



Université d'Oran 2
Institut de Maintenance et de Sécurité Industrielle

THÈSE

Pour l'obtention du diplôme de Doctorat « L.M.D »
En Sécurité Industrielle et Environnement

**Analyse Quantitative des Risques : Application
sur les Bacs de Stockage**

Présentée et soutenue publiquement par :

M. Guetarni Islam Hadj Mohamed

Le 06 Mai 2019

Devant le jury composé de :

HASSINI Abdelatif	Professeur	Université d'Oran 2	Président
LOUNIS Zoubida	Professeur	Université d'Oran 2	Encadreur
AISSANI Nassima	Maître de conférences A	Université d'Oran 2	Co-Encadreur
OTSMANI Zineb	Maître de conférences A	Université d'Oran 2	Examinatrice
BOUAMRANE Karim	Professeur	Université d'Oran 1	Examineur
ATMANI Baghdad	Professeur	Université d'Oran 1	Examineur

Année 2018/2019

Analyse Quantitative des Risques : Application sur les Bacs de Stockage

Résumé :

La zone de stockage de gaz de pétrole liquéfié est l'une des unités de procédés ou les scénarios les plus catastrophiques sont omniprésents. A cet effet, il est primordial d'implémenter des barrières de sécurité préventives et d'intervention avec un haut niveau de fiabilité, disponibilité, maintenabilité et de sécurité suite à des analyses quantitatives approfondies sur les risques, afin de garantir une totale maîtrise de ces zones, et réduire la gravité et la fréquence d'occurrence de ces scénarios catastrophiques. Cette thèse a tiré profit des principes de la sûreté de fonctionnement, les lois de probabilité ainsi que les différentes méthodes d'Analyse Quantitative des Risques. Après avoir établi un état de l'art sur l'application des Réseaux bayésiens comme étant un outil d'aide à la décision performant et dynamique dans l'analyse Quantitative, nous avons pu définir les équations nécessaires pour l'obtention des facteurs d'importance probabiliste par inférence bayésienne. Afin de mettre en évidence ce travail de recherche une application sur le système déluge à eau, l'une des barrières de sécurité la plus importante installée dans les zone de stockage de GPL, a été étudiée en passant par la modélisation et simulation par les différentes méthodes d'analyse et modèles probabilistes tel que : AMDE, Arbre de défaillance, Simulation de Monté Carlo, Diagramme de décision binaire, loi exponentiel, loi de Weibull et les facteurs d'importance probabilistes. A la fin de ce travail un Réseau Bayésien a été élaborer pour définir l'interaction entre la criticité des équipements et leurs impacts sur l'indisponibilité du système ainsi que l'intégration d'avis d'experts. Ce Réseaux Bayésien a été utilisé comme étant un outils d'aide à la décision dynamique et efficace pour l'optimisation des performances du système étudié.

Mots clés : Analyse Quantitative des Risques, SDF, AMDE, Add, Simulation de Monté Carlo, Réseaux Bayésien, Inférence bayésienne, Facteurs d'importance probabilistes, Système déluge à eau, Aide à la décision.

Quantitative Risk Analysis: Applied on Storage Tanks

Abstract:

The liquefied petroleum gas is one area where catastrophic release scenarios are omnipresent. For this purpose, it is essential to implement preventive and protective safety barriers a high level of reliability, availability, maintainability and safety using in-depth quantitative risk analyzes, to ensure total control of these areas, and reducing the severity and frequency of occurrence of these catastrophic scenarios. This thesis exploit the principles of dependability, the probability laws as well as the different methods of Quantitative Risk Analysis. After establishing a state of the art on the application of Bayesian Belief Networks as a powerful and dynamic decision support tools in the Quantitative analysis, an expression on how to obtain probabilistic importance factors by Bayesian inference was highlighted. In order to give importance to this researcher work: an application on the water deluge system, one of the most important safety barriers installed in LPG storage areas, has been studied through modeling and simulation by the different methods of Analysis and probabilistic models such as: FMEA, Fault Tree Analysis, Monte Carlo Simulation, Binary Decision Diagram, Exponential Law, Weibull Law and Probabilistic Importance Factors. At the end of this work, a Bayesian Belief Network was developed to define the interaction between the criticality of the equipment's and their impact on the unavailability of the system as well as the integration of expert opinions. This Bayesian Network has been used as a dynamic and efficient decision support tool for optimizing the performance of the studied system.

Key words: Quantitative Risk Analysis, dependability, FMEA, FTA, Monte Carlo Simulation, Bayesian Belief Networks, Bayesian Inference, Probabilistic importance Factors, Water Deluge System, Decision Support.

التحليل الكمي للمخاطر: تطبيق على حوامج التخزين

الملخص:

تعد منطقة تخزين غاز البترول المسال إحدى المناطق حيث توجد أكثر السيناريوهات الكارثية. لهذا الغرض، إنه لمن الضروري وضع حواجز السلامة وقائية وحمائية لديها مستوى عالٍ من الموثوقية والتوافر وقابلية الصيانة والسلامة باستخدام تحليلات المخاطر الكمية المتعمقة، لضمان السيطرة الكاملة على هذه المناطق، والحد من شدة وتواتر حدوث هذه السيناريوهات الكارثية. تمثل هذه الأطروحة استفادة نظرية حول مبادئ الاعتمادية وقوانين الاحتمال وكذلك الطرق المختلفة لتحليل المخاطر الكمية. بعد مراجعة أدبية في الأبحاث سابقة عن تطبيق شبكات النظرية الافتراضية باعتبارها أداة دعم القرار قوية وديناميكية في التحليل الكمي، تمكنا من تحديد المعادلات اللازمة للحصول على عوامل الاحتمالية ذات أهمية من خلال الاستدلال في النظرية الافتراضية. من أجل إعطاء أهمية لهذا العمل البحثي، تمت دراسة تطبيقها على شبكة مكافحة الحريق بنظام الطوفان المائي أحد أهم حواجز السلامة المثبتة في مناطق تخزين غاز البترول المسال من خلال النمذجة والمحاكاة باستخدام طرق مختلفة من نماذج التحليل الكمي للمخاطر والاحتمالية مثل: وضع الفشل وتحليل التأثيرات، شجرة تحليل الخطأ، محاكاة مونت كارلو، ثنائي مخطط القرار، القانون الأسي، قانون Weibull وعوامل الاحتمالية ذات أهمية. في نهاية هذا العمل، تم تطوير شبكة النظرية الافتراضية (شبكة بايزي) لتحديد التفاعل بين أهمية المعدات وتأثيرها على عدم توفر شبكة مكافحة الحريق بنظام الطوفان المائي وكذلك تكامل آراء الخبراء. لقد تم استخدام شبكة النظرية الافتراضية كأداة لدعم اتخاذ القرارات الديناميكية والفعالة لتحسين أداء النظام المدروس.

الكلمات المفتاحية: تحليل الكمي للمخاطر، الاعتمادية، وضع الفشل وتحليل التأثيرات، شجرة تحليل الخطأ، محاكاة مونت كارلو، شبكات النظرية الافتراضية، عوامل الاحتمالية ذات أهمية، شبكة مكافحة الحريق بنظام الطوفان المائي ودعم اتخاذ القرار.

Remerciements

Alhamdulillah, c'est par la grâce d'Allah le tout puissant et miséricordieux que ce travail est achevé.

Ce travail est l'aboutissement de plusieurs années de recherche au niveau du LISIDD (Laboratoire de l'Ingénierie de la Sécurité Industrielle et du Développement Durable) de IMSI (l'Institut de Maintenance et de Sécurité Industrielle), Université Mohamed Ben Ahmed Oran 2 au sein de l'équipe des SSI (Systèmes de Sécurité Intelligents). En collaboration avec LM2S (Laboratoire de Modélisation et Sûreté des Systèmes) de l'Institut Charles Delaunay, Université de technologie de Troyes, cette thèse a été accomplie. Je suis vraiment reconnaissant de faire partie de ces équipes.

Je tiens à exprimer mes plus vifs remerciements à mes deux directrices de thèse :

Madame LOUNIS Zoubida d'avoir endossée la responsabilité de directrice de thèse, d'être disponible et attentive malgré ses responsabilités nombreuses, de ses orientations et de ses encouragements tout au long de ce travail.

Et Madame AISSANI Nassima pour son aide inestimable, sa patience, j'admire amplement ses compétences, sa pédagogie, ses méthodes de travail et ses clairvoyances qui ont été un atout indéniable pour la réussite de ces travaux. Sachant que tomber dans les réseaux bayésiens n'arrive jamais par hasard, mais parce qu'un jour, lors de notre première réunion, ma co-encadrante de thèse m'a conseillé de regarder ces "modèles-ci", qui pourraient sûrement m'être utiles. C'est grâce à sa motivation que j'ai pu m'engager dans ce chemin curieux... Merci infiniment Mme Aissani Nassima pour ce judicieux conseil !

Plus globalement je crois sincèrement avoir profité pleinement de leurs expériences de chercheuses mais aussi d'enseignantes, j'estime avoir beaucoup appris sous leurs tutelles.

Je tiens aussi à exprimer mes remerciements à Monsieur CHATELET Eric, Professeur à l'université de Troyes France pour son accueil au laboratoire LM2S, pour l'intérêt qu'il a porté à ce travail, pour sa disponibilité et ses encouragements.

Je remercie Monsieur HASSINI Abdelatif, Professeur à l'université Mohamed Ben Ahmed Oran 2 et Madame OTSMANI Zineb, MCA à l'université Mohamed Ben Ahmed Oran 2, d'avoir accepté de prendre part du jury.

Mes remerciements s'adressent aussi à Monsieur BOUAMRANE Karim, Professeur à l'université Ahmed Ben Bella Oran 1 et à Monsieur ATMANI Baghdad, Professeur à l'université Ahmed Ben Bella Oran 1, d'avoir accepté de prendre part du jury.

Je tiens à remercier aussi mes collègues, doctorants et docteurs et surtout ceux qui m'ont toujours encouragé ainsi que les enseignants et le staff administratif de l'Institut de Maintenance et de Sécurité Industrielle.

J'apprécie profondément le soutien immense de mes chers amis merci d'être là pour moi.

Mes plus sincères remerciements sont réservés aux personnes les plus importantes de mon univers Ma Famille.

Merci à tous ceux qui ont contribué de près ou de loin pour que cette thèse soit finie.

À la mémoire de mon Père,

*À tous les êtres chers dont leur soutien m'a été
indispensable et qui attendent avec impatience ma réussite,*

En espérant être à la hauteur de leurs attentes.

Acronymes

AdD	Arbre de défaillance
AdE	Arbre d'Événement
AMDE	Analyse des modes de défaillance et de leurs effets
AQR	Analyse quantitative des risques
AQRT	Analyse quantitative des risques technologiques
BLEVE	Vaporisation violente à caractère explosif (boiling liquid expanding vapor explosion)
CdM	Chaînes de Markov
CM	Coupe minimale
DDB	Diagramme de décision binaire
FDMS	Fiabilité, disponibilité, maintenabilité et sécurité
FID	Facteur d'importance de Diagnostic Fussel-Vesely
FIC	Facteur d'importance probabiliste Critique
FIM	Facteur d'importance probabiliste marginale de Birnbaum
FIP	Facteurs d'importance probabilistes
GPL	Gaz de pétrole liquéfié
HAZID	hazard identification
HAZOP	hazard and operability
IA	Intelligence Artificiel
LF	Logique floue

MC simulation	Simulation de Monte Carlo
MDT	Durée moyenne d'indisponibilité (Mean Dawn Time)
MTBF	Durée moyenne entre deux défaillances consécutives d'une entité réparée. (Mean Time Between Failure)
MTTF	Durée moyenne de fonctionnement avant la première défaillance (Mean Time To Failure)
MTTR	Durée moyenne de réparation (Mean Time To Repair)
MUT	Durée moyenne de fonctionnement après réparation (Mean Up Time)
RB	Réseau Bayésien
RdN	Réseau de neurones
RdP	Réseau de Pétri
REX	Retour d'expérience
SDE	Système déluge à eau
SdF	Sûreté de fonctionnement
TPC	Table de probabilités conditionnelles
TPE	Test périodique étendu
TPS	Test périodique simple
VCE	Explosion d'un nuage de gaz ou des vapeurs (Vapor Cloud Explosion)

Nomenclature

$R(t)$	Reliability, Fiabilité dépendant du temps t
$F(t)$	Défiabilité dépendant du temps t
$A(t)$	Availability, Disponibilité dépendant du temps t
$U(t)$	L'indisponibilité dépendant du temps t
$M(t)$	Maintenability, Maintenabilité dépendant du temps t
$f(t)$	La densité de probabilité
λ (lambda)	Taux de défaillance constant.
$\lambda(t)$	taux de défaillance instantané.
μ (mu)	Taux de réparation (inverse de la MTTR).
$\gamma(t)$ (gamma)	Taux de défaillance à la sollicitation instantané.
X_n	Distribution d'entrée d'un système
$P[X = 1]$	La probabilité que X soit en état de fonctionnement
$P[X = 0]$	La probabilité que X soit en état de défaillance
$I_i^B(t)$	Facteur d'importance Marginale de Birnbaum
$I_i^{CR}(t)$	Le facteur d'importance critique
$p_{(s i)}(t)$	la probabilité conditionnelle que le système 's' soit défaillant sachant que le composant 'i' est défaillant dépendant du temps t
$P_{(s i)}(t)$	La probabilité conditionnelle que le système 's' soit défaillant sachant que le composant 'i' est en fonctionnement dépendant du temps t .
G	Graphe acyclique orienté
V	L'ensemble des nœuds de G

E	L'ensemble des arcs de G
θ	Ensemble des probabilités de chaque nœud conditionnellement à l'état de ses parents(racine) dans G
$p_i(t)$	La probabilité du composant ' i ' à l'instant ' t '
$p_s(t)$	La probabilité Systeme ' s ' à l'instant ' t '

Glossaire

Selon la norme CEI 61508 [IEC 02] et AFNOR [AFN 88]:

Système :

Ensemble d'éléments qui interagissent selon un modèle précis, un élément pouvant être un autre système, appelé sous-système, les sous-systèmes pouvant être eux-mêmes soit un système de commande soit un système commandé composé de matériel, des composants.

Sous-système :

Ensemble de composant (mécanique, électromécanique, électronique, ...).

Composant :

Un composant est une partie d'un système (matériels ou évènements), non décomposable dans le cadre de l'étude, et pour laquelle on dispose d'informations qualitatives (conditions de fonctionnement, modes de défaillance, ...) et quantitatives (fréquences d'apparitions des pannes, durées de bon fonctionnement, ...) suffisantes. Le type de composants, leurs quantités, leur qualité et leur manière dont ils sont disposés ont un effet direct sur la fiabilité du système.

Entité :

Tout élément, composant, sous-système, système, dispositif, équipement, unité fonctionnelle que l'on peut considérer individuellement.

Redondance

Existence de plus de moyens que strictement nécessaire pour accomplir une fonction requise dans une unité fonctionnelle ou pour représenter des informations par des données.

Sûreté de fonctionnement :

La sûreté de fonctionnement est l'aptitude d'une entité à satisfaire une ou plusieurs fonctions requises dans des conditions données. La sûreté de fonctionnement se caractérise généralement par les paramètres suivants : Fiabilité, Maintenabilité, Disponibilité et Sécurité. On retrouve dans les initiales de ces concepts, le nom de FMDS parfois donné à la sûreté de fonctionnement.

Fiabilité :

Aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant une durée donnée.

Disponibilité:

La disponibilité d'une entité est la probabilité qu'elle accomplisse les fonctions requises dans des conditions données et à un instant donné. Le système peut avoir été réparé dans le passé.

Maintenabilité :

Dans des conditions données d'utilisation pour lesquelles il a été conçu, aptitude d'un bien à être maintenu ou rétabli dans un état dans lequel il peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données, avec des procédures et des moyens prescrits.

Maintenance :

Ensemble des actions permettant de maintenir ou de rétablir une entité dans un état spécifié ou en mesure d'assurer un service déterminé.

Sécurité :

La sécurité est une aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

Défaillance :

Cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise. Une défaillance est un passage d'un état à un autre, par opposition à une panne qui est un état. On entend par "unité fonctionnelle" soit un système complet, soit l'un quelconque de ses éléments.

Défaillance de cause commune :

Défaillance résultant d'un ou plusieurs événements qui, provoquant des défaillances simultanées de deux ou plusieurs canaux séparés dans un système multicanal, conduit à la défaillance du système.

Taux de défaillance :

C'est la probabilité pour que le système soit défaillant, cette définition s'applique pour tout type d'éléments (système, sous-système, composant).

Mode de défaillance :

Effet par lequel une panne est observée.

Panne :

État d'une entité inapte à accomplir une fonction requise, dans des conditions données d'utilisation.

Taux de panne :

Probabilité d'apparition d'une panne dans un intervalle donné, sachant qu'aucune panne n'ait été observée avant, par unité de temps.

Réparable:

Entité susceptible techniquement et/ou économiquement d'être réparée.

Non-réparable :

Entité non susceptible techniquement et/ou économiquement d'être réparée.

Temps de réparation :

Temps pendant lequel les opérations de maintenance corrective sont effectivement réalisées sur l'entité, tous les temps annexes étant exclus.

Temps de fonctionnement avant la première panne (MTTF) :

Durée cumulée des temps de fonctionnement d'une entité depuis l'instant de sa première mise en service jusqu'à l'apparition de la première panne.

Temps moyen de bon fonctionnement (MTBF) :

Temps moyen entre deux pannes consécutives d'une entité réparée à neuf.

MDT (Mean Down Time)

Durée moyenne d'indisponibilité ou de défaillance. Elle correspond à la détection de la panne, la réparation de la panne et la remise en service.

