.1: Valeurs recommandées exprimées par année du risque tolérable et du risque impliquant une correction complémentaire - adapté d'après CCPS [2001].

  Cette étape de comparaison permet aussi d'interclasser les divers scénarios. Comme l'indique la boucle de retour de la figure 5.2, ces étapes seront répétées pour chaque scénario d'incident;

- La dernière étape est utile pour déterminer, en fonction du classement de l'étape précédente, des priorités d'intervention en termes de sécurité et de maintenance.

Pour mémoire, le principe de fonctionnement du moteur bayésien est fondé, en considérant la distribution a priori, la fonction de vraisemblance et la distribution marginale, sur la distribution

a posteriori, qui peut s'exprimer suivant le théorème de Bayes par la relation illustrative:

$$Distribution\ a\ posteriori = \frac{Distribution\ a\ priori\ \times\ Fonction\ de\ vraisemmblance}{Distribution\ marginale} \tag{5.2}$$

Les autres formulations courantes classiques du théorème de Bayes sont:

$$P(A|E) = \frac{P(E|A)\,P(A)}{P(E)} \tag{5.3}$$

où

- le terme P(A) est la probabilité a priori de A, appelée aussi probabilité marginale de A; elle est antérieure au sens qu'elle précède toute information sur E;
- le terme P(A|E) est appelée la probabilité a posteriori de A sachant E (ou encore de A sachant E). Elle est postérieure, au sens qu'elle dépend directement de E;
- le terme P(E|A), pour un E connu, est appelée la fonction de vraisemblance de A;
- le terme P(E) est appelé la probabilité marginale ou a priori de E.

pour des variables et des distributions **discrètes**:

$$P(A_j|E) = \frac{P(E|A_j)\,P(A_j)}{\sum_{i=1}^{n} P(A_i)\,P(E|A_i)} \tag{5.4}$$

où

- le terme $P(A_j|E)$, distribution a posteriori, est la probabilité de A_j connaissant E;
- $P(A_j)$, distribution a priori, probabilité de A_j avant de connaître E;
- $P(E|A_i)$, fonction de vraisemblance, probabilité de E connaissant A_i.

Le dénominateur, probabilité totale de la vraisemblance E, est simplement un terme de normalisation. Ce qui explique la forme abrégée souvent rencontrée dans la littérature utilisant l'opérateur de relation $\propto$:

$$P(A_j|E) \propto P(E|A_j)\,P(A_j) \tag{5.5}$$

pour des variables et des distributions **continues**:

$$f(\lambda|t) = \frac{h(\lambda)\ l(t|\lambda)}{\int_{-\infty}^{+\infty} h(\lambda)\ l(t|\lambda)\ d\lambda} \tag{5.6}$$

où

- $h(\lambda)$ est la fonction continue de densité de probabilité de défaillance (PDF) a priori;

- $l(t|\lambda)$ est la fonction de vraisemblance basée sur les données de l'échantillon t;
- $f(\lambda|t)$ est la fonction continue de densité de probabilité de défaillance a posteriori.

Selon National Laboratory [2003], l'estimation bayésienne peut intégrer le degré de vraisemblance des données génériques et les informations des données échantillonnées spécifiques à l'usine. La vraisemblance préalable, appelée distribution préalable, décrit l'état des connaissances sur le paramètre avant d'obtenir l'échantillon de données. L'estimation peut alors s'articuler autour de deux possibilités. La première consiste à tirer parti des données disponibles pour attribuer une distribution préalable subjective à partir de données historiques. La seconde consiste à utiliser des données supplémentaires ou spécifiques provenant d'usines ou d'industries particulières pour mettre à jour une distribution préalable existante. Les détails des inférences du moteur bayésien de la figure 5.2 pour estimer respectivement les fréquences des défaillances des événements initiateurs et les PDF des couches de protection IPL sont explicités dans les références [Yun, 2007] et [Yun et al., 2009]. Pour faciliter l'estimation par inférence bayésienne, ces auteurs recommandent d'utiliser les relations conjuguées des distributions indiquées dans le tableau 5.2.

Elément	Distribution a priori	Fonction de vraisemblance	Distribution a posteriori
Fréquence élément initiateur	Gamma	Poisson	Gamma
PFD IPL	Beta	Binomiale	Beta

Tableau 5.2: Relations conjuguées recommandées des distributions - adapté d'après Yun et al. [2009].

5.2.2 Exemple d'application du modèle au dépotage en zone portuaire d'un navire méthanier

5.2.2.1 Description sommaire de l'installation portuaire de déchargement

La figure 5.3 présente dans la partie (a) le schéma de principe du plan de circulation du GNL et des équipements d'une station portuaire de déchargement d'un navire méthanier [Yun, 2007]. Une station générique portuaire de déchargement GNL comporte les fonctionnalités principales suivantes:

- Un poste de déchargement méthanier avec un système de transfert par bras métalliques articulés;
- Des lignes de transfert de déchargement GNL;
- Un stockage GNL;
- Des équipements de contrôle de pression (vaporiseur-évent-autres);

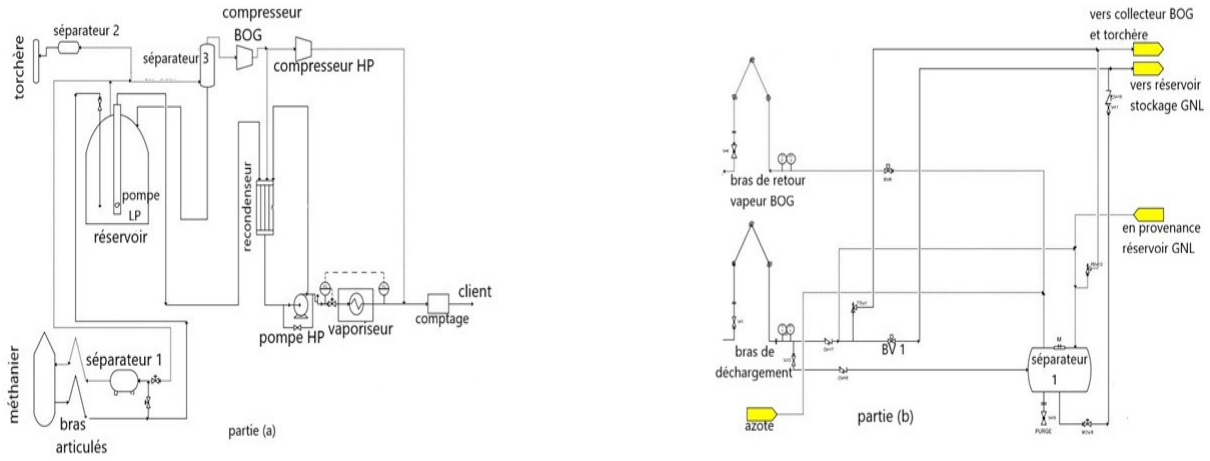

Figure 5.3: Schéma de principe d'une installation portuaire de déchargement d'un méthanier [partie (a)] et schéma PID du poste de déchargement [partie (b)] - adapté d'après Yun [2007].

- Des pompes de soutirage;
- Un poste de comptage fiscal du GNL (optionnel);
- Un poste de ravitaillement navire;
- Des lignes de transfert de ravitaillement GNL;
- Un poste de chargement camion-citerne ou wagon GNL (Optionnel);
- Des unités de contrôle et de sécurité.

5.2.2.2 Application du modèle couplant réseau bayésien et LOPA

5.2.2.2.1 Analyse HAZOP

Les phénomènes dangereux pouvant survenir par perte de confinement dans une installation portuaire de déchargement GNL sont les suivants [AFG, 2019]:

- Feu de nuage, feu flash avec explosion de nuage (UVCE) en zone encombrée;
- Jet enflammé, feu torche;
- Feu de nappe;
- BLEVE de capacité;
- Explosion physique par transition rapide de phase;
- Roll-over préalable dans un réservoir.