Table des Matières

Remerciement

Dédicace

Acronymes

Nomenclature

Glossaire

Table des Matières

Table des Figures

Table des Tableaux

Chapitre I. Introduction Générale

1.1. Contexte.....	2
1.2. Problématique.....	4
1.3. Objectifs de la thèse.....	4
1.4. Plan générale de la thèse.....	5

Chapitre II. Revue de littérature sur l'analyse par sûreté de fonctionnement

2.1. Introduction	10
2.2. Sûreté de fonctionnement des systèmes	11
2.2.1. Définition de la sûreté de fonctionnement	11
2.2.2. Composantes de la SdF	11
2.2.2.1. Fiabilité $R(t)$	11
2.2.2.2. Disponibilité $A(t)$	12
2.2.2.3. Maintenabilité $M(t)$	12
2.2.2.4. Sécurité	13
2.2.3. Métriques de la Sûreté de Fonctionnement	13
2.2.4. Défaillance	14
2.2.4.1. Taux de défaillance $\lambda(t)$	14

2.2.4.2. Taux de réparation $\mu(t)$	15
2.2.4.3. Le taux de défaillance à la sollicitation	15
2.2.5. Approche de la fiabilité par les probabilités.....	16
2.2.6. Autres Principales lois de probabilité	16
2.2.6.1. Les lois de probabilité discrètes	16
2.2.6.2. Les lois de probabilité continues	17
2.3. Notion de Système.....	17
2.3.1. Système et composant	17
2.3.2. Structure d'un système.....	18
2.3.3. Fonctionnement d'un système.....	18
2.3.4. Fiabilité d'un système	19
2.3.4.1. Système série	20
2.3.4.2. Système parallèle.....	20
2.3.4.3. La fiabilité tout au long du cycle de vie d'un système	20
2.3.4.5. Modélisation de la fiabilité des systèmes	21
2.3.4.6. Recueil de données / Bases de données de la fiabilité.....	21
2.4. Conclusion	22

Chapitre III. Démarches et méthodes d'analyse quantitative des risques

3.1. Introduction	25
3.1. Analyse structurelle et fonctionnelle du système	26
3.1.1. Analyse fonctionnelle du système.....	26
3.2. Description des méthodes d'analyse prévisionnelle des risques	27
3.2.1. Qualitative / quantitative	27
3.2.1.1. Méthodes qualitatives	27
3.2.1.2. Méthodes quantitatives	27
3.2.2. Inductive / déductive	27
3.2.2.1. Méthodes inductives	27
3.2.2.2. Méthodes déductives	27
3.2.3. Statiques/dynamiques.....	28
3.2.3.1. Méthodes statiques	28
3.2.3.2. Méthodes dynamiques	28
3.3. Analyse et évaluation dysfonctionnelles	29
3.3.1. AMDE / AMDEC	30

3.3.1.1. AMDE (Analyse des modes de défaillances, de leurs effets).....	30
3.3.1.2. AMDEC (L'analyse des modes de défaillances, de leurs effets et de leur criticité).....	31
3.3.2. Arbre de défaillance	33
3.3.2.1. Analyse qualitative	34
3.3.2.2. Analyse quantitative :	34
3.3.2.3. Facteurs d'importance probabilistes	35
3.3.3. L'arbre d'évènement	37
3.3.4. Simulation de Monte Carlo	38
3.3.5. Réseaux bayésiens.....	40
3.3.6. Réseau de Petri stochastique	40
3.3.6.1. RdP stochastiques classique	42
3.3.6.2. RdP stochastiques généralisés	42
3.3.6.3. RdP stochastiques déterministes :	42
3.3.7. Graphes de Markov	43
3.4. Limitation des méthodes d'analyse quantitatives des risques	44
3.5. Critères de choix d'une méthode d'analyse de risque	46
3.6. Conclusion	47

Chapitre IV. L'approche bayésienne en Analyse des risques

4.1. Introduction	49
4.2. Réseaux Bayésiens	49
4.2.1. Théorème de Bayes'	50
4.2.1.1. Formule de Recomposition.....	51
4.2.1.2. Formule de Bayes	51
4.2.2. Définition du Réseau Bayésien	52
4.2.3. Inférence.....	54
4.2.4. Méthodes de simplification du réseau	55
4.2.5. Réseaux Bayésiens Dynamiques	55
4.2.6. Utilisation des Réseaux Bayésiens.....	55
4.2.7. Limites des Réseaux Bayésiens	56
4.3. Réseaux Bayésiens pour l'analyse quantitative des risques	57
4.3.1. Utilisation des réseaux bayésiens en analyse des risques :	57
4.3.2. Interprétation de AdD en RB	59
4.3.2.1. Convertir l'AdD en RB	61

4.3.2.2. RB obtenu à partir de AdD avec des événements répétés	64
4.3.2.3. L'inférence sur le RB obtenue à partir de AdD.....	66
4.3.3. Facteur d'importance probabiliste en RB	66
4.4. Conclusion	67

Chapitre V. FDMA du système déluge dans la zone de stockage du GPL

5.1. Introduction	70
5.2. Identification des Systèmes à étudier	70
5.2.1. Zone de stockage du GPL	70
4.2.1.1. Stockage sous pression	70
5.2.1.2. Scénarios et phénomènes dangereux dans la zone de stockage de GPL	72
5.2.1.3. Synthèse :	74
5.2.2. Le système déluge à eau comme barrière de sécurité	74
5.2.2.1. Description du système déluge à eau.....	74
5.2.2.2. Équipements et fonctionnement du système déluge à eau	74
5.3. Données d'étude de fiabilité du système déluge.....	76
5.4. Etude FDMA du système déluge à eau	77
5.4.1. Analyse des composants	77
5.4.2.1. AMDE des composants	77
5.4.2.2. Simulation de Monté Carlo	79
5.4.2.3. Fiabilité et disponibilité des composants.....	82
5.4.2.4. Analyse du système	92
5.4.2.4.1. Développement de l'arbre de défaillance	92
5.4.2.4.2. Fiabilité et disponibilité des sous-systèmes et du système	93
5.4.2.4.3. Coupes minimales et leurs importances	97
5.4.2.4.4. Facteurs d'importances probabilistes	98
5.5. Conclusion	101

Chapitre VI. Modèle d'aide à la décision pour les systèmes déluge

6.1. Introduction	103
6.2. Réseau bayésien du système déluge à eau.....	103
6.2.1. Structure du RB à partir de l'AdD.	103
6.2.2. Comparaison des résultats par les différentes méthodes.....	104
6.3. Inférence bayésienne pour l'aide à la décision	105
6.3.1. Exemple d'inférence établie sur le réseau.....	105

6.3.2. Facteurs d'importance obtenus par l'inférence bayésienne	106
6.4. Optimisation des performances du design par processus décisionnel	109
6.4.1. FDMS du nouveau design	111
6.5. Conclusion	116

Chapitre VII. Conclusion Générale

7.1. Conclusion	118
7.2. Bilan.....	118
7.3. Perspectives	119

Annexes

Annexe A : Bases de données et lois de probabilité

A.1. Les lois de probabilité utilisées en fiabilité.....	131
A.1.1. La loi exponentielle	131
A.1.2. Loi de Weibull.....	131
A.1.3. Loi normale	132
A.1.4. Loi log-normale ou loi de Galton	132
A.1.5. Loi uniforme.....	133
A.2. Bases de données	133
A.2.1. Bases de données de fiabilité	133
A.2.2 Limite d'utilisation des bases de données mécaniques	135

Annexe B : Panorama des méthodes d'analyse prévisionnelle

B.1. Analyse par l'AMDEC	137
B.1.1. Effet d'un mode de défaillance :	137
B.1.2. Les modes de défaillance.....	137
B.1.3. Criticité et tableau d'AMDEC	138
B.2. Analyse par Arbre de Défaillances	139

Table des Figures

Figure 2.1 La fiabilité décroissante avec le temps	12
Figure 2.2 Métriques de la Sûreté de Fonctionnement.....	13
Figure 2.3 Évolution du taux de défaillance au cours du temps : courbe en baignoire.....	15
Figure 2.4 Différence entre système compliqué et système complexe	18
Figure 2.5 les différentes configurations de système.	19
Figure 3.1 Organigramme des tâches d'une analyse prévisionnelle	26
Figure 3.2 Organigramme de la méthode AMDE	32
Figure 3.3 Exemple d'une structure d'arbre de défaillance	34
Figure 3.4 Exemple de la structure d'arbre d'événement.....	38
Figure 3.5 Organigramme d'analyse de systèmes par simulation de Monté Carlo.....	39
Figure 3.6 Exemple de réseau de Petri	41
Figure 3.7 Exemple de graphe de Markov	43
Figure 4.1 Thomas Bayes connu pour avoir formulé le théorème de probabilité conditionnelle	50
Figure 4.2 Principe de l'approche Bayésienne.	51
Figure 4.3 RB ou X est la cause de Y	52
Figure 4.4 Réseau bayésien d'un système de détection.	53
Figure 4.5 Taux d'utilisation des réseaux bayésiens en sûreté de fonctionnement	58
Figure 4.6 Tendances d'utilisation des réseaux bayésiens dans l'analyse des risques	58
Figure 4.7 Les publications les plus citées sur les réseaux bayésiens liées à l'analyse des risques jusqu'à 2008.....	59
Figure 4.8 Organigramme représentant un algorithme simplifié pour représenter un AdD en RB.....	61
Figure 4.9 Exemple de Structure d'AdD.....	62
Figure 4.10 Structure du réseau bayésien obtenu à partir de la Figure 4.9	62

Figure 4.11 Arbre de défaillance avec un événement répété	64
Figure 4.12 Réseau bayésien avec nœud répété	64
Figure 4.13 Arbre de défaillance avec une branche répétée.....	65
Figure 4.14 Réseau bayésien avec une branche répétée.....	65
Figure 5.1 Organigramme représentant la démarche de l'évaluation de la sûreté de fonctionnement du système	71
Figure 5.2 Schéma pour décrire les éléments importants composants une sphère de stockage du GPL	72
Figure 5.3 Arbre d'évènement des scénarios catastrophiques dans la zone de stockage de GPL	73
Figure 5.4 Système déluge à eau installé sur une sphère de GPL	75
Figure 5.5 Schéma simplifiant des équipements du système déluge à eau	76
Figure 5.6 Variation de l'indisponibilité du système a t= 8760h par rapport au nombre d'échantillons	80
Figure 5.7 Variation de l'écart type du système a t= 8760h par rapport au nombre d'échantillons	80
Figure 5.8 Variation de l'indisponibilité du système a t= 43800h par rapport au nombre d'échantillons	80
Figure 5.9 Variation de l'écart type du système a t= 43800h par rapport au nombre d'échantillons	81
Figure 5.10 Variation de l'indisponibilité du système a t= 87600h par rapport au nombre d'échantillons	81
Figure 5.11 Variation de l'écart type du système a t= 87600h par rapport au nombre d'échantillons	81
Figure 5.12 Modèle d'indisponibilité représentant la durée de vie d'un composant par teste périodique simple	83
Figure 4.13 Disponibilité et fiabilité du détecteur de flamme.....	83
Figure 5.14 Disponibilité et fiabilité du capteur de pression	84
Figure 5.15 Disponibilité et fiabilité du capteur de niveau	85
Figure 5.16 Modèle d'indisponibilité représentant la durée de vie d'un composant par test périodique étendu	86
Figure 5.16 Disponibilité et fiabilité de la pompe anti incendie	86
Figure 5.17 Disponibilité et fiabilité du moteur électrique	87
Figure 5.18 Disponibilité et fiabilité du moteur diesel.....	88
Figure 5.19 Disponibilité et fiabilité de la vanne manuelle	88
Figure 5.20 Disponibilité et fiabilité du filtre d'eau.....	89

Figure 5.21 Disponibilité et fiabilité de la vanne globe	90
Figure 5.22 Disponibilité et fiabilité de la vanne automatique	90
Figure 5.23 Disponibilité et fiabilité de la pompe du puit	91
Figure 5.24 La structure de l'arbre de défaillance du système déluge à eau avec l'extension de la défaillance du sous-système des pompes en (a), où les événements de base sont énumérés dans le Tableau 5.3.....	93
Figure 5.25 Indisponibilité et défiabilité du système logique de détection.....	93
Figure 5.26 Indisponibilité et défiabilité du système de pompes	94
Figure 5.27 Indisponibilité et défiabilité du système de stockage	95
Figure 5.28 Indisponibilité et défiabilité du système déluge à eau	95
Figure 5.29 Facteur d'importance marginale à 8760h	98
Figure 5.30 Facteur d'importance marginale à 87600h	99
Figure 5.31 Facteur d'importance critique à 8760h	99
Figure 5.32 Facteur d'importance Critique à 87600h	99
Figure 5.33 Facteur d'importance Critique des composants comparé par leur influence sur l'indisponibilité du système	100
Figure 6.1 Structure du réseau bayésien de l'indisponibilité du système déluge à eau, où les nœuds parents sont présentés dans le Tableau 5.3	103
Figure 6.2 l'indisponibilité du système déluge par différentes méthodes.....	104
Figure 6.3 Exemple de la variation d'indisponibilité du système à t = 87600 h avant et après l'inférence bayésienne de quelques composants.....	106
Figure 6.4 Processus décisionnel d'un système industriel	110
Figure 6.5 l'indisponibilité du système déluge à eau après optimisation du design.	114
Figure B.1 Exemple de matrice de criticité.....	138
Figure B.2 Tableau générique d'AMDEC	139
Figure B.3 Les éléments de base pour la construction de la structure de l'arbre de défaillance	139

Table des Tableaux

Tableau 2.1 Lois de probabilité.....	17
Tableau 3.1 Principales méthodes et démarche de la fiabilité	28
Tableau 3.2 Probabilités de défaillance propagées à l'aide d'équations de logique booléien... 35	
Tableau 3.3 Résumé sur les avantages et les limites des méthodes d'analyse quantitatives des risques.....	44
Tableau 4.1 TPC du nœud alarme.....	54
Tableau 4.2 TPC du nœud Evacuation.....	54
Tableau 4.3 Travaux de recherche sur le passage de l'arbre de défaillance vers les réseaux bayésiens	59
Tableau 4.4 TPC de la porte logique « Ou ».....	63
Tableau 4.5 TPC de la porte logique « et ».....	63
Tableau 4.6 TPC de la porte logique « 2 sur 3».....	63
Tableau 5.1 Probabilités d'occurrence des évènements qui peuvent survenir suite à une perte de confinement au niveau de la zone de stockage du GPL. [MAN 05], [OLF 04].....	73
Tableau 5.2 Fréquences d'occurrences des Scénarios catastrophiques dans la zone de stockage du GPL	74
Tableau 5.3 Données de fiabilité des composants du système de déluge d'eau [MAN 05], [SIN 02].....	77
Tableau 5.4 Extrait d'AMDE de quelques composants du systèmes déluge a eau.....	78
Tableau 5.5 Métriques de la sûreté de fonctionnement du détecteur de flamme	83
Tableau 5.6 Résumé de disponibilité et de fiabilité du détecteur de flamme.....	83
Tableau 5.7 Métriques de la sûreté de fonctionnement du capteur de pression.....	84
Tableau 5.8 Résumé de disponibilité et de fiabilité du capteur de pression	84
Tableau 5.9 Métriques de la sûreté de fonctionnement du capteur de niveau.....	84

Tableau 5.10 Résumé de disponibilité et de fiabilité du capteur de niveau	84
Tableau 5.11 Métriques de la sûreté de fonctionnement de la pompe anti incendie.....	86
Tableau 5.12 Résumé de disponibilité et de fiabilité de la pompe anti incendie	86
Tableau 5.13 Métriques de la sûreté de fonctionnement du moteur électrique.....	87
Tableau 5.14 Résumé de disponibilité et de fiabilité du moteur électrique	87
Tableau 5.15 Métriques de la sûreté de fonctionnement du moteur diesel	87
Tableau 5.16 Résumé de disponibilité et de fiabilité du moteur diesel.....	87
Tableau 5.17 Métriques de la sûreté de fonctionnement de la vanne manuelle.....	88
Tableau 5.18 Résumé de disponibilité et de fiabilité de la vanne manuelle	88
Tableau 5.19 Métriques de la sûreté de fonctionnement du filtre d'eau	89
Tableau 5.20 Résumé de disponibilité et de fiabilité du filtre d'eau.....	89
Tableau 5.21 Métriques de la sûreté de fonctionnement de la vanne globe.....	89
Tableau 5.22 Résumé de disponibilité et de fiabilité de la vanne globe	89
Tableau 5.23 Métriques de la sûreté de fonctionnement de la vanne automatique.....	90
Tableau 5.24 Résumé de disponibilité et de fiabilité de la vanne automatique	90
Tableau 5.25 Métriques de la sûreté de fonctionnement de la pompe du puit.....	91
Tableau 5.26 Résumé de disponibilité et de fiabilité de la pompe du puit	91
Tableau 5.27 Métriques de la sûreté de fonctionnement du système logique de détection	93
Tableau 5.28 Résumé de disponibilité et de fiabilité du système logique de détection	94
Tableau 5.29 Métriques de la sûreté de fonctionnement du système de pompes.....	94
Tableau 5.30 Résumé de disponibilité et de fiabilité du système logique de détection	94
Tableau 5.31 Métriques de la sûreté de fonctionnement du système de stockage	94
Tableau 5.32 Résumé de disponibilité et de fiabilité du système de stockage.....	95
Tableau 5.33 Métriques de la sûreté de fonctionnement du système déluge	95
Tableau 5.34 Résumé de disponibilité et de fiabilité du système déluge.....	96
Tableau 5.35 évènement intermédiaire et sous-systèmes.....	97
Tableau 5.36 nombre de coupes minimales et leurs contributions dans l'évènement sommet avec exemple d'indisponibilité de la grande coupe minimale dans chaque ordre à $t = 87600$ h	98
Tableau 6.1 Comparaison des facteurs d'importance pour le capteur de niveau	107
Tableau 6.2 Comparaison des facteurs d'importance pour le capteur de pression	107
Tableau 6.3 Comparaison des facteurs d'importance pour la vanne déluge	108
Tableau 6.4 Comparaison des facteurs d'importance pour la vanne automatique 2	109
Tableau 6.5 les décisions prises sur les 4 composants	110

Tableau 6.6 Résultats d'aide à la décision sur la vanne déluge	111
Tableau 6.7 Résultats d'aide à la décision sur le capteur de niveau	112
Tableau 6.8 Résultats d'aide à la décision sur la vanne automatique 2	113
Tableau 6.9 Résultats d'aide à la décision sur le capteur de pression.....	113
Tableau 6.10 synthèse des résultats d'aide à la décision par réseau bayésien	115
Tableau A.1 Quelques bases de données de fiabilité	133
Tableau B.1 liste de modes de défaillance	137
Tableau B.2 Criticités et probabilités des défaillances	138
Tableau B.3 Règles d'optimisation des arbres de défaillances	140

Chapitre I

Introduction Générale

Sommaire du chapitre:

- 1.1. Contexte..... 2
- 1.2. Problématique 4
- 1.3. Objectifs de la thèse..... 4
- 1.4. Plan générale de la thèse..... 5

1.1. Contexte

L'industrie pétrolière a connu un grand accroissement technologique ces dernières années, d'où la variété et la complexité des procédés et des installations industrielles. Comme résultats des accidents majeurs inhérents tels que les incendies, les phénomènes de BLEVE (vaporisation violente à caractère explosif) et de VCE (Explosion d'un nuage de gaz ou des vapeurs) [ALS 14] ainsi que les Effets domino [NEC 15], [KAD 13], [MAN 05] entraînant de grave conséquence sur l'homme, les installation, l'environnement et l'économie.

La zone de stockage du gaz de pétrole liquéfié (GPL) avec ces installations et sphères de stockage sous pression est l'une des zones où ces scénarios catastrophiques sont plus fréquents à cause de la présence des substances inflammables. Des études de recherche ont montrés que 89% des substances inflammables étaient impliquées dans les accidents d'effet domino [ABD 11], [DAR 10]. Parmi ces accidents catastrophiques les plus récents au niveau des installations de GPL on cite le cas Virginie, au Mississippi (États-Unis), celui de Viareggio (Italie) et plusieurs d'autres [ALS 14].

Afin de garantir la sécurité de ces installations tout en respectant les objectifs de production, des barrières de sécurité robustes et de haute qualité doivent être installées en répondant à des exigences de disponibilité à la demande.

L'une des barrières de sécurité typiques installé dans les zone de stockage de GPL est le système déluge à eau (SDE) [NOL 14], [INC 10], [NEI 07], [BEL 07]. Le système déluge à eau est capable de réduire la gravité des dommages causé par les scénarios catastrophiques par la réduction des températures élevées ainsi que les flux de chaleur [DAV 04], [ROB 04], [VAN 00] en créant des rideaux d'eau. Un système déluge à eau installé dans un complexe de GPL doit être vraiment fiable et disponible pendant toute sa durée de vie en raison de la probabilité d'occurrence élevée des scénarios d'incendies et des effets dominos.

Afin d'assurer un haut niveau de fiabilité, disponibilité, maintenabilité, et sécurité (FDMS) [BEL 16], [DEM 09] des barrières de sécurité, des études d'analyse de risque concrètes et plus approfondies [MAZ 08] doivent être établies afin de mettre en évidence les points critiques au regard de la sécurité de ces systèmes de sécurité et aussi de déterminer les pratiques de maîtrise de leur fonctionnement optimale durant leur durée de vie. Pour cela des analyses qualitatives, semi-quantitatives et quantitatives de risque [KHA 15], [SMI 01], [SPO 99], [VIN 99] ont été développées, elles reposent sur les principes de la sûreté de fonctionnement : Une connaissance parfaite du système à analyser et son environnement est un nombre important de données obtenu par retour d'expérience ou bien par jugements d'expert [BEL 16] [MAN 05].

L'analyse des modes de défaillance et de leurs effets (AMDE) [BOU 13], [TAY 13], [RAU 04] est considérée comme étant une méthode d'analyse qualitative des risques parmi les méthodes les plus recommandées dans l'analyse détaillée de chaque composant que ce soit mécanique ou électronique [PRO 11] qui constitue le système déluge à eau. L'arbre de défaillance (AdD) est aussi, l'une des meilleures méthodes quantitatives utilisées par une large variété d'industrie dans différentes étapes de réalisations de leurs projets (conception, construction ou exploitation et même destruction en fin de cycle de vie) [GUE 18], [KAB 17], [RUI 15], [YU 07],[SMI 01], Elle est utilisée pour l'analyse approfondie du système déluge à eau. L'AMDE permet d'identifier les différents modes de défaillance des composants, leurs causes et leurs effets sur le fonctionnement du système. Par la suite, les composants qui représentent des lacunes vis-à-vis le bon fonctionnement du système sont sélectionnés pour être étudiés profondément et en détail par AdD et ces différentes étapes d'analyse en se basant sur l'ingénierie de la sûreté de fonctionnement.

Un AdD standard présente certaines limites surtout par rapport à l'étude des systèmes complexes, ainsi que les défaillances dépendantes du temps [KHA 13-1], [KHA 11], [BOB 01] à partir de ces limites plusieurs approches pour développer l'AdD ont été proposées pour des études approfondies et dynamiques tels que diagramme de décision binaire (DDB) [DEN 15], [MAT 15], [MER 14] utilisé pour développer efficacement la structure de l'AdD et calculer l'ensemble de coupes minimales (CM), La simulation de Monte Carlo (MC) pour étudier la continuité dans le temps et pour calculer la fiabilité du système par AdD ainsi que la propagation des incertitudes [DUR 09], [MER 16] ainsi que d'autres approches tels que les réseaux de Pétri (RdP) [TAL 16], la logique floue (Lf) [CHE 17], les chaînes de Markov (CdM) [RUI 15] et les réseaux de neurones (RdN)[WAN 12].

Afin de déterminer quel composant contribue le plus dans la défaillance du système étudié par AdD le calcul des facteurs d'importance probabilistes (FIP) [KUO 12] est le plus favorable. Le facteur d'importance probabiliste marginale de Birnbaum (FIM) ou bien le facteur d'importance probabiliste Critique (FIC) sont les plus utilisés pour l'identification et l'évaluation des composants qui représentent un risque sur la disponibilité du système à temps réel, pour le principal but d'établir l'adaptation de nouvelles mesures correctives ou préventives, programmer des tâches de maintenance et / ou optimisation de la conception du système [GUE 18], [AIS 17], [AIS 15] [VAU 11], [VAU 10].

1.2. Problématique

Tous ces techniques et modèles mathématiques d'analyse des risques développés par AdD sont devenus un thème de recherche important mais les solutions à proposer sont loin d'être évidentes, due au manque d'aide à la décision en temps réel des systèmes complexes très importants tels que les systèmes déluges à eau qui jouent un grand rôle dans la protection de l'être humain, les installations, l'environnement et l'économie.

En Algérie, la gestion classique des risques par ces différentes méthodes présente des lacunes considérables pour une cause principale, c'est la non maîtrise de l'aide à la décision qui représente aujourd'hui la solution pour de nombreux problèmes de gestion. Souvent en s'appuyant sur l'utilisation des modèles d'Intelligence Artificiel (IA) [OUA 14], [COR 03]. Alors ce domaine nécessite une maîtrise parfaite et en temps réel relatif de l'information afin d'établir une analyse quantitative des risques (AQR) [SMI 01] approfondie pour contrôler le système à étudier d'où le choix des réseaux Bayésiens (RB) [NAI 07] qui jouent un rôle très important dans la prédiction et la prise de décision.

1.3. Objectifs de la thèse

Les réseaux bayésiens (RB) sont un outil idéal pour modéliser des systèmes complexes et dynamiques dans le temps par leur capacité à représenter la relation entre les composants et leur fonctionnement dans un système et en quantifiant ces relations ainsi que par les probabilités conditionnelles en donnant un modèle prouvé mathématiquement donc fiable et analysable.

En effet, leur utilisation dans le domaine de l'analyse de la fiabilité, la disponibilité, la maintenabilité et Sécurité (FDMS) et analyse des risques en générale [WEB 12], [BIR 07], [SMI 01] a connu un grand accroissement par le fait que le modèle peut effectuer des analyses prévisionnelles et opérationnelles tels que le diagnostic et le changement de design du système (conception) et son optimisation [BOB 01].

A cet effet l'objectif de cette thèse est d'établir une analyse quantitative des risques sur un système déluge à eau installé dans la zone de stockage de GPL sous pression. Nous commencerons par une analyse AMDE pour déterminer les modes de défaillance des composants et de sélectionner les plus indésirables pour le fonctionnement du système ensuite, une modélisation des défaillances probables des différents composants du système sera réalisée par AdD en prenant en considération le traitement des données en effectuant une simulation de Monté Carlo. La structure de l'AdD sera améliorée en ajoutant le diagramme de décision binaire A ce niveau-là, une analyse quantitative de qualité peut être effectuée : Détermination de chaque coupe minimale dans le système et leurs importance et contribution dans

l'indisponibilité du système. Par la suite, la contribution de chaque composant sur l'indisponibilité du système sera analysée, en utilisant les facteurs d'importance probabiliste Marginale et Critique.

Les résultats obtenus à partir de ces différentes approches, en plus des jugements d'experts et les données du retour d'expérience (REX), sont utilisées, comme étant des données a priori permettant le développement du réseau bayésien considéré comme étant l'outil d'aide à la décision dynamique et en temps réel du système déluge a eau. Ce réseau Bayésien sera développé directement à partir de la structure de l'AdD selon un algorithme déterminé [JUN 17], [DON 16], [BAD 13], [CAI 13], [KHA 13-2], [WEB 12], [KAL 09] [LAM 09].

Par la suite, nous proposerons une méthodologie d'obtention des résultats en posteriori des facteurs d'importance probabiliste par les réseaux bayésiens. L'inférence bayésienne sera exploitée pour la prise de décision [GUE 18], [FON 13], [MUR 02] en modifiant le design du système afin d'assurer un haut niveau FDMS du système déluge a eau

Ce concept d'obtenir les facteurs d'importance probabiliste par l'inférence bayésienne permet d'identifier les composants qui contribuent à l'indisponibilité du système et de déterminer le moment où une défaillance s'est produite dans le système. Elle permettra aussi de générer une liste des défaillances de composants pouvant être à l'origine du dysfonctionnement du système. Par la suite, établir les bonnes décisions par l'optimisation des performances du système soit par la proposition des redondances sur les composants clés, par maintenance préventive des composant réparable ou par remplacement des composants non réparable, afin de garantir la fiabilité du système avant qu'une panne grave ne se produise.

1.4. Plan générale de la thèse

Cette thèse est organisée de tel manière qu'elle englobe l'état de l'art sur l'analyse quantitative des risques en passant par le principe de la sûreté de fonctionnement, les méthodes d'analyse quantitatives des risques, les réseaux Bayésien et l'approche originale de la définition d'aide à la décision basée sur l'utilisation conjointe de l'analyse quantitative des risques et de l'approche bayésienne pour élaborer un réseau dynamique.

Ce Chapitre introductif est consacré au cadre de l'étude. L'état de l'art sur les sujets de recherche récents et du même domaine, est présenté, afin de développer une thématique robuste qui répond à la problématique. Et à la fin, le chapitre met en valeur les objectifs à atteindre par ce présent travail.

Le 2ème et 3ème chapitres présentent une revue de littérature sur les principes de sûreté de fonctionnement d'une manière générale d'une part (chapitre 2), et les méthodes d'analyse

quantitative des risques appliqués en sûreté de fonctionnement d'autre part (chapitre3). L'accent sera mis sur les systèmes, les composants du système, le concept fiabilité, disponibilité et maintenabilité des composants et du système. Les principales démarches d'analyse par AdD seront également abordées ainsi que d'autres méthodes d'analyse.

Dans le 4^{ème} chapitre, une présentation générale de l'approche Bayésienne sera proposée, afin de mettre en évidence les réseaux Bayésiens considérés comme étant l'étape la plus importante dans notre démarche de recherche. Par la suite, nous nous intéresserons à l'application des réseaux Bayésien pour la sûreté de fonctionnement et comment établir le réseau à partir de l'arbre de défaillance. Nous présenterons aussi notre démarche pour obtenir les résultats des facteurs d'importance probabilistes en termes de probabilité posteriori en fonction de l'inférence bayésienne. A la fin de ce chapitre, il serait possible de définir un modèle d'aide à la décision par les réseaux bayésiens applicables dans le domaine de la sûreté de fonctionnement. Ceci par l'utilisation conjointe de l'analyse quantitative des risques et de l'approche bayésienne. Nous accordons ici une attention particulière aux travaux de recherches basées sur l'apport des réseaux bayésiens à la sécurité des.

Le 5^{ème} chapitre a pour objectifs de présenter le système déluge à eau installé dans la zone de stockage de GPL étant notre cas d'étude. Nous établirons l'arbre de défaillance par ces différentes étapes. En se basant sur l'analyse préliminaire qualitative qui avait pour objectif de déterminer l'évènement redouté : le dysfonctionnement du système déluge à eau. Nous calculerons aussi des facteurs d'importances probabilistes selon un formalisme mathématique pour déterminer les composants qui contribuent au dysfonctionnement du système.

Le 6^{ème} chapitre est dédié au développement du réseau bayésien et à l'estimation de son efficacité par la comparaison des résultats obtenus avec ceux obtenue par les méthodes classiques. Par la suite des inférences bayésiennes sont établies afin d'obtenir les facteurs d'importance probabilistes et les comparer avec ceux obtenus par les modèles mathématiques numériques. Des mesures d'aide à la décision pour l'optimisation des performances du design sont proposées, soit par maintenances préventives, soit par redondances sur les composants jugés importants. A la fin des mise-à-jours de données à partir du nouveau design sont ajoutés au réseau bayésien.

A la fin une **conclusion et des perspectives** sont proposées. Ce chapitre a pour objectifs de faire le bilan sur nos travaux de recherche et de mettre en relief quelques nouvelles pistes de recherche à explorer.

Des informations complémentaires aux différents chapitres sont citées dans plusieurs Annexes.

Chapitre II

Revue de littérature sur l'analyse par sûreté de fonctionnement

Sommaire du chapitre:

2.1. Introduction	10
2.2. Sûreté de fonctionnement des systèmes	11
2.2.1. Définition de la sûreté de fonctionnement	11
2.2.2. Composantes de la SdF	11
2.2.2.1. Fiabilité $R(t)$	11
2.2.2.2. Disponibilité $A(t)$	12
2.2.2.3. Maintenabilité $M(t)$	12
2.2.2.4. Sécurité	13
2.2.3. Métriques de la Sûreté de Fonctionnement	13
2.2.4. Défaillance	14
2.2.4.1. Taux de défaillance $\lambda(t)$	14
2.2.4.2. Taux de réparation $\mu(t)$	15
2.2.4.3. Le taux de défaillance à la sollicitation	15
2.2.5. Approche de la fiabilité par les probabilités.....	16
2.2.6. Autres Principales lois de probabilité	16
2.3. Notion de Système.....	17
2.3.1. Système et composant	17
2.3.2. Structure d'un système.....	18
2.3.3. Fonctionnement d'un système.....	18
2.3.4. Fiabilité d'un système	19
2.3.4.1. Système série	20
2.3.4.2. Système parallèle.....	20

2.3.4.3. La fiabilité tout au long du cycle de vie d'un système	20
2.3.4.5. Modélisation de la fiabilité des systèmes	21
2.3.4.6. Recueil de données / Bases de données de la fiabilité.....	21
2.4. Conclusion	22

2.1. Introduction

C'est depuis quelques décennies que la sûreté de fonctionnement [TOD 16], [BEL 16], [FIN 08] ou bien la fiabilité, disponibilité, maintenabilité et sécurité, est devenue un enjeu crucial dans le domaine de l'analyse quantitative des risques technologiques (AQRT). La sûreté de fonctionnement est apparue assez récemment par comparaison avec les autres domaines de l'ingénierie, à partir des années 1940 dans le domaine d'aéronautique, suivi par l'industrie de l'armement et le secteur nucléaire entre 1960 et 1970 suite à des défaillances dans les systèmes, des ingénieurs se sont intéressés à caractériser les défaillances d'un système en considérant la fiabilité observée du système et la fiabilité de ces composants. Les processus industriels sont en majorité constitués de plusieurs composants et leurs défaillances influencent sur la fiabilité du système, d'où on distingue des composants réparables à la suite d'une dégradation, ou d'une défaillance, ces composants peuvent être restaurés de façon à continuer à accomplir leur mission, grâce à des actions de maintenance qui n'entraînent pas forcément leurs remplacements. En revanche dans certains cas, et souvent pour des raisons économiques ou de facilité technique, il est plus rentable de remplacer le composant défaillant. Ce composant est alors considéré comme un composant non réparable [PRO 11].

Partant de ce concept, des modèles numériques, plusieurs approches probabilistes et diverses méthodes d'analyses ont été développés. Ils sont importants pour une étude approfondie qui a comme principale mission garantir un niveau élevé de service et de sécurité malgré le vieillissement l'usure, les dégradations inhérentes à tout système technique afin d'optimiser l'efficacité et la performance des systèmes.

La sûreté de fonctionnement par ces différentes interventions dans le domaine d'ingénierie et ainsi que son développement est comme étant une discipline à multi outils :

- ✓ Méthodes d'analyse des risques ;
- ✓ Méthodes de calculs prévisionnels de la sûreté de fonctionnement de systèmes ;
- ✓ Outils logiciels dédiés à la sûreté ;
- ✓ Constitution de bases de données statistiques sur la fiabilité des composants.

Après cette brève introduction sur le développement de la sûreté de fonctionnement, ce chapitre présente le cadre global de nos développements. Nous présenterons les différents concepts et définitions utiles dans la sûreté de fonctionnement, des systèmes, et les différentes bases associées comme la fiabilité, la disponibilité, la maintenabilité, le taux de défaillance et le taux de réparation. On détaillera les différents stades qui composent une étude de sûreté de fonctionnement des systèmes complexes dans le cadre de l'ingénierie système à savoir l'analyse de ses

dysfonctionnements et l'évaluation de ces performances en termes de fiabilité, de disponibilité et maintenabilité.

2.2. Sûreté de fonctionnement des systèmes

La complexité croissante des systèmes industriels, la réduction de leurs coûts de conception et d'exploitation ainsi que leurs importantes utilisations dans la vie font, de la sûreté de fonctionnement, un domaine incontournable dans le développement de tout système industriel.

2.2.1. Définition de la sûreté de fonctionnement

La sûreté de fonctionnement (SdF) [BOU 13], [DEM 09], [MAZ 08], [SAL 07], [MEG 04], [PRO 03] est une notion générale qui se caractérise comme la science des défaillances, l'analyse de risque [KHA 15], ou bien fiabilité, disponibilité, maintenabilité et sécurité. Elle englobe la connaissance des défaillances, leurs évaluations, leur prévision et leur maîtrise. Elle se caractérise à la fois par les études structurelles statiques et dynamiques des systèmes, du point de vue prévisionnel mais aussi opérationnel et expérimental, en tenant compte des aspects probabilistes et des conséquences induites par les défaillances techniques et humaines. Cette discipline intervient non seulement au niveau des systèmes déjà réalisés mais aussi au niveau conceptuel.

La Sûreté de Fonctionnement est basée sur :

- ✓ Des méthodes et des outils servant à caractériser et à maîtriser les effets des aléas, des pannes et des erreurs,
- ✓ La quantification des caractéristiques de composants et de systèmes pour exprimer la conformité dans le temps de leurs comportements et de leurs actions.

La Sûreté de Fonctionnement ne se réduit pas uniquement à une de ces performances de fiabilité, maintenabilité, disponibilité et sécurité, mais elle se construit à travers toutes ces caractéristiques.

2.2.2. Composantes de la SdF

Prévoir qu'un système tombe en panne fait appel à des critères probabilistes, obtenus à partir des paramètres fondamentaux de la sûreté de fonctionnement (fiabilité, disponibilité, maintenabilité et sécurité) [FEN 13], [DEM 09], [STA 09], [BIR 07], [SMI 01] afin de définir les objectifs attendu par un système et d'évaluer sa qualité de service attendu en vue de cibler les points critiques à améliorer.

2.2.2.1. Fiabilité $R(t)$

La fiabilité [TOD 16], [BEL 16], [PRO 11], [SAT 09], [FIN 06] d'une entité est la probabilité qu'elle accomplisse les fonctions requises dans des conditions données pendant une

durée entre 0 et t, sachant que l'entité n'est pas en panne à l'instant 0 et ne peut fonctionner éternellement, on peut considérer que :

- ✓ $R(t)$ est une fonction non croissante variant de 0 à 1 sur $[0, +\infty[$;
- ✓ $\lim_{t \rightarrow +\infty} R(t) = 0$.
- ✓ La défiabilité $F(t)$. Elle est le complément à 1 de la fiabilité, est définie comme étant : $F(t) = 1 - R(t)$.

La fiabilité est une fonction décroissante du temps (Figure 2.1), de telle manière que : $R(t_1) > R(t_2)$ si $t_1 < t_2$.

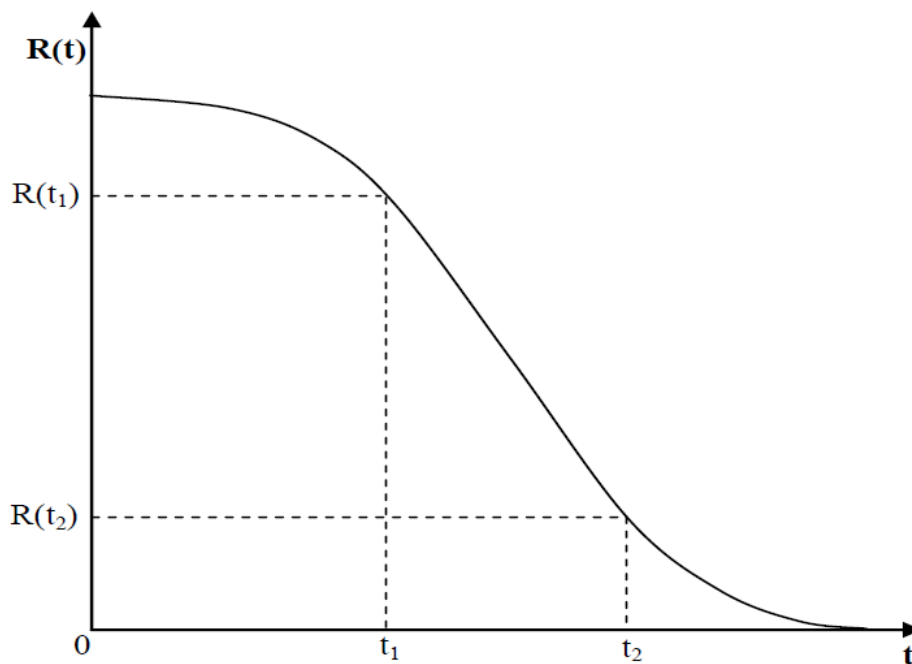


Figure 2.1 La fiabilité décroissante avec le temps

2.2.2.2. Disponibilité $A(t)$

La disponibilité [TAY 13], [SAT 09] d'une entité est la probabilité qu'elle accomplisse les fonctions requises dans des conditions données et à un instant donné. Dans le cas d'un composant non réparable, la disponibilité et la fiabilité se confondent : $A(t) \sim R(t)$ dans le cas contraire : $A(t) \geq R(t)$. L'indisponibilité $U(t)$ est le complément à 1 de la disponibilité, est définie comme étant : $U(t) = 1 - A(t)$.