La mise en œuvre de la méthode HAZOP a été limitée aux trois nœuds suivants de l'installation:

- déchargement du GNL liquide du navire méthanier vers le réservoir de stockage;
- refoulement du GNL par la pompe LP vers le recondenseur et l'aspiration de la pompe HP;
- système du réservoir de stockage GNL.

Les résultats de la session de travail ont permis de consigner 20 causes d'accident potentiel. Les experts ont alors considéré de ne retenir pour l'étude LOPA que 7 scénarios cause-conséquence, en raison de la gravité des conséquences et de l'importance des équipements examinés, répertoriés dans le tableau 5.3.

Nœud	Scénario	Descriptif du scénario
1	1	fuite GNL des bras de transfert pendant le déchargement
1	2	augmentation de la pression dans les bras de transfert en raison de la fermeture de la vanne BV1 pendant le déchargement
2	3	cavitation et dommages de la pompe HP dus à la baisse de pression dans le recondenseur résultant de la fermeture anormale de la vanne BV 32
2	4	température excessive dans le recondenseur en raison de l'augmentation du débit Boil Off Gas (BOG) résultant de l'ouverture totale anormale de la vanne de contrôle de débit FCV 32
3	5	surpression dans le réservoir de stockage due au phénomène de rollover entrainant des stratifications en en couches dommageables pour les parois du réservoir
3	6	augmentation du niveau entrainant du GNL dans l'espace annulaire, suite au mauvais positionnement d'une ligne réservoir (erreur opérateur)
3	7	dépression dans le réservoir due à un pompage en l'absence de BOG résultant de la défaillance de la vanne BV 45 avec possible endommagement du réservoir

Tableau 5.3: Inventaire des scénarios sélectionnés pour application de la méthode LOPA - adapté d'après Yun et al. [2009].

5.2.2.2.2 Exemple du scénario 2

Le scénario 2 "augmentation de la pression dans les bras de transfert en raison de la fermeture de la vanne BV1 pendant le déchargement GNL" est utilisé à titre d'exemple pour montrer

l'utilisation de la méthode réseau bayésien-méthode LOPA. La partie (b) du schéma PID de la figure 5.3 montre qu'une vanne de sectionnement, BV-1, est installée pour arrêter le débit de GNL dans la conduite de déchargement en cas d'urgence. Cependant, si la vanne est fermée accidentellement pendant la procédure de déchargement, la pression à l'intérieur des bras de déchargement et de la canalisation augmentera jusqu'à la pression d'arrêt des pompes du navire méthanier. Cela peut avoir des conséquences indésirables dans les bras et la canalisation.
La fréquence du déclenchement intempestif de la fermeture d'une vanne de sectionnement en tant qu' événement déclencheur peut être estimée à l'aide des données de l'OREDA et de la base de données sur les défaillances des installations de GNL. OREDA fournit la fréquence de défaillance d'un déclenchement intempestif d'une vanne d'arrêt. Elle est utilisée comme informations préalables des données génériques dans l'estimation bayésienne. La base de données sur les défaillances des installations de GNL fournit les heures de fonctionnement, le nombre de défaillances et la durée moyenne entre pannes MTBF (Mean Time Between Failures) des vannes cryogéniques, qui peuvent être utilisées comme informations de vraisemblance des données spécifiques au sytème de transfert.
Pour ce scénario 2, une seule couche de protection IPL est considérée. Il s'agit de la soupape de sécurité thermique (TSV). La probabilité de défaillance à la demande PFD d'une TSV peut être estimée à l'aide des données de l'EIReDA et de la base de données des défaillances des installations de GNL. EIReDA fournit la valeur moyenne de la PFD et les valeurs des paramètres α et β dans la fonction de distribution beta pour une soupape de sécurité (PRV). Comme la TSV a presque la même configuration de conception que la PRV, les données de défaillance de la PRV seront donc utilisées, comme informations préalables a priori. La base de données des défaillances des installations de GNL fournit les heures de fonctionnement, le nombre de défaillances et le MTBF des vannes cryogéniques. Mais la base de données ne fournit pas de données spécifiques sur les défaillances des soupapes de sécurité. Par conséquent, les données relatives aux soupapes cryogéniques seront utilisées pour les soupapes de sécurité thermique sous pression dans la méthode de calcul.
Il est alors possible d'estimer la fréquence du scénario 2 comme indiqué dans la septième étape correspondante de la figure 5.2. Le détail des calculs de la méthode appliquée est consultable dans l'annexe C de la référence [Yun, 2007].
Le tableau 5.4 permet de comparer les valeurs numériques estimées des fréquences des fonctions a priori, de vraisemblance et a posteriori de l'événement initiateur, de la couche de protection IPL et du scénario 2.

Elément	a priori	vraisemblance	a posteriori
Evénénement initiateur	$5,53 \times 10^{-3}$	$5,50 \times 10^{-3}$	$5,51 \times 10^{-3}$
PDF - IPL TSV	$4,70 \times 10^{-4}$	$5,50 \times 10^{-3}$	$5,3 \times 10^{-4}$
Scénario 2	$2,60 \times 10^{-6}$	$3,03 \times 10^{-5}$	$2,90 \times 10^{-6}$

Tableau 5.4: Récapitulatif des fréquences des différentes fonctions estimées dans le scénario 2 - adapté d'après Yun et al. [2009].

Le tableau 5.5 regroupe les valeurs respectives des fréquences des sept scénarios étudiés lors de

l'application du modèle réseau bayésien-méthode LOPA.

Scénario	a priori	vraisemblance	a posteriori
1	$2,45 \times 10^{-8}$	$1,35 \times 10^{-7}$	$9,87 \times 10^{-7}$
2	$2,60 \times 10^{-6}$	$3,03 \times 10^{-5}$	$2,90 \times 10^{-6}$
3	$1,08 \times 10^{-5}$	$6,01 \times 10^{-5}$	$1,37 \times 10^{-5}$
4	$1,48 \times 10^{-7}$	$1,43 \times^{-9}$	$1,88 \times 10^{-9}$
5	$5,13 \times 10^{-11}$	$8,50 \times^{-10}$	$6,12 \times 10^{-10}$
6	non défini	$3,16 \times 10^{-7}$	$2,80 \times 10^{-7}$
7	$1,48 \times 10^{-14}$	$4,54 \times 10^{-11}$	$5,50 \times 10^{-14}$

Tableau 5.5: Récapitulatif des fréquences des sept scénarios examinés - adapté d'après Yun [2007].

L'analyse des résultats du tableau 5.5 montre que la fréquence finale estimée des sept scénarios est toujours inférieure à la valeur de 10^{-4} du risque tolérable pour l'installation. Il est aussi possible de hiérarchiser la contribution potentielle de chaque scénario en constatant par exemple que les scénarios 3 et 2 présentent les fréquences les plus importantes. Enfin le retour d'expérience de l'évaluation des risques des terminaux portuaires méthaniers montre que les ordres de grandeurs des fréquences annuelles d'accidents sont en accord avec les valeurs de l'exemple traité [DNV, 2005].

5.3 Approche hybride probabiliste et de logique floue à la méthode LOPA

Cette section développe une approche hybride de logique floue et de probabilité pour agréger efficacement une base de données génériques et des données spécifiques au procédé à l'aide d'un jugement d'experts, en tenant compte à la fois des incertitudes des données et des connaissances des experts. Cette approche hybride ne détermine pas seulement la valeur moyenne du taux de défaillance, mais quantifie également l'incertitude.