2.2.2.3. Maintenabilité $M(t)$

La Maintenabilité [TOD 16], [PRO 11], [SAT 09] d'une entité est la probabilité qu'elle est réparée entre 0 et t.

- ✓ $M(t)$ est une fonction non décroissante variant de 0 à 1 sur $[0, +\infty[$;
- ✓ $\lim_{t \rightarrow +\infty} M(t) = 1$.

2.2.2.4. Sécurité

La sécurité est une aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des évènements critiques ou catastrophiques.

2.2.3. Métriques de la Sûreté de Fonctionnement

Les grandeurs [BEL 16], [TOD 16], [TAY 13], [USH 12], [PRO 11], [RAU 04], [SMI 04], [SMI 01] présentées ci-après caractérisent des durées moyennes associées à la sûreté de fonctionnement :

- ✓ MTTF : durée moyenne de fonctionnement avant la première défaillance (Mean Time To Failure).

$$MTTF = \int_0^{\infty} R(t)dt \quad (2.1)$$

- ✓ MTTR : durée moyenne de réparation (Mean Time To Repair).

$$MTTR = \int_0^{\infty} (1 - M(t))dt \quad (2.2)$$

- ✓ MUT : durée moyenne de fonctionnement après réparation (Mean Up Time).
- ✓ MDT : durée moyenne d'indisponibilité (Mean Dawn Time). Cette durée comptabilise le temps de détection de la panne, le temps de réparation et la remise en service.
- ✓ MTBF : durée moyenne entre deux défaillances consécutives d'une entité réparée. (Mean Time Between Failure).

$$MTBF = MDT + MUT \quad (2.3)$$

Ces grandeurs sont représentées sur le diagramme de la [Figure 2.2](#)

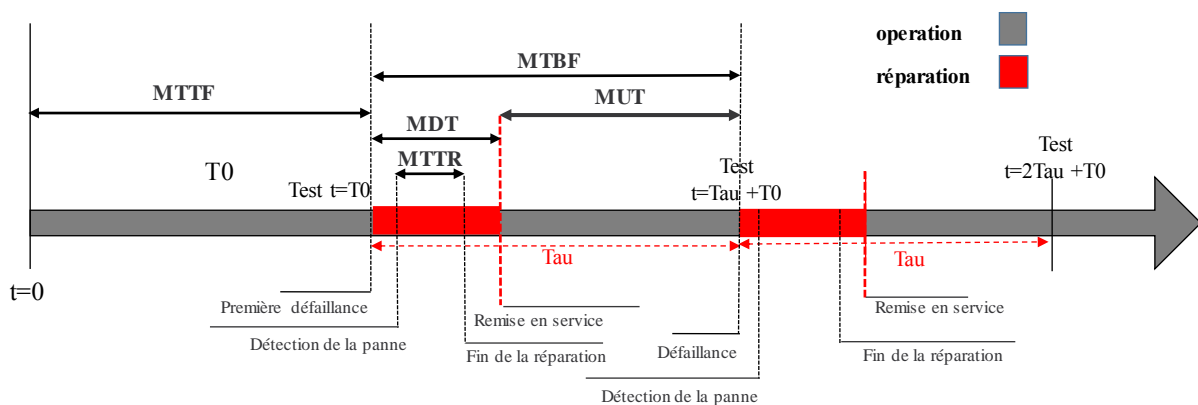


Figure 2.2 Métriques de la Sûreté de Fonctionnement

2.2.4. Défaillance

La défaillance est la cessation de l'aptitude d'une entité à accomplir une fonction requise, c'est le passage de l'état de fonctionnement à l'état de panne. Cette cessation peut être complète (l'entité ne remplit plus sa fonction) ou partielle (la fonction est assurée dans certaines limites, on parle alors de modes dégradés). Les défaillances peuvent être momentanées (indisponibilité du composant à remplir sa fonction pendant un temps donné, le composant redevient disponible sans réparation) ou permanentes (la défaillance du composant est irréversible, une maintenance est nécessaire pour remettre le composant en service).

On distinguera sa cause (circonstances ayant entraîné la défaillance), son mécanisme (processus ayant entraîné la défaillance) et son taux $\lambda(t)$ qui représente la proportion de dispositifs qui, ayant vécu un temps t , ne sont plus en vie à $t+dt$.

2.2.4.1. Taux de défaillance $\lambda(t)$

Généralement, la probabilité de défaillance [BEL 16], [PRO 11], [NAC 05] d'un composant dépend principalement de l'âge du composant. Cet âge est un taux horaire (homogène à l'inverse d'un temps) représentant la probabilité que le composant tombe en panne entre t et $t+dt$, sachant qu'il a fonctionné de 0 à t . Il est défini de la manière suivante (en appelant les probabilités P) :

$$\lambda(t) = \lim_{\Delta t \rightarrow 0} \frac{1}{\Delta t} \cdot P [\text{panne du composant entre } t \text{ et } t + \Delta t \text{ sachant qu'elle n'a pas eu lieu entre } 0 \text{ et } t]$$

En terme de probabilité conditionnelles, on a :

$$\lambda(t) = \lim_{\Delta t \rightarrow 0} \frac{1}{\Delta t} \cdot \frac{P [\text{panne du composant } t \text{ et } t + \Delta t \text{ et pas de panne du composant entre } 0 \text{ et } t]}{P[\text{pas de panne du composant entre } t \text{ et } t + \Delta t]}$$

$$\lambda(t) = \lim_{\Delta t \rightarrow 0} \frac{1}{\Delta t} \cdot \frac{P[\text{panne du composant entre } t \text{ et } t + \Delta t] - P[\text{panne du composant entre } 0 \text{ et } t]}{P[\text{pas de panne du composant entre } t \text{ et } t + \Delta t]}$$

Par l'introduction de la fiabilité $R(t)$ on obtien :

$$\lambda(t) = \lim_{\Delta t \rightarrow 0} \frac{1}{\Delta t} \cdot \frac{[(1 - R(t + \Delta t)) - (1 - R(t))]}{R(t)} \rightarrow \lambda(t) = \lim_{\Delta t \rightarrow 0} \frac{1}{\Delta t} \cdot \frac{[R(t + \Delta t) - R(t)]}{\Delta t \cdot R(t)}$$

$$\lambda(t) = -\frac{1}{R(t)} \cdot \frac{dR(t)}{dt} \quad (2.3)$$

La [Figure 2.3](#) représente l'évolution du taux de défaillance d'un composant au cours de son cycle de vie

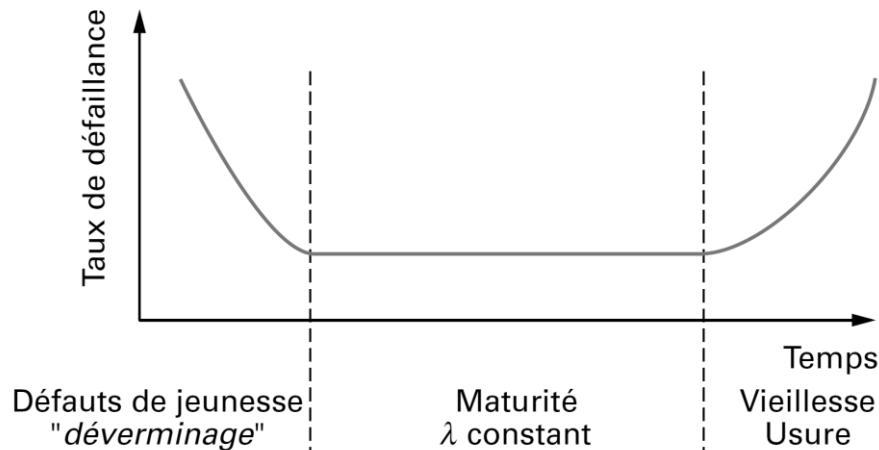


Figure 2.3 Évolution du taux de défaillance au cours du temps : courbe en baignoire

Le Taux de défaillance est ainsi élevé dans la période jeunesse liées à des erreurs de conception ou de fabrication, par la suite des défaillances aléatoires relativement constant dans la durée d'utilisation et à la fin une défaillance élevée dans sa période de vieillesse suite aux fatigues et l'usure.

2.2.4.2. Taux de réparation $\mu(t)$

La probabilité de réparation [BEL 16], [PRO 11], [NAC 05] d'un composant est principalement en fonction du temps écoulé depuis l'instant de défaillance. Il existe un certain délai avant que le composant puisse être réparé. Ce délai comprend le temps de détection et le temps mis pour qu'une équipe de réparation arrive sur place. Il s'y ajoute le temps de réparation proprement dit et la fin le temps de la remise en marche.

$$\mu(t) = \lim_{\Delta t \rightarrow 0} \frac{1}{\Delta t} \cdot P[\text{composant est réparé entre } t \text{ et } t + \Delta t \text{ sachant qu'il était en panne entre } 0 \text{ et } t]$$

Par l'introduction de la maintenabilité $M(t)$ on obtien de la meme manière que $\lambda(t)$:

$$\mu(t) = \frac{1}{1 - M(t)} \cdot \frac{dM(t)}{dt} \quad (2.4)$$

2.2.4.3. Le taux de défaillance à la sollicitation

La fonction d'un composant peut s'étendre sur une durée dite de fonctionnement. Dans ce cas, les défaillances du composant sont décrites par le taux de défaillance $\lambda(t)$. Mais la fonction à assurer peut-être « ponctuelle », comme un système de protection qui agit lorsqu'un événement dangereux se déroule. Dans ce cas, c'est un taux de défaillance à la sollicitation $\gamma(t)$ qui caractérise ce type de défaillance « ponctuelle ». Il est défini comme la probabilité que le composant tombe en panne lorsqu'il est sollicité. Ce taux peut s'exprimer sous la forme d'un taux de défaillance :

$$\lambda(t) = \gamma(t) \cdot P[\text{le composant est sollicité à } t]$$

2.2.5. Approche de la fiabilité par les probabilités

En général, les composants d'un système font l'objet d'une période de mise en service (pour éviter les défaillances de « jeunesse ») et de maintenance préventive (pour éliminer les défaillances d'usure). Ainsi, durant la période de fonctionnement du système, l'approximation des taux constants est souvent admise. En considérant le taux de défaillance $\lambda(t) = \lambda$ et le taux de réparation $\mu(t) = \mu$ constants alors on peut écrire, à partir des principes des section §2.2.2 et §2.2.3 ainsi que des équations 2.3 et 2.4 :

$$R(t) = e^{-\lambda \cdot t} \quad (2.5)$$

$$F(t) = 1 - e^{-\lambda \cdot t} \quad (2.6)$$

$$A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} \cdot e^{-(\lambda + \mu) \cdot t} \quad (2.7)$$

$$U(t) = \frac{\lambda}{\lambda + \mu} \cdot (1 - e^{-(\lambda + \mu) \cdot t}) \quad (2.8)$$

$$MTBF = \frac{1}{\lambda} \quad (2.9)$$

$$MDT = \frac{1}{\mu} \quad (2.10)$$

On calcule les valeurs asymptotiques de la disponibilité $A(\infty)$ et de l'indisponibilité $U(\infty)$:

$$A(\infty) = \frac{\mu}{\lambda + \mu} = \frac{MTBF}{MTBF + MDT} \text{ et } U(\infty) = \frac{\lambda}{\lambda + \mu} = \frac{MDT}{MTBF + MDT}$$

En considérant la définition des paramètres temporels, on remarque que la disponibilité asymptotique correspond à la proportion de temps pendant lequel l'entité est en état de fonctionner et que, de même, l'indisponibilité asymptotique correspond à la proportion du temps pendant lequel l'entité est en panne. Il est démontré que ce résultat est aussi valable lorsque les taux λ et μ ne sont pas constants.

Dans le cas où le temps moyen de réparation est négligeable par rapport au temps moyen de fonctionnement, on peut exprimer l'indisponibilité par : $U(\infty) = \frac{\lambda}{\mu}$

2.2.6. Autres Principales lois de probabilité

Parmi les lois de probabilité les plus utilisées en fiabilité et maintenabilité, les lois de probabilité discrète ou continue [BEL 16], [TOD 16], [DEM 09], [FIN 08], [BIR 07], [NAC 05], [RAU 04]. Voir tableau 1.

2.2.6.1. Les lois de probabilité discrètes

Sont utilisées, par exemple, lorsqu'il s'agit de quantifier la défaillance à la sollicitation, qui se produit lorsqu'une entité refuse de changer d'état lorsque cela lui est demandé.

2.2.6.2. Les lois de probabilité continues

Sont associées aux variables aléatoires continues, par exemple, lorsqu'il s'agit de quantifier la durée de bon fonctionnement d'une entité.

Tableau 2.1 Lois de probabilité.

Type de variable aléatoire	Nom de loi	Application
Discrète	Loi binomiale	Défaillance à la sollicitation
	Loi de Poisson	défaillance à la sollicitation, lorsque le nombre d'expériences est élevé et quand l'espérance mathématique de la variable aléatoire est constante
Continue	Loi de Weibull	Taux de défaillance décroissant, croissant ou constant
	Loi exponentielle	Taux de défaillance constant
	Loi normale	Incertitude liée à des mesures, fabrication
	Loi Log-Normale	Données de maintenabilité et défaillances dues à la fatigue

La description des lois de probabilité continues est présentée en [Annexe A.1](#).

2.3. Notion de Système

2.3.1. Système et composant

Un système est un ensemble d'éléments (composants, équipements) discrets qui interagissent entre eux [BOU 13], [SMI 10], [BIR 07], [NAC 05], [MEG 04], [RAU 04].

Formé d'éléments en interaction dynamique, un système correspond à une portion d'entité réelle, définie par une frontière établie en fonction d'un but, qui se distingue de son contexte ou de son milieu tout en procédant à des échanges avec son environnement.

Un système peut être défini aussi comme un ensemble de composants interdépendants, conçus pour réaliser une fonction donnée, dans des conditions données et dans un intervalle de temps donné. Pour chaque système, il importe de définir clairement les éléments qui le caractérisent, à savoir : la fonction, la structure, les conditions de fonctionnement, les conditions d'exploitation et l'environnement dans lequel il est appelé à opérer.

Un système peut être considéré de plusieurs façons :

- ✓ Depuis son environnement, comme élément spécifique de type « boîte noire » avec des entrées et des sorties qui permettent d'en étudier le fonctionnement,
- ✓ De l'intérieur, par la mise en évidence :
 - De ses caractéristiques physiques (par décomposition organique en sous-systèmes et composants),

- De ses modes d'organisation (relationnelles, hiérarchiques, ...),
- De ses propriétés (autonomie, robustesse, vulnérabilité, ...),
- De son comportement (dynamique d'évolution, productivité, ...).

Un système peut être complexe à cause de la nature des interactions entre les éléments qui le composent en faisant émerger de nouvelles propriétés qui ne figurent pas dans les éléments eux-mêmes. La distinction entre un système complexe et un système compliqué comme apparu dans la [Figure 2.4](#), c'est qu'il peut exister dans les deux cas un nombre élevé de composants par contre dans un système compliqué, les relations entre les composants sont simples, de type arborescence.

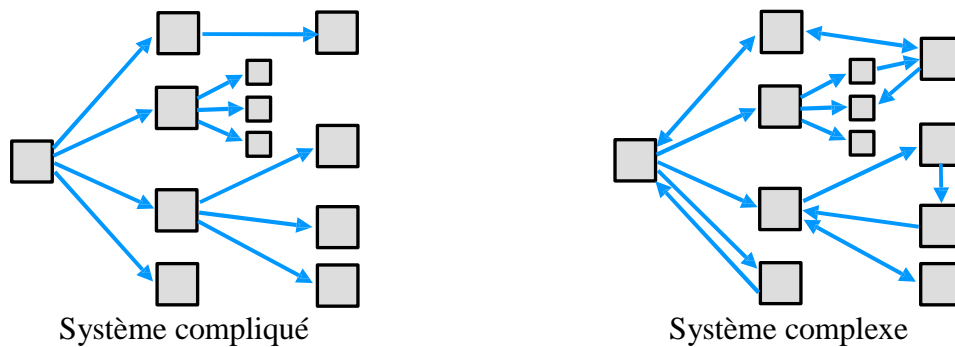


Figure 2.4 Différence entre système compliqué et système complexe

2.3.2. Structure d'un système

La structure d'un système peut être définie de trois manières :

- ✓ Fonctionnelle : résulte de la décomposition de ses fonctions opérationnelles en une hiérarchie de sous fonctions.
- ✓ Organique : consiste à définir le système par une décomposition itérative des différentes hiérarchies de ses constituants jusqu'aux composants physiques élémentaires.
- ✓ Organisationnelle : consiste à déterminer ses modes d'organisation en intégrant les aspects hiérarchiques et relationnels.

2.3.3. Fonctionnement d'un système

Tout système se caractérise par une ou plusieurs fonctions qu'il doit accomplir. Les éléments définissant le fonctionnement d'un système sont :

- ✓ Les fonctions à assurer par le système.
- ✓ L'architecture du système, qui comprend les divers composants mis en jeu et leurs connexions.
- ✓ Le système d'exploitation, qui représente les comportements du système durant son fonctionnement. Cela comprend les diverses actions en réponse aux

événements : cela va de la sollicitation d'un dispositif de sécurité (système d'alarme, mesures de sécurité) aux changements de configurations du système (modes de secours) en passant par les maintenances de certains composants.

2.3.4. Fiabilité d'un système

Généralement les industriels s'intéressent à la fiabilité de systèmes complexes formés de plusieurs composants élémentaires (joints, roulement, arbres, soupape garniture d'étanchéité mécanique, ...) [TOD 16], [USH 12], [SMI 10], [BIR 07], [NAC 05]. L'étude d'un système passe par sa décomposition en composants élémentaire. On étudie ensuite la fiabilité de chaque composant élémentaire et on déduit la fiabilité du système. La détermination de la fiabilité d'un système nécessite de connaître la loi de la fiabilité (ou la loi de défaillance) de chacun des composants intervenant dans le système.

Un système complexe peut former différentes configurations en matière d'analyse de la fiabilité. Plus la complexité du système augmente, plus la fiabilité de celui-ci diminue, à moins que des mesures compensatoires soient prises (la redondance). Une modélisation fonctionnelle sous forme de schéma bloc de ces systèmes permet d'en déterminer la fiabilité. Chaque bloc représente un composant ou mode de défaillance. Les configurations les plus couramment rencontrées sont les associations série, parallèle, série parallèle. D'autres types de configurations sont envisageables, notamment pour modéliser une redondance ou un élément de secours (redondances actives m parmi n et les redondances passives).

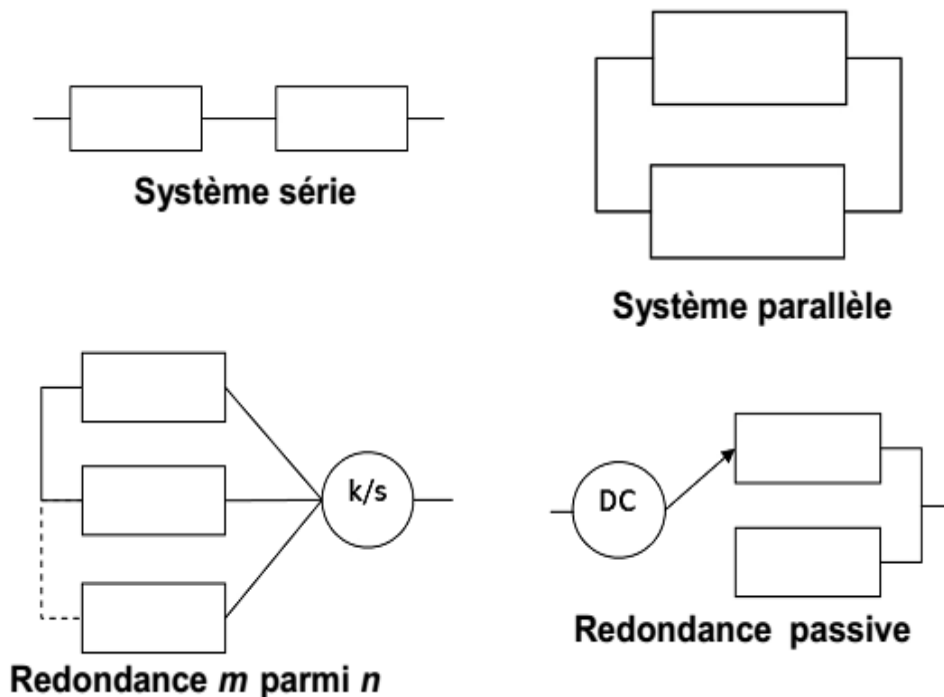


Figure 2.5 les différentes configurations de système.

2.3.4.1. Système série

Dans ce cas, chaque composant est indispensable au fonctionnement du système, la défaillance de n'importe lequel entraîne la défaillance de tout le système. La fiabilité du système est exprimée de la manière suivante :

$$R(t)_{\text{système}} = \prod_{i=1}^n R(t)_{\text{composant } i} \quad (2.11)$$

On démontre aisément à partir de la formule précédente l'expression du taux de défaillance instantanée du système en fonction de ceux des composants :

$$\lambda(t)_{\text{système}} = \sum_{i=1}^n \lambda(t)_{\text{composant } i} \quad (2.12)$$

2.3.4.2. Système parallèle

Dans ce cas, le système compte i composants, la défaillance du système n'a lieu que si tous les composants sont défaillants. Le système présente alors une ou plusieurs redondances.

La fonction cumulée de défaillance du système s'exprime alors en fonction de défaillance des composants :

$$F(t)_{\text{système}} = \prod_{i=1}^n F(t)_{\text{composant } i} \quad (2.13)$$

On en déduit la fiabilité du système :

$$R(t)_{\text{système}} = 1 - \prod_{i=1}^n (1 - R(t)_{\text{composant } i}) \quad (2.14)$$

2.3.4.3. La fiabilité tout au long du cycle de vie d'un système

De nombreux industriels travaillent à l'évaluation et l'amélioration de la fiabilité de leurs systèmes au cours de leur cycle de développement, afin de développer leurs connaissances sur le rapport Coût/Fiabilité et maîtriser les sources de défaillance. La dégradation de la fiabilité d'un système est directement liée aux mécanismes de dégradation du système et/ou de ses composants. La fiabilisation d'un système fait appel à divers méthodes et outils pour évaluer ces différents éléments de la fiabilité.

- ✓ La fiabilité prévisionnelle
- ✓ La fiabilité expérimentale
- ✓ La fiabilité opérationnelle

Ces méthodes et outils d'évaluation sont présents pour chaque phase :

- ✓ **Évaluation prévisionnelle de la fiabilité** : cette phase consiste dès le début du projet à étudier la fiabilité à travers des analyses qualitatives (APR, HAZOP, AMDE, ...) et quantitatives (Arbre de défaillance, Arbre d'évènement, ...), en intégrant les différents recueils de données. Pour des systèmes complexes, il est possible de modéliser la fiabilité par des Simulations de Monté Carlo, réseaux de Petri ou chaînes de Markov. La fiabilité prévisionnelle permet de prendre des orientations optimales en matière de conception.
- ✓ **Évaluation expérimentale de la fiabilité** : cette phase intervient dès que le développement du produit est suffisamment avancé et que l'on dispose des premiers prototypes, il est possible de réaliser des essais de robustesse (appelés également essais aggravés) afin de connaître les faiblesses et les marges de conception. Une fois que le produit est mature (marges suffisantes), une campagne d'essais peut être menée pour estimer la fiabilité. Lors de la production, l'élimination des défauts de jeunesse (dérive process, composant faible, ...) est opérée par des essais de déverminage.
- ✓ **Évaluation opérationnelle de la fiabilité** : une fois que le produit est en exploitation, une estimation de la fiabilité est réalisée à partir des données de REX. Elle se pratique dès les premières mises en service et permet ainsi de corriger des défauts de conception et de fabrication/réalisation.

2.3.4.5. Modélisation de la fiabilité des systèmes

L'industrie s'intéresse particulièrement à la fiabilité, pour assurer le bon fonctionnement de ses systèmes et gérer au mieux leurs maintenances. La détermination de la fiabilité d'un système mécanique ou électronique nécessite tout d'abord de connaître la loi de la fiabilité (ou loi de défaillance) de chacun des composants. Pour les systèmes mécaniques, étant généralement complexes, la fiabilité du système repose sur la fiabilité de quelques composants élémentaires responsables de son dysfonctionnement obtenu par le résultats d'une étude qualitative (AMDE), dit composants "responsables" ou "critiques" (parfois un seul), contribuant presque totalement à la probabilité de défaillance de l'ensemble.

2.3.4.6. Recueil de données / Bases de données de la fiabilité

Au fil du temps plusieurs bases de données sont élaborées suite à des résultats d'exploitation, des résultats d'essais en laboratoire et au retour d'expérience. La possession ou l'accès aux données de fiabilité ou de maintenabilité sont une ressource extrêmement précieuse pour évaluer des risques. Ces données peuvent être propres au système ou bien communes à d'autre système.

Le processus de dégradation des équipements (modes, mécanismes et causes de défaillance), les conditions d'utilisation et l'évolution des technologies sont des paramètres nécessaires pour le calcul des taux de défaillance et l'élaboration des modèles prévisionnels de la fiabilité, or il est difficile de les prendre tous en considération. Les données sont souvent inappropriées aux systèmes et environnements réels. Par conséquent, aucune de ces sources ne fournit des données parfaites pour une évaluation plus précise de la fiabilité, les informations recueillies ne permettent qu'une exploitation partielle des données, cependant elles restent toujours utiles pour de nouvelles conceptions afin d'obtenir des valeurs rapprochées. D'ailleurs, La base de données OREDA [SIN 02] est l'une des bases utilisée pour le développement de notre analyse. Plusieurs bases de données de différents domaines sont présentées en **Annexe A.2**.

2.4. Conclusion

Ce chapitre a fait l'œuvre d'une revue de littérature sur l'analyse par sûreté de fonctionnement, une discipline de plus en plus utilisée dans les systèmes industriels pour des questions de contrôle de sécurité, d'amélioration de la disponibilité et de garantie de la fiabilité en tenant en considération la notion du coût. Ces dernières années la sûreté de fonctionnement s'est dotée de multiples méthodes qui permettent le diagnostic et le contrôle de la fiabilité, disponibilité, maintenabilité et sécurité des systèmes. Mais avant de présenter quelques méthodes jugées utiles pour notre travail parmi ces différentes méthodes. Il a été nécessaire de passer par ce chapitre où nous avons présenté les notions de base de la sûreté de fonctionnement à savoir; les concepts de la fiabilité, disponibilité, maintenabilité et sécurité. Par la suite, une métrique de sûreté de fonctionnement a été abordée, elle représente les différentes phases par lesquelles un composant passe, ainsi que le taux de défaillance et de réparation et l'approche de la fiabilité par les probabilités. A la fin une large partie a été consacrée aux notions du système en passant par sa structure, son fonctionnement, ça fiabilité et les données de fiabilité.

Chapitre III

Démarches et Méthodes d'analyse quantitative des risques

Sommaire du chapitre:

3.1. Introduction	25
3.2. Analyse structurelle et fonctionnelle du système	26
3.2.1. Analyse fonctionnelle du système.....	26
3.3. Description des méthodes d'analyse prévisionnelle des risques	27
3.3.1. Qualitative / quantitative	27
3.3.1.1. Méthodes qualitatives	27
3.3.1.2. Méthodes quantitatives	27
3.3.2. Inductive / déductive	27
3.3.2.1. Méthodes inductives	27
3.3.2.2. Méthodes déductives	27
3.3.3. Statiques/dynamiques.....	28
3.3.3.1. Méthodes statiques	28
3.3.3.2. Méthodes dynamiques	28
3.4. Analyse et évaluation dysfonctionnelles	29
3.4.1. AMDE / AMDEC	30
3.4.1.1. AMDE (Analyse des modes de défaillances, de leurs effets).....	30
3.4.1.2. AMDEC L'analyse des modes de défaillances, de leurs effets et de leur criticité.....	31
3.4.2. Arbre de défaillance	33
3.4.2.1. Analyse qualitative	34
3.4.2.2. Analyse quantitative	34
3.4.2.3. Facteurs d'importance probabilistes	35
3.4.3. Arbre d'évènement.....	37

3.4.4. Simulation de Monte Carlo	38
3.4.5. Réseaux bayésiens.....	40
3.4.6. Réseau de Petri stochastique	40
3.4.6.1. RdP stochastiques classique	42
3.4.6.2. RdP stochastiques généralisés	42
3.4.6.3. RdP stochastiques déterministes :	42
3.4.7. Graphes de Markov	43
3.5. Limitation des méthodes d'analyse quantitatives des risques	44
3.6. Critères de choix d'une méthode d'analyse de risque	46
3.7. Conclusion	47

3.1. Introduction

La Sûreté de Fonctionnement est une discipline qui s'appuie sur un support méthodologique applicable aux systèmes technologiques tout au long de leur cycle de vie:

- ✓ Expression du besoin, conception, industrialisation, production, utilisation,
- ✓ Diffusion, maintenance, voire même retrait de service.

Ces démarches bénéficient du support de méthodologies rigoureuses et d'outils pratiques et puissants. Les méthodes de la sûreté de fonctionnement ont toutes au moins trois points communs, qui peuvent être résumés en trois types d'action :

- ✓ Identifier les processus pouvant affecter la fiabilité, la disponibilité, la maintenabilité ou la sécurité,
- ✓ Modéliser ces différents processus afin de faciliter la compréhension des mécanismes mis en jeu,
- ✓ Valoriser les résultats des analyses en utilisant les modèles obtenus pour apprécier le niveau de sûreté de fonctionnement du système étudié, en relever les éventuelles insuffisances par rapport aux objectifs de performances poursuivis, en hiérarchiser les points forts et les points faibles.

Les connaissances requises pour une telle analyse de la sûreté de fonctionnement sont multiples :

- ✓ Une bonne connaissance technique du système.
- ✓ Un retour d'expérience sur l'exploitation et les éventuelles défaillances observées du système ou d'un système similaire.
- ✓ Une bonne expérience des méthodes d'analyse de sûreté qui requièrent de l'intuition et du bon sens de la part de l'analyste.

On peut diviser une analyse de sûreté de fonctionnement de système en plusieurs étapes principales à savoir :

- ✓ L'analyse structurelle et fonctionnelle du système ;
- ✓ L'analyse qualitative du système ;
- ✓ L'analyse quantitative du système ;
- ✓ La synthèse des analyses précédentes et une conclusion.

L'organigramme de la [Figure 3.1](#) Présente l'enchaînement entre ces différentes étapes. Il faut remarquer que ces étapes ne sont pas totalement disjointes et présentent des aspects communs. De plus, une étude réelle est itérative, les étapes principales sont répétées plusieurs fois jusqu'à l'obtention d'une conclusion acceptable (objectifs réalisés).

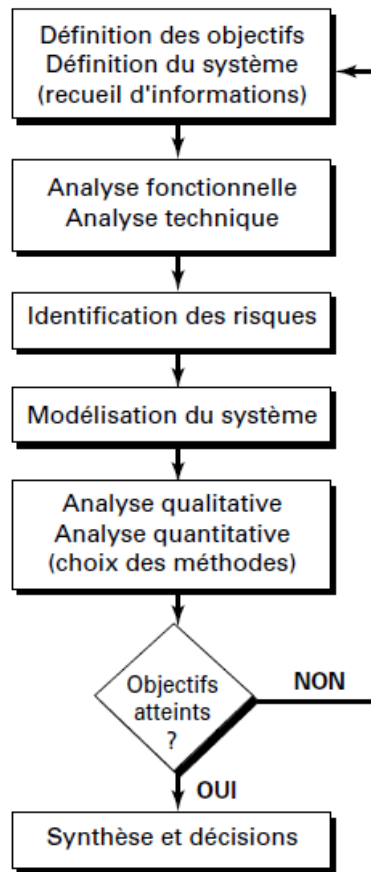


Figure 3.1 Organigramme des tâches d'une analyse prévisionnelle

Ce chapitre présente les démarches et méthodes les plus utilisées dans l'étude de sûreté de fonctionnement des systèmes.

3.2. Analyse structurelle et fonctionnelle du système

3.2.1. Analyse fonctionnelle du système

L'analyse fonctionnelle a pour but de caractériser le fonctionnement du système. On identifie ainsi les composants du système, leur rôle ainsi que les contraintes de fonctionnement. Les différentes configurations que peut prendre le système sont répertoriées (modes fonctionnement normaux, mode de secours, mode spécifique pour la maintenance préventive,). Les fonctions que le système se doit d'assurer sont explicitées afin de définir les événements redoutés qui font l'objet de l'étude de sûreté.

Les méthodes d'analyse fonctionnelle permettent :

- ✓ De décrire le besoin d'un utilisateur en termes de fonctions, en faisant abstraction des solutions pouvant les réaliser. A chaque fonction sont attribués des critères d'appréciation et leurs niveaux. Les niveaux des critères d'appréciation sont les caractéristiques quantitatives de chaque fonction du produit. Pour chaque critère

d'appréciation, on peut définir une flexibilité, c'est-à-dire un ensemble d'indications exprimées par le demandeur sur les possibilités de moduler un niveau recherché ;

- ✓ De décrire les choix technologiques que l'on impose au concepteur, en termes de contraintes. Les contraintes peuvent venir de l'environnement, de la technologie, du marché, de la situation et des choix de l'entreprise ou de l'organisme ;
- ✓ De s'assurer, pour chaque fonction, de sa bonne expression en termes d'objectifs et de sa stabilité dans le temps. C'est le but du contrôle de validité ;
- ✓ De décrire le produit envisagé comme solution, en termes de fonctions de service et en termes de fonctions techniques ou de conception ;
- ✓ D'initialiser l'optimisation du produit aussi bien du point de vue coût que du point de vue fiabilité.

3.3. Description des méthodes d'analyse prévisionnelle des risques

Les méthodes d'analyse prévisionnelle [BOU 13], [TAY 13], [SIM 01] se répartissent par ces 3 étapes couramment rencontrés qui se différencient par les techniques de raisonnement :

3.3.1. Qualitative / quantitative

3.3.1.1. Méthodes qualitatives

Les résultats renseignent sur les caractéristiques du système : points faibles du système, fausses redondances, influence d'un élément donné sur la fiabilité du système, repérage des chemins critiques, test (pour les chemins critiques) des méthodes d'élimination, ...

3.3.1.2. Méthodes quantitatives

Les résultats sont ceux de calcul de fiabilité, disponibilité, ... par exemple, la probabilité d'occurrence d'une combinaison d'événements.

3.3.2. Inductive / déductive

3.3.2.1. Méthodes inductives

Basées sur une démarche descendante, elles considèrent un événement initiateur (défaillance technique, dysfonctionnement organisationnel, ...) dont elles cherchent à caractériser les conséquences sur le système et son environnement. Ces approches partent donc des causes pour en déduire les conséquences.

3.3.2.2. Méthodes déductives

Basées sur une démarche ascendante, elles considèrent un événement redouté (arrêt du système, anomalie de fonctionnement, ...) dont elles cherchent à expliquer les causes, le plus souvent sous forme de séquences d'événements.

3.3.3. Statiques/dynamiques

3.3.3.1. Méthodes statiques

Elles permettent d'analyser le système d'un point de vue structurel sans tenir compte des évolutions au cours du temps et s'appuient sur un modèle mathématique booléen du système qui fournit, par exemple, les combinaisons de défaillances entraînant le dysfonctionnement du système mais sans représenter les interrelations temporelles qui l'affectent.

3.3.3.2. Méthodes dynamiques

Les méthodes dynamiques permettent la prise en compte des aspects comportemental et temporel.

La mise en œuvre de ces méthodes rend indispensables des décompositions hiérarchiques matérielles ou fonctionnelles du système.

Le [Tableau 3.1](#) Quelques démarches ou méthodes utilisées

Tableau 3.1 Principales méthodes et démarche de la fiabilité

Méthode	Inductive/ déductive	Qualitative/ quantitative	Statique/ dynamique	Objectifs visés
Analyse des Modes de Défaillance de leurs Effets et de leurs Criticité (AMDEC)	Inductive	Qualitative	Statique	Identifier les effets des modes de défaillance des composants sur le fonctionnement du système.
Arbre de Défaillance (AdD)	Déductive	Qualitative Quantitative	Statique	Représenter de façon synthétique l'ensemble des combinaisons d'événements qui peuvent engendrer un événement redouté.
Arbre d'Événement (AdE)	Inductive	Qualitative Quantitative	Statique	Représenter sous forme de scénarios les conséquences potentielles d'un événement initiateur, d'une défaillance.
Réseau de Pétri	Inductive	Qualitative Quantitative	Dynamique	Repérer le passage par les états de défaillance sur le fonctionnement du système.
Chaînes de Markov	Inductive	Qualitative Quantitative	Dynamique	Repérer le passage par les états de défaillance sur le fonctionnement du système.

Réseaux Bayésien dynamique	Inductive	Qualitative Quantitative	Dynamique	Identification de l'évolution du système dans les états bon fonctionnement, dégradé, panne
----------------------------	-----------	-----------------------------	-----------	--

Les données d'entrée de ces méthodes sont de deux ordres :

- ✓ Connaissance du système résultant généralement d'une étude fonctionnelle,
- ✓ Données de nature événementielle, sous forme brute : états, historiques, ... ou sous forme de modèle statistique : lois mathématiques décrivant les fonctions de distribution des événements.

Les résultats établis en sortie sont :

- ✓ Des modèles de comportement du système (vis-à-vis des défaillances, réparations, sollicitations, service, ...) :
 - Modèles de sûreté de fonctionnement,
 - Modèles mixtes sûreté de fonctionnement/performance, ...,
- ✓ Des grandeurs établies à partir des modèles et pouvant revêtir différentes formes:
 - Probabilités d'états ou d'occurrence d'événements,
 - Quantificateurs FMDS, etc.
 - Métriques évoluées de performance et de coût,
- ✓ Des éléments de stratégies d'actions ou d'aide à la décision:
 - De maintenance : contrôle, fréquence d'entretien, ...,
 - De gestion de risques : protection, évitement, ...

3.4. Analyse et évaluation dysfonctionnelles

Identification et hiérarchisation des risques, bien entendu, les risques à prendre en compte sont directement liés aux enjeux de l'étude considérée. Cependant, lorsque le système étudié présente un comportement complexe, il est indispensable d'aller plus loin et de procéder à une modélisation servant de support à des analyses qui, selon le cas, pourront être purement qualitatives, semi quantitatives ou purement quantitatives.

Les résultats théoriques sont confrontés aux connaissances pratiques des spécialistes du terrain afin de mettre en évidence les éléments qui pourraient les choquer et procéder aux rectifications nécessaires. Cette étape peut être le point de départ d'une nouvelle itération si elle conduit à la remise en cause de la conception du système en cours d'analyse.

Les méthodes utilisées pour l'analyse dysfonctionnelle se présentent sous des aspects divers : formes tabulaires, arborescence, réseaux, graphes, ...

3.4.1. AMDE / AMDEC

3.4.1.1. AMDE (Analyse des modes de défaillances, de leurs effets)

Cette méthode [failure mode and effect analysis (FMEA) en anglais], développée au début des années 60 en aéronautique [TAY 13], [BOU 13], [SMI 01], [VIN 99] a été depuis, généralisée à de nombreux domaines de l'industrie. Elle est inductive et permet l'étude systématique des causes et des effets des défaillances (modes de défaillance et effets) qui affectent les composants d'un système. La méthode comprend quatre étapes et se caractérise par une présentation sous forme de tableaux qui sont très souvent spécifiques à un secteur industriel concerné.