5.3.1 Méthodologie de l'approche hybride

Hong et al. [2016] ont proposé la structure de l'approche hybride de logique floue et de probabilité illustrée sur la figure 5.4.
Tout d'abord, une première fonction de distribution est générée à partir d'une part de la base de données génériques et d'autre part des données spécifiques disponibles du procédé. Différents types de fonctions de distribution peuvent être utilisés pour établir cette première fonction. Hong et al. [2016] ont retenu la fonction de distribution Log-normale en raison de sa large application aux données de fiabilité et de taux de défaillance. La fonction de densité de probabilité

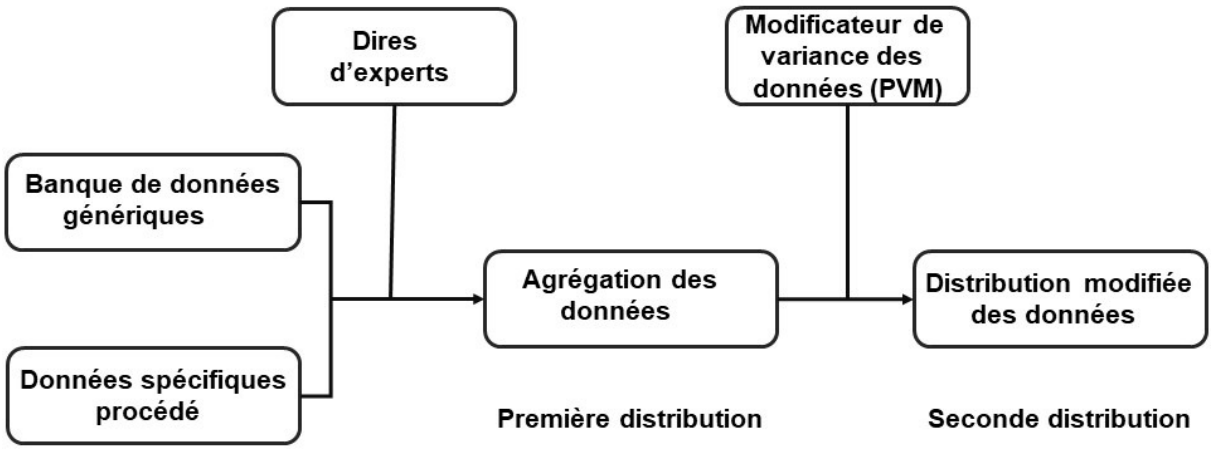

Figure 5.4: Structure de l'approche hybride de logique floue et de probabilité - adapté d'après Hong et al. [2016].

d'une distribution Log-normale est décrite par les équations:

$$f(x|m,\nu) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{(\ln x - \mu)^2}{2\sigma^2}\right] \tag{5.7}$$

$$m = \exp\left(\mu + \frac{\sigma^2}{2}\right) \tag{5.8}$$

$$\nu = \exp(2\mu + \sigma^2)(\exp(\sigma^2) - 1) \tag{5.9}$$

où
μ est la moyenne du Logarithme normal de la variable,
σ est l'écart-type du Logarithme normal de la variable,
m est la moyenne de la distribution Log-normale,
ν est la variance de la distribution Log-normale.
Les valeurs m et ν seront obtenues en ajustant une fonction de distribution à l'ensemble des données collectées. D'après Hong et al. [2016], la meilleure façon de procéder serait de demander à des experts de donner leur avis sur la fiabilité des données et de l'inclure dans l'incertitude exprimée dans l'écart-type, tout en conservant la moyenne. En présentant une série de qualificatifs fixes, les experts peuvent choisir une correction de la valeur ν. Cette approche semble plus simple pour réaliser l'élicitation d'avis d'experts, que la pondération de facteurs pour lesquels aucune référence n'est disponible. La logique floue va permettre d'atteindre cet objectif au moyen d'un modificateur de variance des paramètres (PVM) mis au point pour modifier la première distribution sur la base de quatre paramètres:

- la qualité de la base de données;
- la pertinence de la base de données;

- la quantité de données spécifiques au procédé;
- le niveau d'expérience des experts.

La structure de modélisation floue du modificateur de variance des paramètres est indiquée sur la figure 5.5.

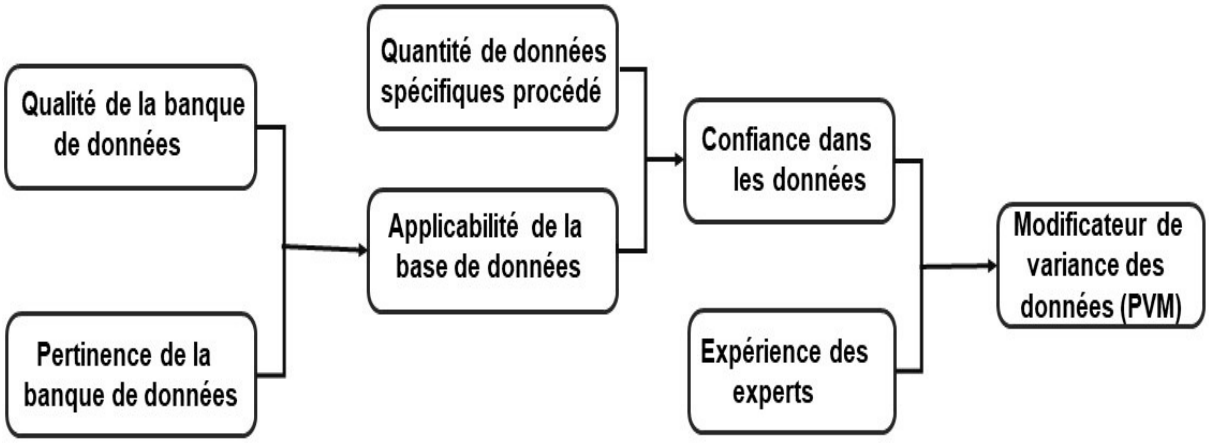

Figure 5.5: Structure de modélisation floue du modificateur de variance des paramètres - adapté d'après Hong et al. [2016].

La qualité et la pertinence de la base de données déterminent l'applicabilité du paramètre "base de données". Ce dernier et la quantité de données spécifiques du procédé établissent le bloc "confiance dans les données". Enfin le couplage confiance dans les données et niveau de compétences et d'expérience des experts génère finalement le modificateur PVM de variance des paramètres. Chacune des étapes est conduite en adoptant la structure du système de logique floue de type 1, soit fuzzification, inférence et défuzzification. La première étape de la procédure consiste à fuzzifier toutes les différentes entrées et la sortie. Le tableau 5.6 récapitule la liste des variables et leurs descriptions en termes linguistiques.

Variable linguistique	Domaine	Description en termes linguistiques
PVM	$(0, 1)$	marginal, adéquat, bon, excellent
Qualité base de données	$(0, 1)$	mauvaise, faible, moyenne, bonne
Pertinence base de données	$(0, 1)$	non pertinente, marginale, applicable, identique
Applicabilité base de données	$(0, 1)$	douteuse, possible, pratique, large
Quantité données procédé	$(0, 30)$ points	peu, limitée, juste, suffisante
Confiance données	$(0, 1)$	mauvaise, moyenne, bonne, supérieure
Expérience experts	$(0, 10)$ ans	débutant, intermédiaire, senior, expert

Tableau 5.6: Description des variables linguistiques floues - adapté d'après Hong [2017].

Les règles floues sont introduites en fonction de l'ingénierie et des connaissances des experts. L'inférence floue dite de Mamdani est utilisée pour la modélisation floue. Pour que les règles

restent simples, seuls deux entrées antécédentes sont utilisés à chaque fois. En utilisant la règle floue "SI" et "ALORS", les résultats, estimés à l'aide de l'outil Matlab Fuzzy Toolbox, sont récapitulés sous forme de tableaux fournissant respectivement l'applicabilité de la base de données, la confiance dans les données et le facteur de modification PVM dans les références [Hong et al., 2016] et [Hong, 2017]. La lecture en est aisée. Par exemple, pour le paramètre "Applicabilité", SI la qualité de la base de données est *mauvaise* et SI la pertinence de la base de données est *non pertinente*, ALORS l'applicabilité est *douteuse*.
La variance ν^* de la fonction de distribution modifiée est calculée en fonction du modificateur PVM de variance et de la variance de la fonction de distribution initiale par la relation:

$$\nu^* = \frac{\nu}{\sqrt{PVM}} \tag{5.10}$$

Le tableau 5.7 indique quelques exemples de résultats de la modélisation floue du modificateur PVM de variance.

Exemple	Entrées				Sortie
	Qualité (0-1)	Pertinence (0-1)	Données (0-30)	Expert (0-10)	PVM (0-1)
a	1	$0,7$	15	5	$0,99$
b	1	$0,7$	0	5	$0,65$
c	1	$0,7$	6	10	1
d	1	1	0	10	$0,97$
e	$0,8$	$0,6$	2	5	$0,80$

Tableau 5.7: Exemples de résultats de la modélisation floue du modificateur de variance - adapté d'après Hong [2017].

5.3.2 Exemple d'application à une colonne de distillation

Le schéma simplifié de la colonne de distillation avec son instrumentation est présenté sur la figure 5.6. La colonne de 2 m de diamètre et de 15 m de hauteur, qui fonctionne à une température de $120°$C et sous une pression de $0,39$ MPa, contient une masse totale de n-hexane de 40 tonnes.
Le principe de base en termes de sécurité procédé consiste à maintenir l'équilibre énergétique dans la colonne entre le rebouilleur et le condenseur. L'application de la méthode HAZOP a permis d'identifier les causes principales de perturbation du fonctionnement de la colonne suivantes:

- perte de l'alimentation en eau de refroidissement à l'entrée du condenseur;
- défaillance de la pompe de distillat;
- défaillance de la boucle de contrôle de niveau haut (LIC) dans la recette de distillat;
- vanne manuelle de distillat maintenue fermée après l'arrêt de l'installation;

- défaillance du régulateur de débit vapeur (FIC) au rebouilleur en cas d'excès de débit vapeur.

L'exemple étudié est constitué par le couple cause-conséquence: perte de l'alimentation en eau à l'entrée du condenseur - relâchement de 5000 kg d'un nuage inflammable dans l'unité suite à l'ouverture de la soupape de sécurité. La fréquence de la perte de l'eau de refroidissement considérée comme l'événement initiateur est de l'ordre de 10^{-1} d'après les tables de données. La figure 5.6 montre la présence de deux alarmes hautes de température et de pression sur la colonne. Ces alarmes affichées sur le système de contrôle distribué alertent l'opérateur (OP) pour qu'il ferme la vanne. Cet ensemble opérateur - alarmes constitue la première couche de protection (IPL). La PDF d'un opérateur, qui ne réagit pas à une alarme de type haut dans la moitié du délai maximum de 10 minutes, est de un échec sur 10 demandes, soit 10^{-1}.

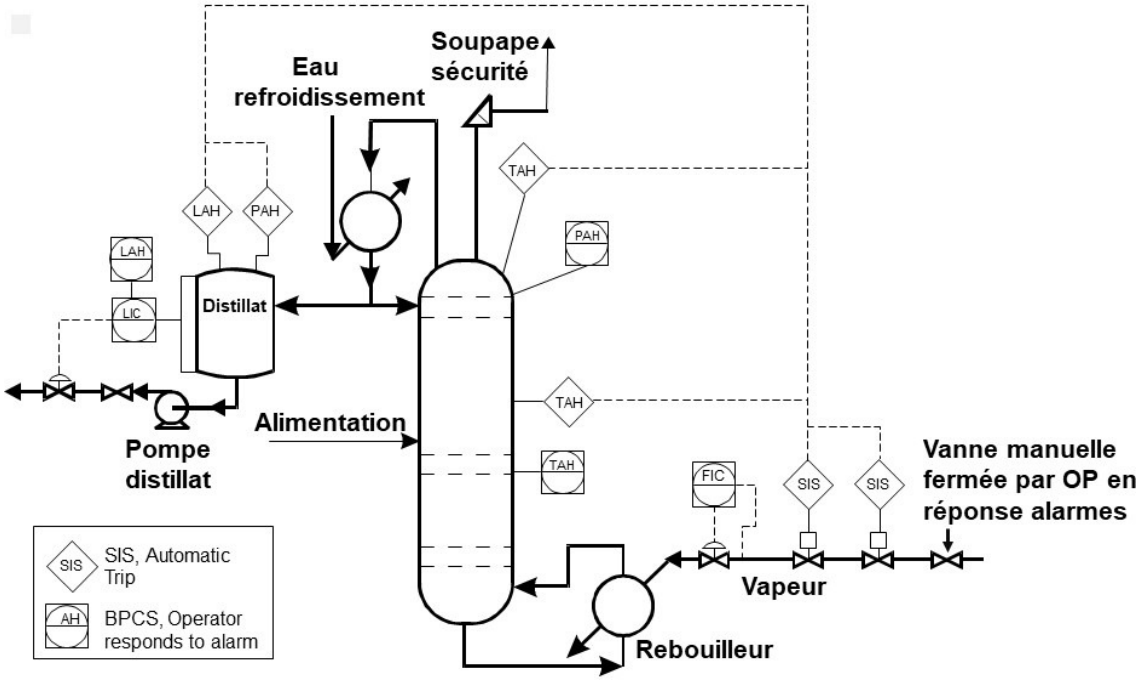

Figure 5.6: Schéma de principe de la colonne de distillation avec instrumentation - adapté d'après Hong et al. [2016].

La seconde couche de protection est réalisée avec un Système Instrumenté de Sécurité de niveau SIL donné (Instrumented Integrity Level). Ici cette seconde IPL est constitutée par une vanne SIL 2 qui doit stopper l'arrivée de chauffage du rebouilleur. D'après la norme internationale IEC 61508, la PFD SIL 2 est comprise entre 10^{-3} et 10^{-2}. Par mesure conservatoire, la méthode LOPA adopte la valeur 10^{-2}. La fréquence finale de la conséquence du scénario, qui est obtenue en multipliant la fréquence de l'événement initiateur par les fréquences successives des PFD des IPL, est donc de 10^{-4} en méthode LOPA traditionnelle.
Les résultats finaux de l'approche hybride et de l'approche LOPA traditionnelle sont regroupés dans le tableau 5.8 sous la forme des distributions "Log-normale" des fréquences et des taux de défaillance exprimées sous la forme $f(m, \sqrt{\nu})$.