- ✓ **Définition du système, de ses fonctions et de ses composants** : définition des principales fonctions du système, de ses limites fonctionnelles (systèmes et composants) et des spécifications relatives au fonctionnement du système, de ses composants ou à l'environnement du système.
- ✓ **Établissement des modes de défaillance des composants et leurs causes** : cette phase doit être la plus complète possible et demeure le point faible de la méthode. On classe les modes de défaillances en général en quatre catégories (normalisées) :
 - Fonctionnement prématuré (ou intempestif) ;
 - Ne fonctionne pas au moment prévu ;
 - Ne s'arrête pas au moment prévu ;
 - Défaillance en fonctionnement.
- ✓ **Étude des effets des modes de défaillance** : étude complète des effets sur les fonctions des systèmes et sur chacun des composants, en supposant un seul mode de défaillance (les autres composants étant tous en état de fonctionner). Il faut tenir compte des variations des paramètres importants et étudier leurs effets (modèles de phénomènes physiques parfois nécessaires) en sachant distinguer ceux qui concernent le système lui-même et ceux qui concernent son environnement (suivant les objectifs, les uns ou les autres peuvent être prioritaires). Cette phase permet également d'identifier les défaillances secondaires.
- ✓ **Conclusions, recommandations** : à partir des étapes précédentes, on peut conclure et établir des recommandations, compte tenu des objectifs de l'étude. Les

recommandations permettent d'émettre des propositions : ajout de redondances, de procédures de détection et de maintenance pour chaque mode de défaillance.

Les modes de défaillances sont définis par rapport à un fonctionnement précis du système et sont donc dépendants de celui-ci. Pour aider l'analyste, on utilise des tableaux en Annexe B donnant une liste-guide de modes génériques de défaillance. Ainsi qu'un tableau d'AMDE.

3.4.1.2. AMDEC (L'analyse des modes de défaillances, de leurs effets et de leur criticité)

Cette méthode AMDEC est une extension de la méthode AMDE (failure mode, effects and criticality analysis – FMECA en anglais) [BOU 13], [SMI 01], [PRO 11], [RAU 04], [SPO 99]. Est une méthode ascendante qui, considère la probabilité d'occurrence de chaque mode de défaillance et la gravité des effets associés pour effectuer une classification suivant une échelle en criticité, ou elle permet d'évaluer les effets de chaque mode de défaillance des composants du système sur les différentes fonctions de celui-ci et d'identifier ceux influant les caractéristiques FMDS (Fiabilité, Maintenabilité, Disponibilité, Sécurité) du système.

L'AMDE est établie à partir des définitions suivantes qui sont mises en évidence pour chaque mode de défaillance :

- ✓ Une défaillance est la cessation de l'aptitude d'un élément ou d'un système à accomplir une fonction requise,
- ✓ Un mode de défaillance est l'effet par lequel une défaillance est observée sur un élément du système,
- ✓ Une cause de défaillance est constituée par les événements qui conduisent aux défaillances,
- ✓ L'effet d'un mode de défaillance regroupe les conséquences associées à la perte de l'aptitude d'un élément à remplir une fonction requise,
- ✓ Les moyens de détection représentent les actions permettant de détecter la défaillance (les tests périodiques, les inspections, les alarmes, etc.).

Pour évaluer la criticité d'une défaillance, l'AMDEC apparaît comme une suite logique à l'AMDE. La criticité évalue pour chaque mode de défaillance :

- ✓ La probabilité d'occurrence,
- ✓ La gravité : associe pour chaque mode de défaillance, une classe des effets (mineurs, significatifs, critiques ou catastrophiques etc.),
- ✓ Le risque de la non-détection : qui est d'autant plus important qu'aucune barrière matérielle ou logicielle n'est prévue pour éviter la défaillance, La criticité d'une défaillance est égale au produit de la probabilité d'occurrence, de la gravité et du

risque de non-détection. L'AMDEC reprend en effet les principales étapes de l'AMDE et ajoute une évaluation quantitative de la criticité.

La démarche générale de l'AMDEC se résume de l'organigramme en [Figure 3.2](#), plus de détails sur l'analyse par AMDEC sont présentés en [Annexe B.1](#).

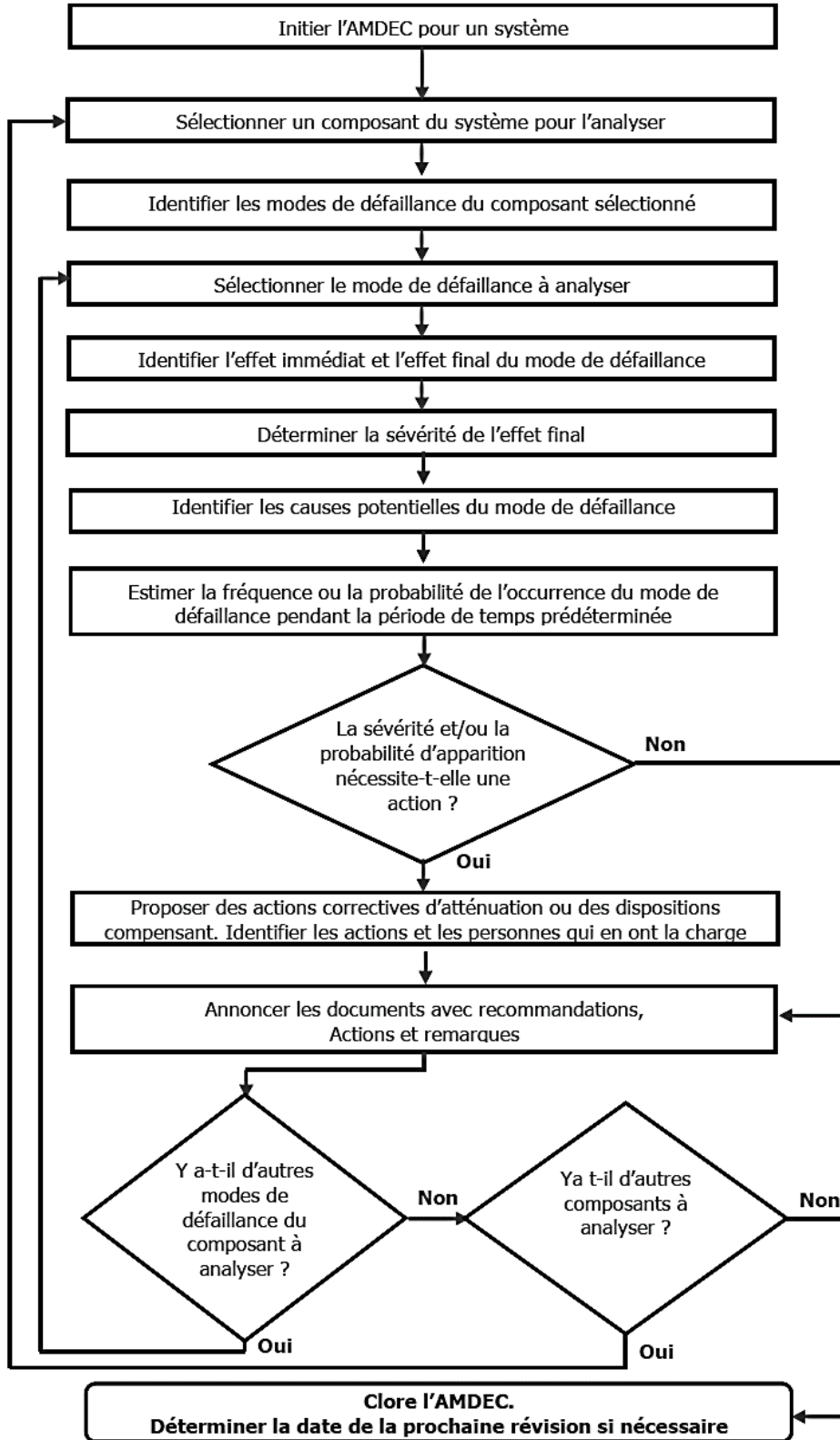


Figure 3.2 Organigramme de la méthode AMDE

3.4.2. Arbre de défaillance

L'ADD ou en anglais (Fault tree Analysis FTA) est l'une des techniques connues par leurs utilisations dans l'analyse de la sécurité et de la fiabilité des processus [GUE 18], [AIS 15], [DEN 15], [BOU 13], [CHA 13], [MEC 11], [DEM 09]. Appelée aussi l'arbre des causes ou l'arbre des fautes a été élaboré au début des années 1960 par la compagnie « Bell téléphone ». Cette méthode déductive permet de combiner les composants par identification des causes relatives aux événements redoutés et des fonctions d'un système.

La méthode consiste en une représentation graphique des multiples causes d'un événement redouté.

Elle permet de visualiser les relations entre les défaillances d'équipement, les erreurs humaines et les facteurs environnementaux qui peuvent conduire à des accidents. On peut donc éventuellement y inclure des facteurs reliés aux aspects organisationnels.

L'analyse par Arbre de Défaillances se déroule généralement en 3 étapes :

- ✓ Spécification du système et de ses frontières.
- ✓ Spécification des événements redoutés préalablement identifiés par exemple par AMDE.
- ✓ Construction des arbres de défaillances : On cible les événements redoutés un par un et on essaye d'identifier les successions et les combinaisons d'événements de base permettant de les atteindre.

Toutefois, un événement de base doit répondre à un certain nombre de critères, en l'occurrence :

- ✓ Il doit être indépendant des autres événements de base.
- ✓ Il ne doit pas être décomposable en éléments plus simples.
- ✓ Il doit avoir une fréquence évaluable.

A partir de l'évènement sommet, on construit en utilisant le symbolisme de logique booléenne, une arborescence (schéma graphique en forme d'arbre inversé) représentant l'enchaînement logique des évènements intermédiaires jusqu'à la mise en cause des évènements élémentaires (défaillance d'un composant). Il est ainsi possible d'identifier toutes les défaillances élémentaires pouvant conduire à l'évènement redouté.

L'analyse par un arbre des défaillances est fondée sur les principes suivants :

- ✓ Un évènement est une combinaison d'évènements de base non décomposables,
- ✓ Les évènements de base sont indépendants,
- ✓ La probabilité d'occurrence des évènements de base peut être évaluée.

Les liens entre les différents évènements sont réalisés grâce à des opérateurs logiques, (et, ou, k -sur- n ...). Cette méthode utilise une représentation graphique qui permet de présenter les résultats dans une structure arborescente développée généralement et surtout pour les structures compliquées par un algorithme du diagramme de décision binaire.

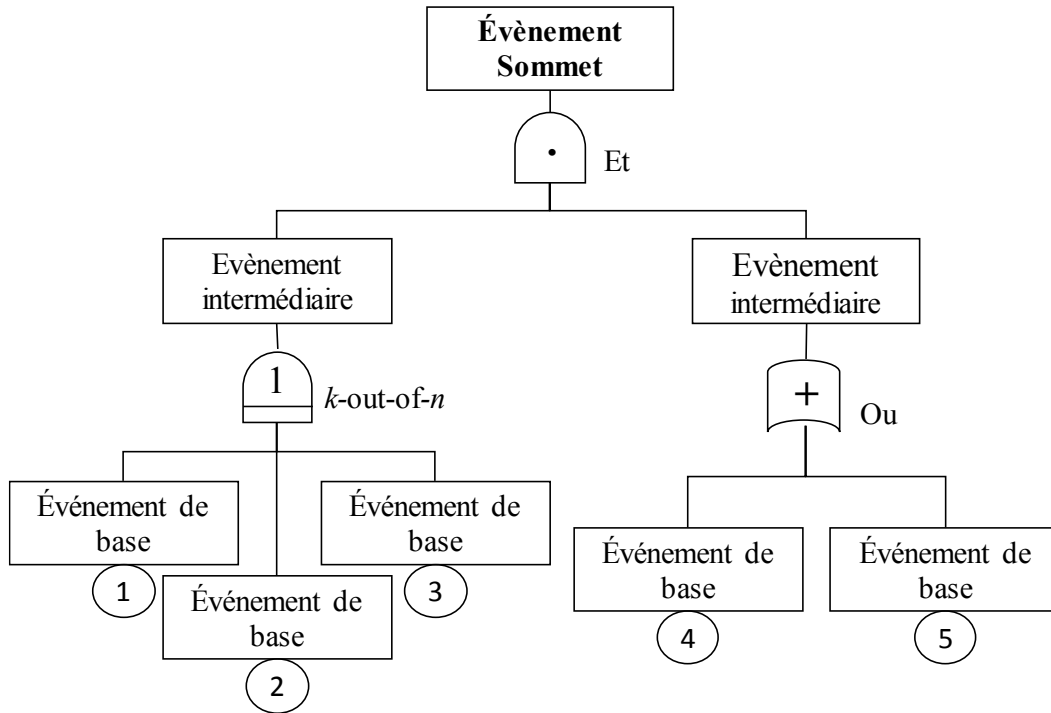


Figure 3.3 Exemple d'une structure d'arbre de défaillance

L'analyse par Arbre de défaillance est résumée par :

3.4.2.1. Analyse qualitative

Cette analyse permet de déterminer les faiblesses du système. Elle est faite dans le but de proposer des modifications afin d'améliorer la fiabilité du système. La recherche des éléments les plus critiques est faite en déterminant les chemins qui conduisent à un évènement sommet par les coupes minimales [CHA13], (ensemble d'évènements de base et de conditions suffisant pour produire l'évènement-sommet). Ces chemins critiques représentent des scénarios qui sont analysés en fonction des différentes modifications qu'il est possible d'apporter au système.

Plus de détails sur l'analyse par AdD sont présentés en [Annexe B.2](#).

3.4.2.2. Analyse quantitative

Après l'étude FDMS des évènements de base il est possible à partir de leurs valeurs numériques, et par l'utilisation des équations logiques tirées de la structure de l'arbre et d'évaluer la probabilité de l'évènement sommet [USH 12], [MER 10], [BIR 07].

Pour un système de distribution d'entrée X_1, X_2, \dots, X_n le [Tableau 3.2](#) résume les équations de probabilité des portes logiques

Tableau 3.2 Probabilités de défaillance propagées à l'aide d'équations de logique booléien

Portes	Équations de probabilité
Et	$P[and(X_1, \dots, X_n) = 1] = P[X_1 = 1 \wedge \dots \wedge X_n = 1] = P[X_1 = 1] \times \dots \times P[X_n = 1]$
Ou	$P[or(X_1, \dots, X_n) = 1] = 1 - P[or(X_1, \dots, X_n) = 0] = 1 - P[X_1 = 0 \wedge \dots \wedge X_n = 0] = 1 - (1 - P[X_1 = 1]) \times \dots \times (1 - P[X_n = 1])$
k-sur-n	$P[koon(X_1, \dots, X_n) = 1] = P[(X_1 = 1 \wedge \dots \wedge X_k = 1) \vee (X_1 = 1 \wedge \dots \wedge X_{k-1} = 1 \wedge X_{k+1} = 1) \vee \dots \vee (X_{n-k} = 1 \wedge \dots \wedge X_n = 1)]$
P [X = 1] indique la probabilité que X soit en état de fonctionnement et P [X = 0] indique la probabilité que X soit en état de défaillance, à condition que, en k-sur-n, k soit l'entrée minimale en état de fonctionnement (k-out-of-n: G).	

3.4.2.3. Facteurs d'importance probabilistes (FIP)

Les facteurs d'importance sont des indicateurs calculés pour chaque événement de base d'un arbre de défaillance [GUE 18], [AIS 17], [AIS 15], [KUO 12], [VAU 11], [VAU 10], [RAU 04]. Ces indicateurs visent à évaluer les contributions relatives des différents composants du système au risque global.

- ✓ **Facteur d'importance Marginale de Birnbaum (FIM):** Le facteur d'importance probabiliste Marginale est le 1^{er} facteur d'importance proposé par Z.W. Birnbaum en 1968, ce facteur dépend de la structure de l'arbre de défaillance et de la fiabilité des autres composants. Pour un système 'S' de n composants le FIB pour un composant 'i' à l' instant 't' et définie par :

$$I_i^B(t) = \frac{\partial p_s(t)}{\partial p_i(t)} \text{ for } i = 1, 2, \dots, n \quad (2.1)$$

Ce facteur d'importance peut être interprété comme la probabilité pour que le système se trouve dans un état de fonctionnement ayant 'i' comme composant critique, sachant que 'i' est en fonctionnement, soit :

$$I_i^B(t) = p_{(s|i)}(t) - p_{(s|\bar{i})}(t) \quad (2.2)$$

Où:

$p_{(s|i)}(t)$ la probabilité conditionnelle que le système soit défaillant sachant que le composant 'i' est défaillant et $p_{(s|\bar{i})}(t)$ la probabilité conditionnelle que le système soit défaillant sachant que le composant 'i' est en fonctionnement.

Les composants avec une valeur très faible du facteur FIM ont un effet négligeable sur la fiabilité du système. Le FIM est utilisé pour définir d'autres facteurs, telles que le facteur de criticité.

- ✓ **Facteur d'importance Critique** : ce facteur est relié à FIM, il nous renseigne sur les augmentations / diminutions de risque associées à l'augmentation / diminution de la défiabilité d'un composant de base associé à un système. C'est-à-dire. sur quels composants il est nécessaire d'effectuer des actions de réparation, pour que le système fonctionnera à nouveau.

Le facteur d'importance critique $I_i^{CR}(t)$ pour un composant 'i' a l'instant 't' est la probabilité que le composant 'i' est défaillant et ait provoqué la défaillance du système sachant que le système est défaillant a l'instant 't'.

$$I_i^{CR}(t) = \frac{p_i(t)}{p_s(t)} \times I_i^B(t) \text{ for } i = 1, 2, \dots, n \quad (2.3)$$

Le FIC est approprié pour améliorer les performances du système en se concentrant sur les composants qui sont vraiment importants, en permettant d'éviter d'attribuer une haute importance aux composants qui sont très peu susceptibles de se produire.

- ✓ **Facteur d'importance de Diagnostic Fussel-Vesely (FID)**: ce facteur est la probabilité pour que le composant 'i' soit en panne sachant que le système est en panne. Ce facteur tient son nom de son utilité dans le diagnostic des causes de défaillance d'un système.

$$F_i(t) = p_{(i|s)}(t) = \frac{p_i(t)}{p_s(t)} \times p_{(s|i)}(t) \quad (2.4)$$

Ainsi que représente la part des coupes minimales dans lesquelles apparaît au moins une fois l'événement de base 'i', il indique alors le gain en disponibilité que l'on peut attendre sur le système global, résultant d'une fiabilisation totale de 'i'. Cet indicateur est notamment précieux dans la phase de conception d'un système, là où des modifications fonctionnelles et/ou de design importantes peuvent intervenir, et faire varier le risque associé à un système dans d'importantes proportions.

L'arbre de défaillances est une méthode statique basée sur la logique booléenne pour représenter le système étudié. Elle est adaptée à des systèmes à configuration statique, c'est-à-dire des systèmes dont les relations fonctionnelles entre leurs composants restent figées.

Les méthodes les plus adaptées à la modélisation et à l'analyse des systèmes dynamiques sont les modèles états transitions tels que les graphes d'états (les graphes de Markov et les réseaux Bayésiens) et les approches basées sur les réseaux de Petri.

3.4.3. L'arbre d'évènement

L'analyse par arbre d'évènement (Event tree Analysis ETA) [KHA 15], [MAN 05], [RAU 04], [SMI 01], [VIN 99] a été développée au début des années 1970 pour l'évaluation du risque lié à une centrale nucléaire. Comme étant une technique inductive, L'analyse par Arbre d'Évènements permet d'identifier et d'analyser les fréquences de danger par la convention des différents évènements initiateurs en conséquences éventuelles relatives au fonctionnement ou à la défaillance du système selon les dispositifs techniques, humains, et organisationnels.