Evénement initiateur ou IPL	PDF	PDF $(PVM = 1)$	PDF $(PVM = 0,80)$	PDF $(PVM = 0,65)$	LOPA classique
EI	$f(10^{-1}, 10^{-1})$	$f(10^{-1}, 10^{-1})$	$f(10^{-1}, 1,24 \times 10^{-1})$	$f(10^{-1}, 1,54 \times 10^{-1})$	10^{-1}
OP	$f(10^{-1}, 10^{-1})$	$f(10^{-1}, 10^{-1})$	$f(10^{-1}, 1,24 \times 10^{-1})$	$f(10^{-1}, 1,54 \times 10^{-1})$	10^{-1}
SIS	$f(5 \times 10^{-3}, 2 \times 10^{-3})$	$f(5 \times 10^{-3}, 2 \times 10^{-3})$	$f(5 \times 10^{-3}, 2,5 \times 10^{-3})$	$f(5 \times 10^{-3}, 3,1 \times 10^{-3})$	10^{-2}
Mean	5×10^{-5}	5×10^{-5}	5×10^{-5}	5×10^{-5}	10^{-4}
95 percentile	$1,78 \times 10^{-4}$	$1,78 \times 10^{-4}$	$1,86 \times 10^{-4}$	$1,99 \times 10^{-4}$	

Tableau 5.8: Exemples de résultats de la modélisation floue du modificateur de variance - adapté d'après Hong [2017].

Hong et al. [2016], qui ont aussi présenté les résultats sous forme d'histogrammes, ont montré qu'une faible valeur du modificateur PVM de variance augmentait de façon importante l'écart-type des distributions. En termes d'analyse et de maîtrise des risques, il est aussi possible d'examiner la différence entre la valeur moyenne et la valeur du 95e percentile. Si l'écart est supérieur à un ordre de grandeur, une IPL supplémentaire peut être appliquée pour réduire la fréquence de défaillance du scénario considéré. Mais ce n'est pas le cas sur cet exemple.
Cet exemple a révélé que l'approche hybride permet d'obtenir une valeur plus précise du taux de défaillance avec les données disponibles et le jugement d'experts. La comparaison montre aussi que la convolution des distributions fournit une valeur de fréquence plus faible du scénario que la méthode LOPA traditionnelle.

5.3.3 Apport d'une cascade de logique floue à la méthode LOPA

Cette section présente un modèle Fuzzy-LOPA en cascade pour l'évaluation SIL, qui utilise les données obtenues à partir de l'analyse préliminaire des risques ainsi que celles des bases de données. Ce modèle hybride utilise deux blocs:

- le premier est un modèle flou permettant d'obtenir la gravité;
- le second utilise les résultats obtenus au moyen d'une deuxième boucle floue pour évaluer le SIL de tout dispositif de protection supplémentaire.

Une comparaison est effectuée sur un exemple entre les résultats obtenus par l'approche LOPA traditionnelle et le modèle flou en cascade proposé.

5.3.3.1 Modèle d'évaluation des risques par une cascade de logique floue couplée à la méthode LOPA

Khalil et al. [2012] recommandent d'utiliser le modèle de Mamdadi. Pour mémoire, les étapes de ce modèle sont:

- définir une valeur de référence pour les paramètres de l'étude;
- fuzzifier la valeur de référence;
- préparer les régles "si"-"alors" (if then);

- mettre en œuvre ces règles pour obtenir la sortie sous forme floue;
- défuzzifier pour obtenir la valeur nette de sortie.

Chaque modèle proposé comporte deux entrées et une seule sortie.

5.3.3.1.1 Modèle flou de gravité

La gravité du procédé est évalué simultanément en termes de sécurité du procédé et du point de vue économique pour l'entreprise. Les niveaux de gravité respectifs sont répertoriés dans le tableau 5.9.

Nombre de décès	Gravité procédé	Pertes économiques (USD)	Gravité économique
< 1	négligeable	< 1 Million	négligeable
1 to 10	faible	1-10 Millions	faible
10 to 50	modérée	10-100 Millions	modérée
50 to 200	haute	10^2-10^3 Millions	coûteuse
> 200	catastrophique	$> 10^3$ Millions	catastrophique

Tableau 5.9: Niveaux de gravité sécurité procédé et pertes économiques - d'après Khalil et al. [2012].

Les formes retenues des fonctions d'appartenance sont de distribution trapézoïdale pour la gravité procédé et de distribution normale transfomée en log_{10} pour la gravité des pertes économiques. L'ensemble des règles floues qui permettent de prendre les décisions relatives à la gravité est présenté dans le tableau 5.10.

		Effet économique				
		Faible	Modéré	Haut	Trés haut	Catastrophique
Sécurité	Catastrophique	Catastrophique	Catastrophique	Catastrophique	Catastrophique	Catastrophique
	Haut	Haut	Haut	Haut	Très haut	Catastrophique
	Modéré	Moyen	Moyen	Haut	Très haut	Catastrophique
	Faible	Faible	Moyen	Haut	Très haut	Catastrophique

Tableau 5.10: Tableau de décisions de la cotation globale de la gravité - adapté d'après Khalil et al. [2012].

5.3.3.1.2 Modèle flou en cascade de la classification SIL

Le niveau d'intégrité de sécurité (SIL) est basé sur la fréquence et la gravité d'un certain scénario. Selon la norme IEC 61508 avec 4 SIL standard, Khalil et al. [2012] ont retenu le niveau d'intégrité de sécurité en quatre niveaux, mais en ajoutant un niveau ultra et un niveau infra. L'acronyme NSSR "No Specific SIL Required" peut être considéré comme un niveau inférieur, tandis que le niveau ultra NR "Not Recommended" correspond à des situations très risquées ou lorsque rien ne permet de réduire le risque à des limites acceptables. Les probabilités de

défaillances (PFD) et les facteurs de réduction des risques (RRF) relatifs à chaque niveau SIl sont regroupés dans le tableau 5.11.

SIL	PFD	RRF
NSSR	10^{-1}-1	1-10
1	10^{-2}-10^{-1}	10-10^{2}
2	10^{-3}-10^{-2}	10^{2}-10^{3}
3	10^{-4}-10^{-3}	10^{3}-10^{4}
4	10^{-5}-10^{-4}	10^{4}-10^{5}
NR	10^{-6}-10^{-5}	10^{5}-10^{6}

Tableau 5.11: Probabilités de défaillance et facteur de réduction des risques pour chaque niveau SIL- d'après Khalil et al. [2012].

L'ensemble des règles floues qui permettent de prendre les décisions relatives à la fréquence est présenté dans le tableau 5.12.

		Fréquence							
		PP	P	VL	L	M	H	VH	S
Gravité	Catastrophique	1	2	2	3	4	NR		
	Très haute	1	1	2	3	4			
	Haute	1	1	1	2	2	4	4	4
	Moyenne	NSSR			1	2	3	3	4

Tableau 5.12: Tableau de décisions de la cotation globale du niveau SIL - Cotation: PP-peu probable; P-probable; VL-très faible; L-faible; M-moyenne; H-haute; VH-très haute; S-certaine - adapté d'après Khalil et al. [2012].

En conclusion de cette description de deux parties, la figure 5.7 montre l'architecture de la cascade des deux modèles flous et la relation entre eux. L'ensemble flou de sortie de la cascade est constitué par aggrégation des ensembles flous obtenus successivement par les différentes règles d'association. Khalil et al. [2012] ont utilisé le logiciel Matlab de logique floue pour simuler les résultats.

5.3.3.1.3 Exemple d'application

L'exemple concerne une unité de gaz combustible typique alimentant une usine de gaz. Cette usine à gaz a une capacité de 470×10^3 $m^3.h^{-1}$, le méthane résultant étant comprimé par un compresseur centrifuge à trois étages à 45 barg pour le transport. L'usine est alimentée par trois turbines à gaz tandis que le compresseur est entraîné par une turbine à gaz de 40 MW. L'usine à gaz utilise le gaz naturel comme gaz combustible, ce gaz naturel provient du processus lui-même. Lorsque l'usine est perturbée, l'approvisionnement en gaz est réalisé par une source

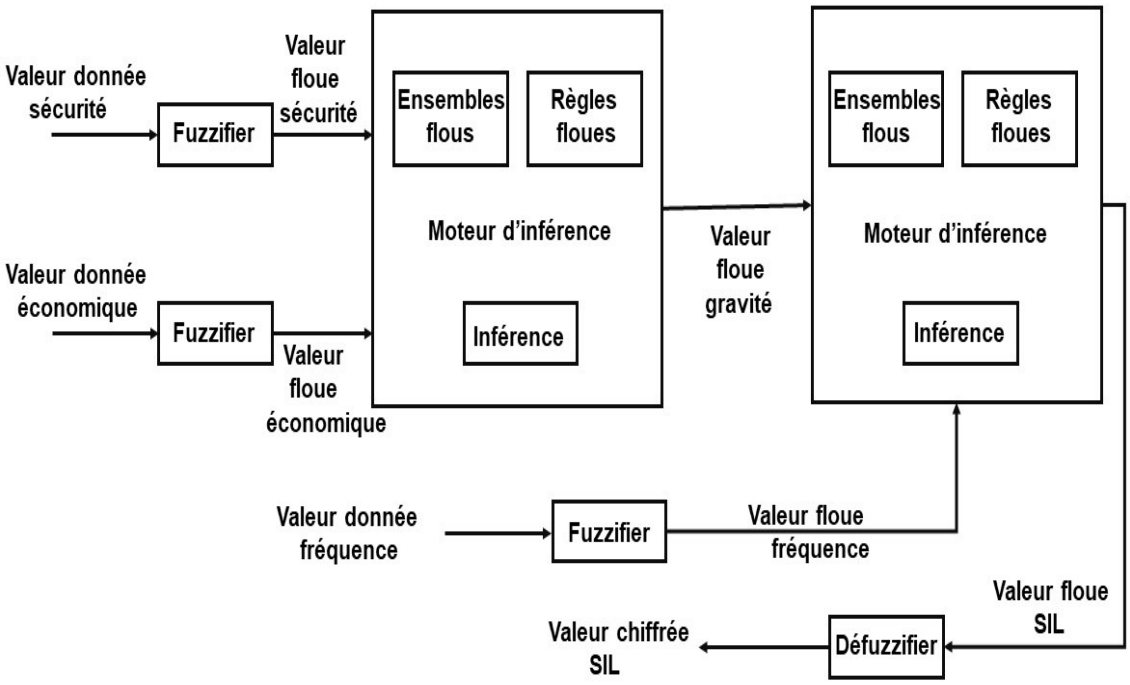

Figure 5.7: Architecture du modèle de la cascade de logique floue adapté à la méthode LOPA - adapté d'après Khalil et al. [2012].

extérieure. Cette qualité de gaz contient une grande quantité d'eau condensable et libre. Un filtre coalesceur est utilisé pour séparer toutes les particules de liquide libre accumulé. Le liquide accumulé est purgé par une vanne manuelle vers l'unité de traitement. Ce séparateur dispose d'un haut niveau de protection sous la forme d'un verrouillage instrumenté (I 32-04) qui déclenche l'arrêt de toutes les turbines à gaz en cas de niveau élevé. Mais ce verrouillage dispose aussi d'un by-pass manuel qui est activable en permanence pour éviter les déclenchements intempestifs. Le schéma de principe de l'ensemble amont séparateur-coalesceur est présenté sur la figure 5.8.
Une analyse préliminaire des risques a permis d'identifier trois scénarios relatifs à un excès de niveau de liquide dans le filtre coalesceur en amont des turbines, qui pourraient leur causer des conséquences dommageables.

- Absence d'intervention de l'opérateur pour purger le liquide (eau et huile) accumulé dans le système;
- Dysfonctionnement du transmetteur de niveau LAHH;
- Erreur de l'opérateur permettant le bypass de l'interverrouillage 32- 04 lors de l'utilisation d'une source d'approvisionnement extérieure en gaz.

L'objectif de l'application consiste à estimer les valeurs SIL du Système Instrumenté de Sécurité applicables à différents scénarios de dysfonctionnement du séparateur-coalesceur. Le tableau

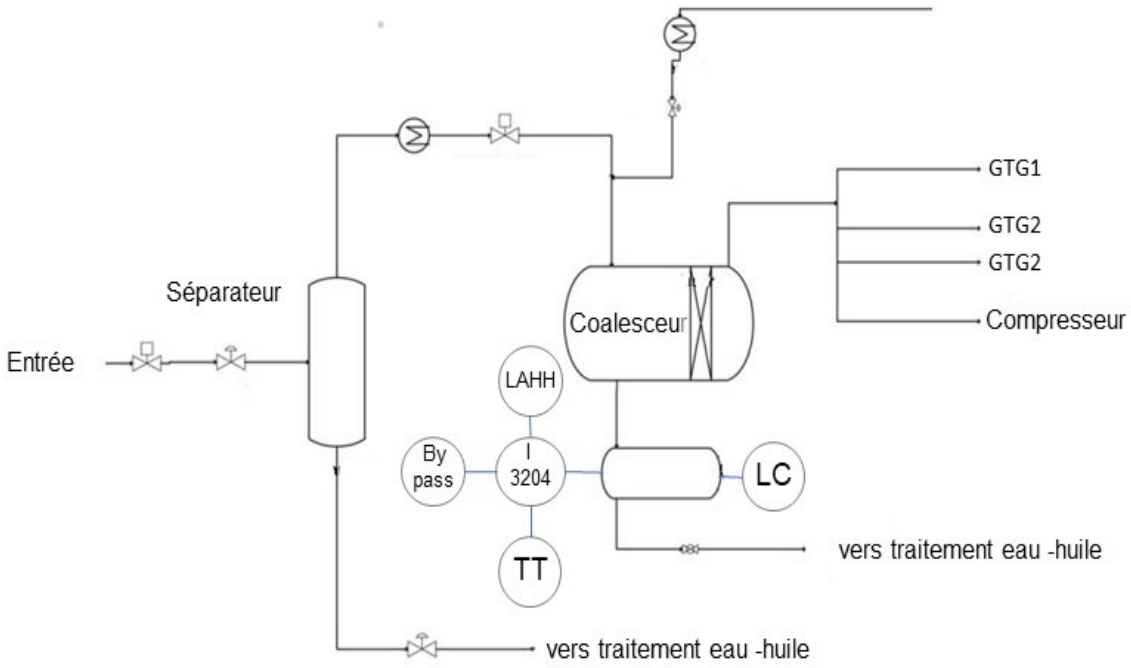

Figure 5.8: Schéma de principe de l'ensemble amont séparateur-coalesceur - adapté d'après Khalil et al. [2012].

5.13 compare les niveaux SIL requis respectivement par la méthode LOPA traditionnelle, par le modèle conventionnel de logique floue et par le modèle flou en cascade. Pour mémoire, la méthode LOPA traditionnelle a été employée pour définir le niveau SIL à partir de la probabilité moyenne de défaillance par année [Jin et al., 2016]. Il est possible de remarquer que le modèle conventionnel de logique floue et le modèle floue en cascade conduisent à la même exigence SIL, soit la valeur SIL 2, pour les scénarios "Absence d'intervention de l'opérateur" et "Bypass de l'interlock I 3204". Par contre le modèle floue en cascade est moins exigeant pour la valeur SIL dans le scénario "Dysfonctionnement du transmetteur de niveau". Enfin le modèle en cascade proposé a donné des résultats comparables à ceux obtenus avec la méthode traditionnelle LOPA.

Pour aller plus loin

- L'application de la méthode bayésienne - couche de protection LOPA pour l'évaluation des risques des systèmes de compression de gaz sous-marins.
Documentation: Ifelebuegu et al. [2017].
- Application d'un réseau bayésien au calcul de l'intégrité sécurité d'un séparateur pétrole-gaz.
Documentation: Unnikrishan [2021].
- Les réseaux bayésiens rendent la méthode LOPA plus efficace, l'analyse quantitative des risques plus transparente et plus flexible et la sécurité des procédés plus facile à évaluer.
- Documentation: Pasman and Rogers [2013].