À l'inverse de l'analyse par Arbre de Défaillances, l'analyse par Arbre d'Évènements suppose la défaillance d'un composant ou d'une partie du système et s'attache à déterminer les évènements qui en découlent.

L'analyse par Arbre d'Évènements se déroule en plusieurs étapes préliminaires

- ✓ Considération d'un évènement initiateur ;
- ✓ Identification des fonctions de sécurité prévues pour contrôler son évolution ;
- ✓ Construction de l'arbre ;
- ✓ Description et exploitation des séquences d'évènements identifiées.

Il serait plus pertinent d'élaborer un Arbre d'Évènements à l'issue d'une première analyse identifiant les accidents potentiels à l'image de l'APR. Les fonctions de sécurité doivent être assurées par des barrières ayant pour objectif d'empêcher le processus de matérialisation d'un accident provoqué par un évènement initiateur.

La construction de l'arbre consiste à envisager soit le bon fonctionnement soit le dysfonctionnement de la première fonction de sécurité en partant de l'évènement initiateur. La suite de la méthode consiste à examiner le développement de chaque branche en considérant systématiquement le fonctionnement ou la défaillance de la fonction de sécurité jusqu'à l'atteinte d'un accident potentiel.

On peut ajouter un aspect quantitatif à l'arbre d'évènement en indiquant les probabilités des événements pris en compte. A chaque alternative on indique la probabilité de la branche supérieure (l'autre étant son complément à 1). La propagation des probabilités d'occurrence des évènements initiateurs permet de calculer la probabilité de l'évènement redouté. La [figure2.4](#) ci-après illustre l'exemple de l'arbre d'évènement.

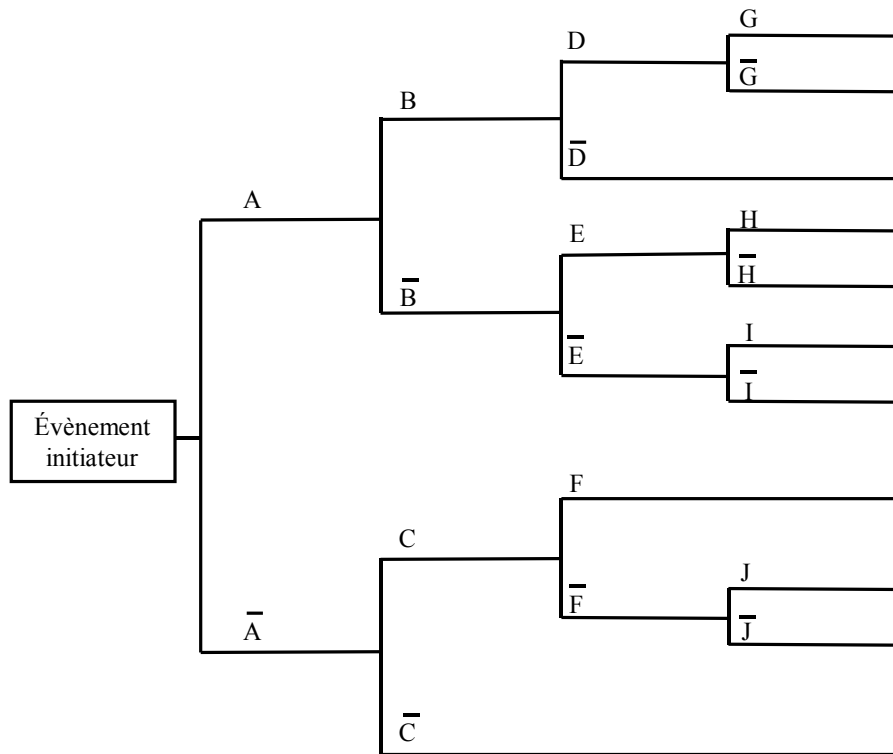


Figure 3.4 Exemple de la structure d'arbre d'événement

3.4.4. Simulation de Monte Carlo

Appelée Monte Carlo par allusion aux jeux de hasard, la simulation de Monte Carlo, [CHE 15], [BOU 13], [FIT 11], [MEG 04], a été utilisée depuis plusieurs siècles, même si ce n'est qu'après la seconde guerre mondiale qu'elles ont acquis un véritable statut de méthode. Le principe de la méthode par simulation Monte Carlo est de remplacer le calcul analytique par du calcul statique en réalisant un grand nombre d'histoires (échantillons) du système étudié par l'attribution d'une valeur numérique aux variables dépendantes du déroulement des processus stochastiques.

Le principe de la méthode par simulation de Monte Carlo est de simuler la « vie » du système au cours de sa période de fonctionnement [MER 16], [RUI 15], [TAY 13]. Plusieurs échantillons sont nécessaires pour déterminer de façon statistique les indices de sûreté de fonctionnement du système. Les résultats donnés par cette méthode ne sont pas les solutions numériques exactes mais des intervalles de confiance les contenant avec une probabilité donnée.

Au cours d'un échantillon, les événements sont tirés de façon aléatoire selon leur loi de probabilité (uniforme, normale, logarithmique, ...). Ensuite, de façon chronologique, le système est analysé à chaque nouvel événement, afin de déterminer s'il fonctionne ou non. Les indices, sont ensuite, mis à jour. L'atout de cette méthode est que l'on peut modéliser n'importe

quelle loi de probabilité, contrairement aux méthodes précédentes où l'emploi de lois de probabilité exponentielles est nécessaire pour le calcul des indices de sûreté du système comme montré dans l'organigramme de la [Figure 3.5](#).

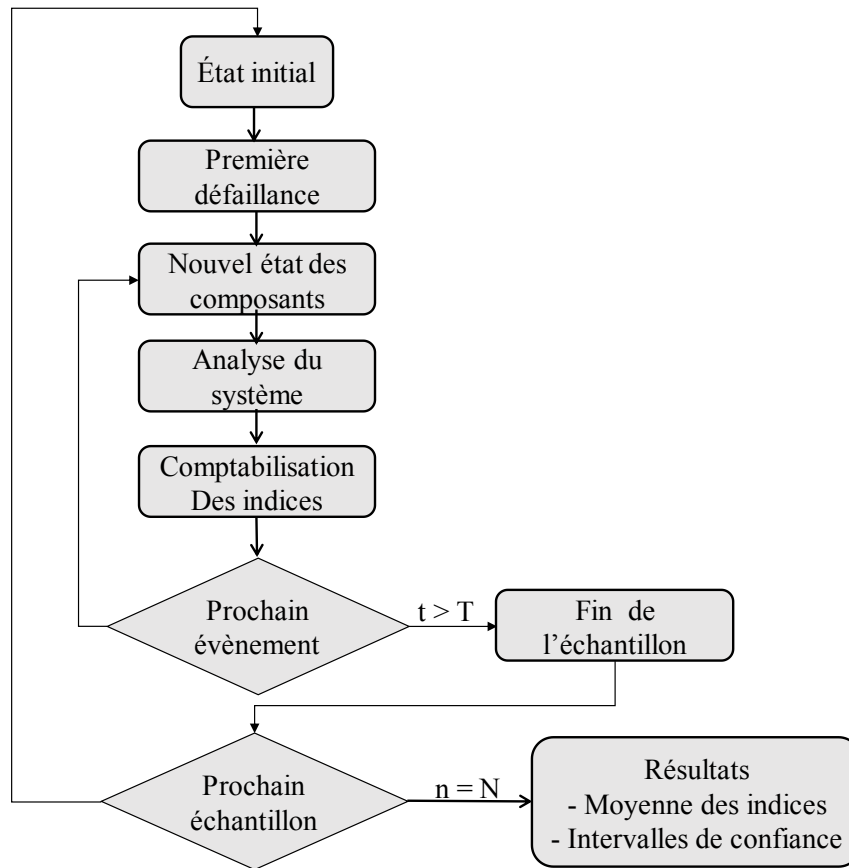


Figure 3.5 Organigramme d'analyse de systèmes par simulation de Monté Carlo

Pour modéliser le système, il faut décrire, d'une part, le fonctionnement des composants et, d'autre part, le fonctionnement du système. Pour un composant, on peut établir différents modèles de fonctionnement suivant la façon dont il est employé.

La description du système doit, à chaque événement, décrire le comportement du système face aux défaillances à savoir toutes les étapes de :

- ✓ Détection de la panne
- ✓ Diagnostic de l'état du système
- ✓ Changement de mode de fonctionnement
- ✓ Maintenance des composants endommagés
- ✓ Remise en service

Cette description regroupe ainsi la détermination de l'état du système après un événement et les éventuelles actions correctrices. Cette description constitue la difficulté majeure de cette méthode puisque chaque système possède une façon de fonctionner bien spécifique.

Les étapes de réalisation de la simulation Monte Carlo sont les suivantes:

- ✓ Définition du système en utilisant un modèle,
- ✓ Génération des numéros aléatoires,
- ✓ Génération des variables aléatoires,
- ✓ Evaluation du modèle,
- ✓ Analyse statistique des résultats,
- ✓ Etude de l'efficacité et de la convergence de la simulation.

On peut effectuer une simulation de MC à partir d'un grand nombre de modèles comportementaux (automates d'états, réseaux de Petri, arbres de défaillance...) pour la résolution d'un problème de fiabilité prévisionnelle [PER 09].

3.4.5. Réseaux bayésiens

Les réseaux bayésiens issus de la théorie des graphes, sont des graphes acycliques orientés. Utilisés dans un but d'aide à la décision et plus précisément dans l'élaboration de stratégies de maintenance des systèmes complexes à travers du diagnostic. Comme étant la méthode choisie pour l'élaboration de ce travail les réseaux bayésiens font objet d'un chapitre détaillé qui suivra ce présent chapitre.

3.4.6. Réseau de Petri stochastique

Un réseau de Petri [TAL 16], [BOU 13], [CHA 13], [DEM 09], [MKH 08], [SAL 07] est un graphe d'état dans lequel on retrouve des états et des transitions auxquelles sont affectées des lois de transitions. Les lois de transitions peuvent être des lois de probabilités ou des délais constants. L'état du graphe est marqué par un « jeton » qui se trouve dans un des états du graphe. On peut affecter aux transitions :

- ✓ Des équations « d'entrée » : pour que la transition soit valide il faut que les conditions imposées sur les variables soient vérifiées.
- ✓ Des changements de variables : lorsque la transition est validée, les valeurs de certaines variables sont modifiées.

Basés sur la description des relations existant entre les conditions et les événements intervenant sur le système, ils s'appuient sur une représentation mathématique qui s'ouvre à différentes formes d'analyse. Un réseau de Petri est un graphe orienté constitué de places, de transitions et d'arcs [Figure 3.6](#):

- ✓ Les places sont représentées graphiquement par des cercles et peuvent être marquées par une ou plusieurs marques appelées jetons. L'ensemble des jetons associés aux différentes places constitue le marquage de réseau et correspond à un état du système modélisé,

- ✓ Les transitions sont représentées par des rectangles et agissent, sous certaines conditions, sur le marquage du réseau,
- ✓ Les arcs sont représentés par des flèches qui lient une place à une transition (arc amont) ou inversement une transition à une place (arc aval). Un poids (entier positif) peut leur être affecté. Par défaut, il est égal à 1.

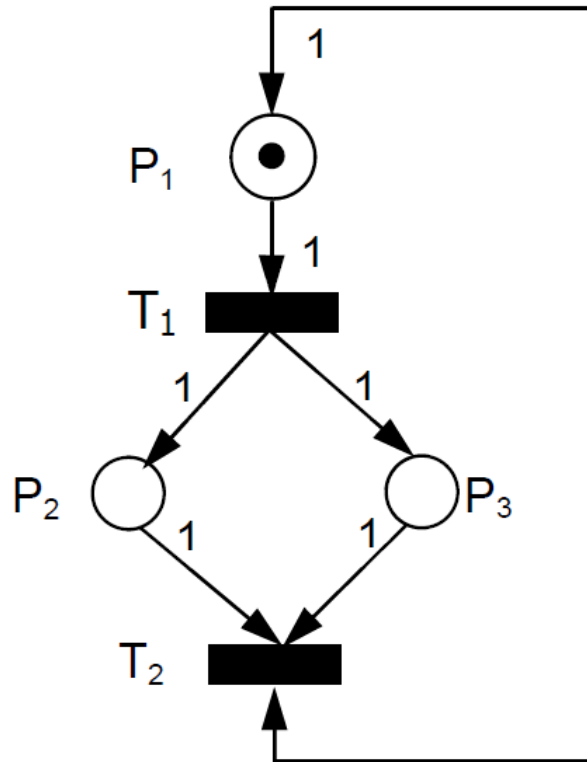


Figure 3.6 Exemple de réseau de Petri

L'ensemble des places, transitions et arcs constitue la partie statique de la structure du réseau de Petri. La partie dynamique du réseau (évolution) est obtenue par des franchissements de transition qui affectent son marquage. Dans le modèle réseau de Petri d'un système, le marquage du réseau représente l'état du système. Le comportement du système est simulé par les franchissements de transitions qui changent l'état du système. Pour qu'une transition soit franchie, il faut qu'elle soit valide ou sensibilisée, c'est à dire que toutes les places amont de la transition doivent posséder un nombre de jetons au moins égal au poids de l'arc qui les relie à la transition. Elle peut alors être franchie et ce franchissement consiste à retirer un nombre de jetons égal au poids de l'arc amont de chacune des places amont associées et à ajouter un nombre de jetons égal au poids de l'arc aval dans chacune des places aval associées. Le nouveau marquage du réseau correspond au nouvel état atteint par le système.

Les RdP stochastiques sont une extension des réseaux de Pétri pour lesquels est associée à chaque transition une variable aléatoire temporelle avec sa fonction de densité de probabilité. Trois classes des RdP stochastiques sont définies:

3.4.6.1. RdP stochastiques classique

Les délais associés à chaque transition sont des variables aléatoires qui suivent des lois de distribution exponentielle. A ce RdP stochastique, on peut associer une chaîne de Markov équivalente. Le graphe de Markov est obtenu directement à partir du graphe d'accessibilité du RdP stochastique en étiquetant chaque arc par un taux de transition d'un marquage à un autre. Le taux de transition est le paramètre de la loi exponentielle qui détermine le délai de franchissement de la transition respective. Pour les différents états, le calcul de probabilités instantanées est obtenu à partir du graphe de Markov.

3.4.6.2. RdP stochastiques généralisés

Dans les RdP stochastiques généralisés, les délais associés aux transitions temporisées suivent des lois de distribution exponentielle et certaines transitions sont immédiates (franchies dès la validation). Un RdP stochastique généralisé comprend deux types d'états : les états tangibles, pour lesquelles toutes les transitions sensibilisées sont temporisées et les états virtuels pour lesquelles il existe une transition immédiate sensibilisée. Une fois que les états virtuels sont éliminés, l'évaluation du marquage reste un processus markovien homogène.

3.4.6.3. RdP stochastiques déterministes :

Dans les RdP stochastiques déterministes, les délais associés aux transitions temporisées suivent des lois de distribution exponentielle ou autre et certaines transitions sont immédiates. Pour ce type de RdP stochastiques, l'évaluation statistique est obtenue, généralement, à l'aide de la simulation Monte Carlo, afin de déterminer les probabilités des différents états car il n'existe pas d'expression analytique dans le cas général. Les RdP stochastiques permettent deux formes d'exploitation:

- ✓ L'analyse directe du graphe des marquages conséquents qui permet de caractériser les propriétés générales et spécifiques (analyse de points de vue) du modèle (le traitement du graphe de marquage est une analyse qualitative),
- ✓ L'exploitation du processus stochastique associé (markovien, semi markovien, avec points de régénération...) qui permet d'évaluer le comportement en régime permanent et transitoire du modèle (fréquence moyenne de franchissement de transition (événement), temps moyen de séjour dans les états tangibles...), cette approche est quantitative.

3.4.7. Graphes de Markov

Les graphes de Markov [BOU 13], [CHA 13], [USH 12], [FIT 11], [MEC 11], [MER10], [DEM 09] sont les plus connues et les plus utilisés, des méthodes mises en œuvre pour le traitement probabiliste des systèmes se comportant dynamiquement. Leur principe est de représenter tous les états du système (états des composants, et mode de fonctionnement du système) et toutes les transactions possibles entre ces états. Le graphe des états permet de visualiser les différents états d'un système qui sont représentées par des cercles et reliés entre eux par des arcs orientés qui correspondent aux transitions (pannes et réparations) entre états.

Les sommets du graphe correspondent aux différents états du système qui sont représentés par des cercles. Ils sont reliés par des arcs orientés affectés d'un taux (ou de probabilités) de transition non nuls associés aux événements correspondant aux conditions de transitions (pannes l et réparation m) qui font évoluer le système d'un état à un autre [Figure 3.7](#). Pour un système à n composants, si chaque composant a deux états (fonctionnement et panne), le nombre maximum d'états est 2^n .

Les graphes de Markov sont couramment utilisés pour étudier la fiabilité des systèmes réparables. Le modèle associe une représentation graphique et une écriture matricielle (matrice de transition).

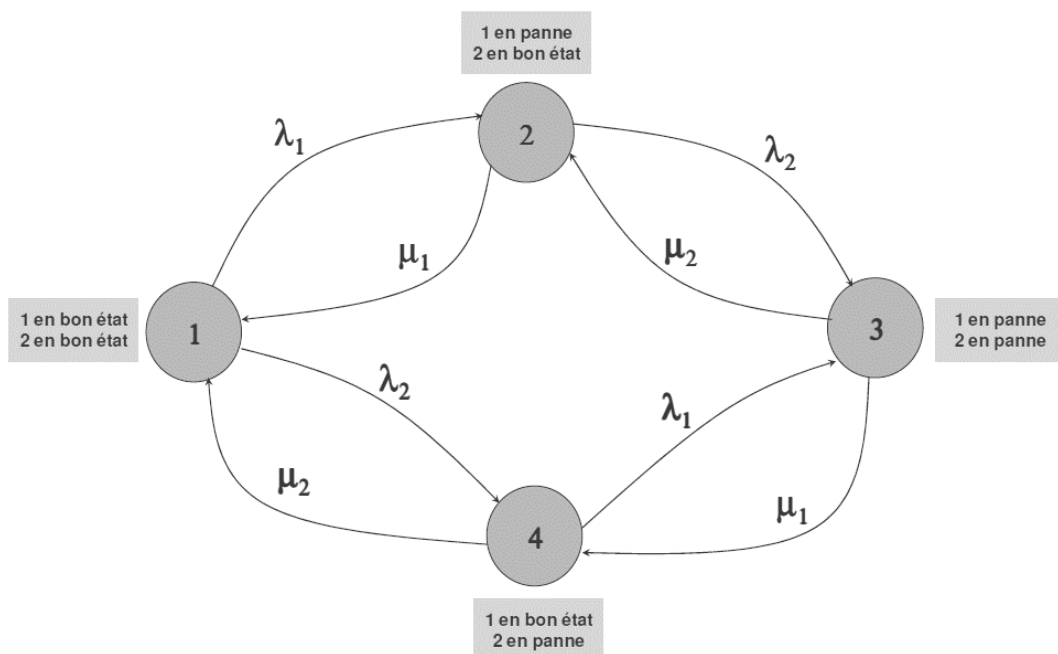


Figure 3.7 Exemple de graphe de Markov

Les traitements relèvent du calcul matriciel: à chaque instant t , la probabilité d'occupation d'un état du système ne dépend que de la distribution initiale (à $t = 0$) d'occupation des états et de la matrice de transition.

Les résultats sont quantitatifs : probabilités d'occupation d'états, fréquence d'événements etc, en régime transitoire ou permanent.

Une structure de coût (bénéfices, pénalités...) peut être associée aux temps d'occupation d'états ou aux événements déclencheurs de changement d'états permettant d'établir facilement différentes caractéristiques économiques.