Scénario	LOPA		Modèle flou			Cascade floue		
	Gravité	SIL	Gravité	RRF	SIL	Gravité	RRF	SIL
Absence opérateur	Haute	10^{-2} SIL 1/2	$0,596$ Haute Très haute	676	SIL 2	$0,435$ Haute	162	SIL 2
Défaillance transmetteur niveau	Haute	3×10^{-3} SIL 2	$0,596$ Haute Très haute	2398	SIL 3	$0,435$ Haute	524	SIL 2
Bypass Interlock	Haute	10^{-2} SIL 1/2	$0,596$ Haute Très haute	676	SIL 2	$0,435$ Haute	162	SIL 2

Tableau 5.13: Comparaison des résultats entre la méthode LOPA traditionnelle, la méthode fuzzy-LOPA conventionnelle et le modèle de cascade floue LOPA - adapté d'après Khalil et al. [2012].

- Implication des Systèmes Instrumentés de Sécurité (SIS) dans l'analyse dynamique des risques et la gestion des barrières: Exemple d'application au surremplissage d'un réservoir de stockage atmosphérique de substances inflammables.
- Documentation: Lee et al. [2021].

Bibliographie

A. Adriaensen, W. Decre, and L. Pintelan. Can complexity thinking methods contribute to improving Occupational Safety in Industry 4.0 ? a review of safety analysis methods and their concepts. *Safety*, 5:1–33, 2019.

AFG. Guide de maitrise des risques technologiques de stations satellites GNL soumises à autorisation. Technical Report RT1-F-Rev3, Technip FMC, Neuilly-sur-Seine (France), Mars 2019.

M. T. Amin, F. Khan, and P. Amyotte. A bibliometric review of process safety and risk analysis. *Process Safety and Environmental Protection*, 126:366–381, 2019.

K. Aslansefat, S. Kabir, Y. Gheraibia, and Y. Papadopoulos. *Dynamic fault tree: State of the art in modelling, analysis and tools*, volume 1, chapter 4, pages 73–112. CRC Press, H. Garg and M Ram edition, 2020.

Y. Bai, S. Xiang, Z. Zhao, B. Yang, and J. Zhao. *Data-driven approaches: Use of digitized operational data in process safety*, volume 6, chapter 3, pages 61–99. Academic Press Elsevier, F. Khan and H. Pasman and M. Yang edition, 2022.

P. Baybutt. Layers of protection analysis for human factors (LOPA-FH). *Process Safety Progress*, 21(2):119–124, 2002.

P. Baybutt. A critique of the Hazard and Operability (HAZOP) study. *Journal of Loss Prevention in the Process Industries*, 33:52–58, 2015.

F. Berdouzi, C. Villemur, N. Olivier Maget, and N. Gabas. Dynamic simulation for risk analysis: Application to an exothermic reaction. *Process Safety and Environmental Protection*, 113: 149–163, 2018.

A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla. Improving the analysis of dependable systems by mapping FTs into Bayesian networks. *Journal of Reliability Engineering and System Safety*, 71:249–260, 2001.

CCPS. *Layers of protection analysis (LOPA): simplified process risk assessment*. CCPS - AIChE, New-York (USA), 2001.

M. Cepin. Optimization of safety equipment outages improves safety. *Reliability Engineering and System Safety*, 77:71–80, 2002.

M. Cepin and B. Mavko. A dynamic fault tree. *Reliability Engineering and System Safety*, 75: 83–91, 2002.

C. Chambers. Comparison of a single initiating event versus a multiple initiating event approach to Layer Of Protection Analysis. In *HAZARD 30 - Symposium Series 167*, pages 2–8, Rugby, UK, 2020. IChem.

F. Chen, C. Wang, J. Wang, Y. Zhi, and Z. Wang. Risk assessment of chemical process considering dynamic probability of near misses based on Bayesian theory and event tree analysis. *Journal of Loss Prevention in the Process Industries*, 68:104280, 2020.

CSB. Mixing and heating a flammable liquid in an open top tank. Technical Report 2006-08-I-IL, US Chemical Safety Board, Washington (USA), April 2007.

B. Debray. Méthodes d'analyse des risques générés par une installation industrielle. Technical Report Omega 7, INERIS DRA 35, Verneuil-en-Halatte, France, Octobre 2006.

DNV. Analyse des risques technologiques d'un terminal méthanier - Projet RABASKA - Annexe F1. Technical Report 2005-0430, Det Norske Veritas DNV, Hovik (Norvège), Novembre 2005.

R. Ferdous. Methodology for computer aided fuzzy fault tree system. Master's thesis, Faculty of Engineering and Applied Science, Memorial University of Newfoundland, Canada, July 2006.

R. Ferdous, F. Khan, R. Sadiq, P. Amyotte, and B. Veitch. Handling data uncertainties in event tree analysis. *Process Safety and Environmental Protection*, 87:283–292, 2009.

S. Givehchi and A. Heidari. Bayes networks and fault tree analysis application in reliability estimation (Case study: automatic water sprinkler system). *Environmental Energy and Economic Research*, 2(4):325–341, 2018.

Y. Hong. *Application of fuzzy logic to quantify the uncertainty in layer of protection analysis*. PhD thesis, Mary Kay O' Connor Process Safety Center, Texas AM University (USA), May 2017.

Y. Hong, H. J. Pasman, S. Sachdeva, A. S. Markowski, and M. S. Mannan. A fuzzy logic and probabilistic hybrid approach to quantify the uncertainty in layer of protection analysis. *Journal of Loss Prevention in the Process Industries*, 43:10–17, 2016.

O. Iddir. Le nœud papillon: une méthode de quantification du risque majeur. *Techniques de l'Ingénieur - Environnement*, SE 4055:1–23, Avril 2008.

O. Iddir. Evolutions of the LOPA method to a full quantified method. *Process Safety Progress*, 42(2):290–298, 2023.

A. Ifelebuegu, E. Awotu-Ukiri, S. Theophilus, A. Arewa, and E. Bassey. The application of Bayesian-Layer of Protection analysis method for risk assessment of critical subsea gas compression systems. *Process Safety and Environmental Protection*, 113:305–318, 2017.

H. Jin, W. Mostia, and A. Summers. High/continuous demand hazardous scenarios in LOPA. In *12th Global Congress on Process Safety*, pages 1–12, Houston, USA, 2016. AIChE SIS-TECH.

S. Kabir. An overview of fault tree analysis and its application in model based dependability analysis. *Expert Systems with Applications*, 77:114–135, 2017.

M. Kalantarnia, F. Khan, and K. Hawboldt. Dynamic risk assessment using failure assessment and Bayesian theory. *Journal of Loss Prevention in the Process Industries*, 22:600–606, 2009.

D. R. Karanki, V. N. Dang, M. T. MacMillan, and L. Podofillini. A comparison of dynamic event tree methods - case study on a chemical batch reactor. *Reliability Engineering and System Safety*, 169:542–553, 2018.

N. Khakzad, F. Khan, and P. Amyotte. Safety analysis in process facilities: comparison of fault tree and Bayesian network approaches. *Reliability Engineering and System Safety*, 96: 925–936, 2011.

N. Khakzad, F. Khan, and P. Amyotte. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environmental Protection*, 91:46–53, 2013.

M. Khalil, M. A. Abdou, M. S. Mansour, H. A. Farag, and M. E. Ossman. A cascaded fuzzy-LOPA risk assessment model applied in natural gas industry. *Journal of Loss Prevention in the Process Industries*, 25:877–882, 2012.

F. Khan, S. Rathnayaka, and S. Ahmed. Methods and models in process safety and risk management: Past, present and future. *Process Safety and Environmental Protection*, 98:116–147, 2015.

F. Khan, P. Amyotte, and S. Adedigba. Process safety concerns in process digitalization. *Education for Chemical Engineers*, 34:33–46, 2021.

M. Kujath, P. Amyotte, and F. Khan. A conceptual offshore oil and gas process accident model. *Journal of Loss Prevention in the Process Industries*, 23(2):323–330, 2010.

A. Laurent. *Sécurité des procédés chimiques: Connaissances de base et méthodes d'analyse de risques*. Tech & Doc Lavoisier, Paris, France, 2011.

S. Lee, M. A. Lundteighen, and N. Paltrinieri. Dynamic risk analysis from the perspectivve of life cycle approach in IEC 61508 and IEC 61511. *Chemical Engineering Transactions*, 86: 265–270, 2021.

F. P. Lees. *Loss Prevention in the Process Industries*. Butterworth Heinemann, Oxford, UK, 1996.

X. Li, L. Zhang, F. Khan, and G. Chen. *Dynamic operational risk assessment in process safety management*, volume 6, chapter 9, pages 309–351. Academic Press Elsevier, F. Khan and H. Pasman and M. Yang edition, 2022.

Y. A. Mahmood, A. Ahmadi, A. K. Verma, A. Srividya, and U. Kumar. Fuzzy fault tree analysis: A review of concept and application. *International Journal of System Assurance Engineering and Management*, 4(1):19–32, 2013.

A. S. Markowski, M. S. Mannan, and A. Bigoszewska. Fuzzy logic for process safety analysis. *Journal of Loss Prevention in the Process Industries*, 22:695–702, 2009.

A. Meel and W. D. Seider. Plant specific dynamic failure assessment using bayesian theory. *Chemical Engineering Science*, 61:7036–7056, 2006.

A. Meel, L. M. O'Neill, J. H. Levin, W. D. Seider, U. Oktem, and N. Keren. Operational risk assessment of chemical industries by exploiting accident database. *Journal of Loss Prevention in the Process Industries*, 20:113–127, 2007.

R. E. Melchers and W. R. Feutrill. Risk assessment of LPG automotive refuelling facilities. *Reliability Engineering and System Safety*, 74:283–290, 2001.

P. Mithun, A. George, and M. Panchal. A study on the application of dynamic risk assessment in chemical process industries. *International Journal of Research Publication and Reviews*, 4(1):2298–2307, 2023.

R. Mokhtarname, A. A. Safavi, L. Urbas, F. Salimi, M. M. Zerafat, and N. Harasi. Toward HAZOP 4.0 approach for managing the complexities of the hazard and operability of an industrial polymerization reactor. In *1st Virtual IFAC Congress Paper On Line ScienceDirect*, volume 53, pages 13593–13600, Berlin, Germany, 2020. Elsevier.

R. Mokhtarname, L. Urbas, M. M. Zerafat, A. A. Safavi, F. Salimi, and N. Harasi. Integration of mathematical modeling with HAZOP study of a polymerization plant: Capabilities and lacunae. In *7 th International Conference on Control, Instrumentation and Automation (ICCIA)*, pages 1–6, Tabriz, Iran, 2021. IEEE.

R. Mokhtarname, L. Urbas, M. M. Zerafat, A. A. Safavi, F. Salimi, and N. Harasi. Application of multivariable process monitoring technique to HAZOP studies of complex processes. *Journal of Loss Prevention in the Process Industries*, 74:104674, 2022.

R. Mokhtarname, L. Urbas, A. A. Safavi, F. Salimi, and H. Taghipoor. A typical skill 4.0 platform for process safety management. In *8 th International Conference on Control, Instrumentation and Automation (ICCIA)*, pages 1–5, Tehran, Iran, 2022a. IEEE.

S. Sandia National Laboratory. *Handbook of parameter estimation for probalistic risk assessment*. US Governement Printing Office, Washington, USA, 2003.

H. Pasman and W. Rogers. Risk assessment by means of Bayesian networks: A comparative study of compressed and liquefied hydrogen transportation and tank station risks. *International Journal of Hydrogen Energy*, 37:17415–17425, 2012.

H. Pasman and W. Rogers. Bayesian networks make LOPA more effective, QRA more transparent and flexible and thus safety more definable ! *Journal of Loss Prevention in the Process Industries*, 26:434–442, 2013.

L. Podofillini and V. N. Dang. Conventional and dynamic safety analysis: Comparison on a chemical batch reactor. *Reliability Engineering and System Safety*, 106:146–159, 2012.

Y. Qian, D. Vaddiraju, and F. Khan. Safety education 4.0 - A critical review and response to the process industry 4.0 need in chemical engineering curriculum. *Safety Science*, 161:106069, 2023.

S. Rajakarunakaran, A. M. Kumar, and V. A. Prabhu. Application of fuzzy fault tree analysis and expert elicitation for evaluation of risk in LPG refuelling station. *Journal of Loss Prevention in the Process Industries*, 33:109–123, 2015.

E. Ruijters and M. Stoelinga. Fault tree analytsis: A survey of the state of the art in modelling, analysis and tools. *Computer Science Review*, 15-16:39–62, 2015.

F. F. Salimi, F. Salimi, H. Taghipoor, R. Mokhtarname, A. A. Safavi, and L. Urbas. Active learning on the collaborative digital twin of the process plant. In *Educon*, pages 878–883, Tunis, Tunisia, 2022. IEEE Global Engineering Conference.

R. J. Stack. Evaluating non independent protection layers. *Process Safety Progress*, 28(4): 317–324, 2009.

G. Unnikrishan. *Bayesian network for loss of containment from oil and gas separator*. CRC Press - Taylor & Francis, Oxon, USA, 2021.

T. Vairo, M. F. Milazzo, P. Bragatto, and B. Fabiano. A dynamic approach to fault tree analysis based on Bayesian beliefs networks. *Chemical Engineering Transactions*, 77:829–834, 2019.

J. A. Vilchez, V. Espejo, and J. Casal. Generic event trees and probabilities for the release of different types of hazardous materials. *Journal of Loss Prevention in the Process Industries*, 24:281–287, 2011.

Y. Wang, H. West, N. Hasan, and S. Mannan. QRA study of an activated carbon filter safegard system. *Process Safety and Environmental Protection*, 83 (B2):191–196, 2005.

M. Yazdi, E. Zarei, S. Adumene, R. Abbassi, and P. Rahnamayiezekavat. *Uncertainty modeling in risk assessment of digitalized process systems*, volume 6, chapter 11, pages 389–416. Academic Press Elsevier, F. Khan and H. Pasman and M. Yang edition, 2022.

G. W. Yun. Bayesian-LOPA methodology for risk assessment of LNG importation terminal. Master's thesis, Texas A M University, College Station, TX, USA, December 2007.

G. W. Yun, W. J. Rogers, and M. S. Mannan. Risk assessment of LNG importation terminals using the Bayesian-LOPA methodology. *Journal of Loss Prevention in the Process Industries*, 22:91–96, 2009.

E. Zarei, A. Azadeh, M. M. Aliabadi, and I. Mohhammadfam. Dynamic safety risk modeling of process systems using Bayesian networks. *Process Safety Progress*, 36(4):399–407, 2017.

E. Zarei, A. Azadeh, N. Khakzad, M. M. Aliabadi, and I. Mohhammadfam. Dynamic safety assessment of natural gas stations using Bayesian network. *Journal of Hazardous Materials*, 321:830–840, 2017a.