3.5. Limitation des méthodes d'analyse quantitatives des risques

Le [Tableau 3.3](#) présente les avantages et les limites des méthodes d'analyse sélectionnées pour élaborer nos travaux de recherche.

Tableau 3.3 Résumé sur les avantages et les limites des méthodes d'analyse quantitatives des risques

Méthode	Avantage	Limite
AMDEC	<p>Un outil incontournable d'analyse et d'évaluation de défaillances simples susceptibles de conduire à des défaillances globales au niveau système et aussi d'études de moyens adaptés permettant de limiter leurs effets et prévenir leurs occurrences.</p> <p>Les résultats de l'AMDEC sont spécifiquement détaillés et notamment en ce qui concerne la propagation des défaillances et leurs conséquences.</p> <p>Il peut accompagner quasiment tout le cycle de vie du développement d'un système : conception, validation, test, etc.</p>	<p>Est très difficile à maîtriser, compte tenu du volume important d'informations à traiter et l'impossibilité de décrire des défaillances multiples.</p> <p>L'analyse est complétée par d'autres méthodes telles que les arbres de défaillances.</p> <p>La méthode ne produit pas de façon exhaustive les modes communs et n'évalue pas systématiquement les combinaisons de pannes</p>
AdD	<p>Étude prioritaire des défaillances relatives à des événements redoutés dont la gravité de production est plus significative. Elle permet de considérer</p>	<p>La méthode exige une parfaite connaissance des scénarios événementiels et donc du</p>

	<p>des combinaisons d'évènements pouvant conduire à un événement redouté.</p> <p>Un autre point fort essentiel est la lisibilité à travers la représentation graphique des combinaisons de causes aboutissant à des défaillances.</p> <p>Les coupes minimales représentent des résultats synthétiques qui montrent directement les criticités des composants.</p> <p>L'analyse peut prendre en compte les défaillances multiples et de cause commune.</p>	<p>fonctionnement du système et de son interaction avec son environnement.</p> <p>La lisibilité des arbres de défaillances peut s'avérer très compliquée quand il s'agit de systèmes complexes ou d'évènement indésirable trop générique ou mal spécifié.</p> <p>Cette méthode est efficace pour analyser de petits systèmes. L'analyse d'un système complexe nécessiterait sa décomposition en plusieurs sous-systèmes. Néanmoins, la dernière décennie a vu paraître plusieurs logiciels offrant, entre autres, des fonctionnalités d'aide et d'assistance pour la conception graphique, la recherche systématique des coupes minimales et la propagation des probabilités.</p> <p>Les dépendances ne sont pas prise en compte ainsi que les effets du comportement physique et dynamique du système</p> <p>Dans le cas de gros arbres, il est possible d'oublier des évènements, surtout pour des systèmes à haut risque qui présentent nombreuses redondances et protections</p> <p>La quantité de travail pour construire l'arbre est remarquable.</p> <p>Non continuée dans le temps.</p> <p>Pas de quantification des dépendances temporelles.</p>
--	---	---

		<p>Exploite une vision totalement statique du système.</p> <p>Elle ne prend pas en compte la dimension temporelle ; elle ne rend pas compte de la dynamique d'un système.</p>
AdE	<p>L'analyse par arbre d'évènements permet d'analyser l'évolution des événements initiateurs jusqu'à la réalisation d'un événement redouté.</p> <p>Déterminer la fréquence potentiel d'un scénario catastrophique</p>	<p>La méthode peut s'avérer rapidement fastidieuse si les événements initiateurs ne sont pas bien définis.</p> <p>Il convient donc de sélectionner les événements initiateurs pouvant effectivement conduire à des situations critiques.</p>

3.6. Critères de choix d'une méthode d'analyse de risque

Nous avons retenu l'essentiel des critères pesant dans la mise en œuvre d'une méthode plutôt qu'une autre dans l'étude d'un système donné :

- ✓ Domaine de l'étude.
- ✓ Stade de l'étude (spécification, conception, ..., démantèlement).
- ✓ Perception du risque dans ce domaine.
- ✓ Culture de la Sûreté de Fonctionnement de l'organisation.
- ✓ Caractéristiques du problème à analyser.
- ✓ Niveau envisagé de la démonstration de la sécurité.
- ✓ Savoir-faire des intervenants.
- ✓ Nature des informations disponibles (spécifications du système et de ses interfaces, contraintes, etc.).
- ✓ Retour d'expérience et base de données disponibles.
- ✓ Moyens humains, logistiques et autres.
- ✓ Délais et autres contraintes de management de projet.

Toutefois, l'utilisation séparée d'une seule méthode d'analyse de risque peut ne pas apporter une démonstration définitive de la réalisation des objectifs de sécurité. En effet, il est nécessaire de combiner plusieurs méthodes pour une meilleure complétude et une bonne cohérence en termes de résultats.

3.7. Conclusion

Dans le cadre de ce présent chapitre, nous avons essayé de mieux situer les démarches et méthodes d'analyse des risques, nous avons d'abord clarifié les techniques de raisonnement de l'analyse prévisionnelle des risques où on a présenté la différence entre les méthodes inductive/ déductive, qualitative/ quantitative et statique/ dynamique. Ensuite, les méthodes les plus utilisées dans l'analyse de la sûreté de fonctionnement ont été définies avec le processus de leurs fonctionnements. Après avoir décelé les avantages et les limites des méthodes d'analyse choisis pour le développement de notre travail de recherche, nous avons trouvé intéressant de proposer ensuite les critères de choix d'une méthode d'analyse de risque.

L'**Annexe B** présente plus de détails sur les méthodes d'analyse prévisionnelle des risques utilisées pour l'élaboration de cette thèse.

Dans le chapitre suivant, nous allons revenir avec plus de détails sur l'approche bayésienne et son application dans le domaine de la sûreté de fonctionnement. Nous expliquerons aussi le passage de l'arbre de défaillance vers les réseaux bayésiens ainsi que l'utilisation de l'inférence bayésienne pour l'obtention des facteurs d'importances.

Chapitre IV

L'approche bayésienne en Analyse des risques

“Today's posterior is tomorrows prior.” D. Lindley, 1970.

“Under Bayes' theorem, no theory is perfect. Rather, it is a work in progress, always subject to further refinement and testing.” N. Silver, 2011.

Sommaire du chapitre:

4.1. Introduction	49
4.2. Réseaux Bayésiens	49
4.2.1. Théorème de Bayes'	50
4.2.1.1. Formule de Recomposition.....	51
4.2.1.2. Formule de Bayes	51
4.2.2. Définition du réseau bayésien	52
4.2.3. Inférence.....	54
4.2.4. Méthodes de simplification du réseau	55
4.2.5. Réseaux Bayésiens Dynamiques	55
4.2.6. Utilisation des Réseaux Bayésiens.....	55
4.2.7. Limites des Réseaux Bayésiens	56
4.3. Réseaux bayésiens pour l'analyse quantitative des risques	57
4.3.1. Utilisation des réseaux bayésiens en analyse des risques :	57
4.3.2. Interprétation de ADD en RB	59
4.3.2.1. Convertir l'ADD en RB	61
4.3.2.2. RB obtenu à partir de ADD avec des événements répétés	64
4.3.2.3. L'inférence sur le RB obtenu à partir de ADD.....	66
4.3.3. Facteur d'importance probabiliste en RB	66
4.4. Conclusion	67

4.1. Introduction

Pour étudier la fiabilité d'un système en étant le plus proche de la réalité, il est nécessaire d'effectuer des inférences probabilistes à partir des données à priori (bases de donnée, retour d'expérience ...). Cependant, pour des systèmes de l'industrie à risques majeurs (tel que le nucléaire, l'aéronautique et les hydrocarbures...) où des composants de qualité de plus en plus fiables sont installés une analyse de fiabilité de haut niveau basée sur le retour d'expérience s'avère difficile. Une difficulté qui réside dans la limite des méthodes classiques pour l'évaluation du comportement du système vis-à-vis l'influence de chaque composant dans son bon fonctionnement ou dysfonctionnement. Une difficulté aussi dans la prise de décision nécessaire au temps opportun pour que le système préserve une fiabilité très élevée.

Une alternance à la limite des méthodes classiques est l'approche bayésienne, Ceci en terme d'aide à la décision en temps réel relatif assurant un haut niveau de fiabilité des systèmes en prenant en considération les mise-à-jour des données (retour d'expérience, avis d'expert, les données de maintenance...). L'utilisation de l'approche s'avère plus appropriée, puisqu'elle permet d'avoir le maximum d'information sur le système en prenant en considération tous les données des composants dans leurs différents états (fonctionnements, en standbys, défaillants ou bien en phase de maintenance) soit par mise-à-jour des données soit par inférence sur le réseau bayésien. Ces nouvelles informations qui vont être comme étant des connaissances a priori contribuent dans l'évaluation du système en temps réel pour une exacte aide à la décision par le biais des probabilités obtenues en posteriori, afin d'assurer un haut niveau de fiabilité, disponibilité, maintenabilité et sur tout sécurité du système.

Dans ce chapitre les réseaux bayésiens sont introduits par leurs formalisme basé sur les théories des probabilités et des graphes, leurs intérêts et leurs importances dans la modélisation de la fiabilité des systèmes à partir des données aprioris, afin d'obtenir un modèle d'aide à la décision dynamique qui évalue l'évolution du système dans le temps. Ce modèle a été établi par le passage d'un arbre de défaillance, comme étant une méthode classique d'analyse quantitative des risques, vers le réseau bayésien en se basant sur des études de recherche récentes et à partir de ce travail nous avons contribué dans le calcul des facteurs probabilistes d'importance en utilisant l'inférence bayésienne.

4.2. Réseaux Bayésiens

La représentation des connaissances et le raisonnement a donné naissance à de nombreux modèles. Les modèles graphiques probabilistes, et plus précisément les réseaux bayésiens, qui doivent leur nom au travaux de Thomas Bayes au XVIIIe siècle sur la théorie des probabilités

Figure 4.1, les réseaux bayésiens sont initiés par Judea Pearl dans les années 1980 [PEA 86], se sont révélés des outils très pratiques pour la représentation de connaissances incertaines, et le raisonnement à partir d'informations incomplètes [BOU13], [FEN 13], [CHA 13], [ZAI 12], [LAM 10], [LEG 09], [LER 09], [NAI 07].

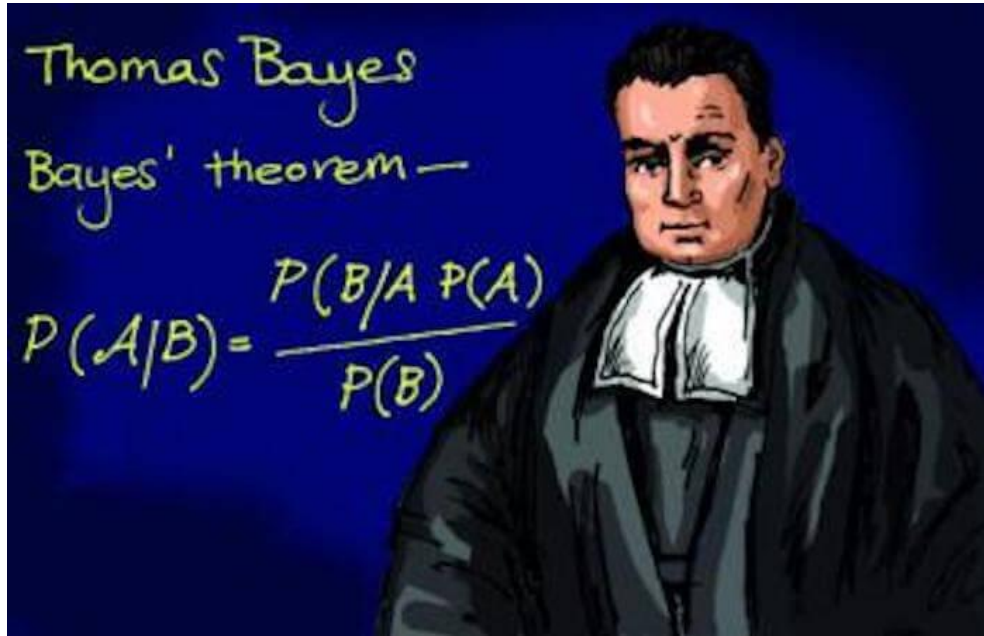


Figure 4.1 Thomas Bayes connu pour avoir formulé le théorème de probabilité conditionnelle

4.2.1. Théorème de Bayes'

Le théorème de Bayes permet de fusionner deux types d'information : la connaissance initiale, dite a priori, obtenu à partir du jugement d'experts ou le retour d'expérience, et la vraisemblance qui représente les observations du retour d'expérience pour obtenir une connaissance enrichie [BEL 16], [FEN 13], dont l'incertitude est plus faible : La probabilité a posteriori représentant ainsi la nouvelle connaissance pour l'expert. Notons que le résultat a posteriori peut devenir l'information a priori si de nouvelles informations issues du retour d'expérience sont disponibles. Ceci représente le principe d'actualisation dynamique des connaissances utilisé particulièrement pour les bases de données.

Pour une Analyse Quantitative des risques, l'application du théorème bayésienne consiste en l'application de l'inférence bayésienne représentée dans la Figure 4.2. Le passage de la distribution a priori à la distribution a posteriori des paramètres du modèle probabiliste est exprimé par la formule de Bayes afin d'établir une aide à la décision, qui peut être par la suite interprétée comme une mise à jour de la connaissance, sur le réseau bayésien.

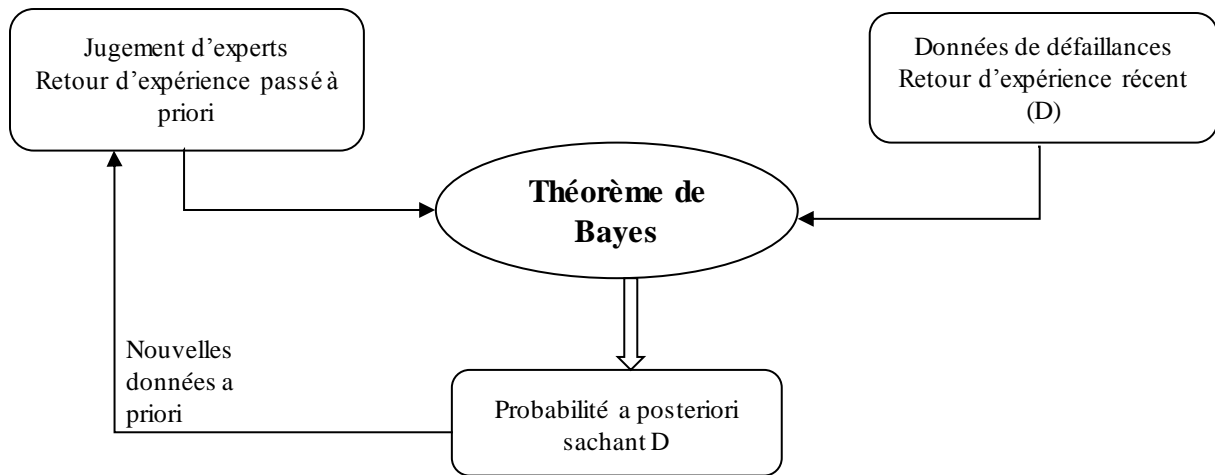


Figure 4.2 Principe de l'approche Bayésienne.

4.2.1.1. Formule de Recomposition

$$\forall A \in I, P(A) = \sum_i^n P(A|B_i)P(B_i) \quad (4.1)$$

4.2.1.2. Formule de Bayes

$$P(B_i/A) = \frac{P(A/B_i) \cdot P(B_i)}{\sum_j [P(A/B_j) \cdot P(B_j)]} \quad (4.2)$$

La probabilité conditionnelle de réalisation d'un événement B sachant que l'événement A s'est produit, est proportionnelle à la probabilité (a priori) de B (probabilité avant que l'on observe A) multipliée par la probabilité d'observer A sachant B.

Où : B: événement étudié,

A: événement(s) observé(s),

$P(B)$: probabilité a priori de réalisation de l'événement B,

(A/B) : vraisemblance de l'occurrence de l'événement B_i sachant que A a été observé,

(B/A) : probabilité a postérieure de réalisation de l'événement B sachant que A a été observé.

Exemple: la Fiabilité d'un système de détection

Un système de détection répond par une alerte à la détection d'une panne intervenant sur une machine donnée. Soient A l'événement « l'alerte est donnée », et B l'événement « le système est en panne », vérifiant les probabilités conditionnelles suivantes :

$$P(A|B) = 0,99 \text{ et } P(A|\bar{B}) = 0,002.$$

Le problème que se pose le service de sécurité est le suivant : si l'alerte est donnée, quelle est la probabilité pour qu'elle corresponde à une panne, sachant qu'une panne survient avec une probabilité égale à 0,01 ?

Il s'agit de calculer $P(B|A)$ égal à :

$$\frac{P(A|B)P(B)}{P(B)P(A|B) + P(\bar{B})P(A|\bar{B})} = \frac{0,99 \times 0,01}{0,01 \times 0,99 + 0,99 \times 0,002} \approx 0,83.$$

4.2.2. Définition du Réseau Bayésien

Un réseau bayésien $RB = (G, \theta)$ peut être défini par :

$G = (V, E)$, un graphe acyclique orienté où V est l'ensemble des nœuds de G , et E l'ensemble des arcs de G .

$\theta = \{P(V_i | Pa(V_i))\}$ Ensemble des probabilités de chaque nœud V_i conditionnellement à l'état de ses parents $Pa(V_i)$ dans G .

Un réseau bayésien est donc un graphe causal auquel on a associé une représentation probabiliste sous-jacente. Cette représentation permet de rendre quantitatifs les raisonnements sur les causalités que l'on peut faire à l'intérieur du graphe.

Le graphe est appréhendé selon un aspect qualitatif et un aspect quantitatif. L'aspect qualitatif du graphe indique les dépendances (ou indépendances) entre les variables et donne un outil visuel de représentation des connaissances, outil plus facilement appréhendable par ses utilisateurs. De plus, l'utilisation de probabilités permet de prendre en compte l'incertain, en quantifiant les dépendances entre les variables, c'est l'aspect quantitatif.

J. Pearl a aussi montré que les réseaux bayésiens permettaient de représenter de manière compacte la distribution de probabilité jointe sur l'ensemble des variables :

$$P(V_1, V_2, \dots, V_n) = \prod_{i=1}^n P(V_i | Pa(V_i)) \quad (4.3)$$

Où $Pa(V_i)$ sont les prédécesseurs de X_i auxquels ça probabilité est sensible, également appelé les parents markoviens de X_i . Rigoureusement, Pa_i est défini comme le sous-ensemble minimal satisfaisant $\{X_1, X_2, \dots, X_n\}$.

Cette décomposition d'une fonction globale en un produit de termes locaux dépendant uniquement du nœud considéré et de ses parents dans le graphe [Figure 4.3](#), est une propriété fondamentale des réseaux bayésiens. Elle permet de calculer $P(V)$ d'une manière plus rapide lorsqu'il y a des dépendances entre les variables. Elle est à la base des premiers travaux portant sur le développement d'algorithmes d'inférences, qui calculent la probabilité de n'importe quelle variable du modèle à partir de l'observation même partielle des autres variables.

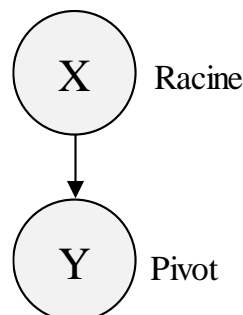


Figure 4.3 RB où X est la cause de Y

$$P(V_i | Pa_i) = P(V_i | V_1, \dots, V_{i-1}) \quad (4.4)$$

Où Pa_i est minimal dans le sens qu'aucun de ses sous-ensembles n'est conforme à l'équation 4.4. La distribution conjointe d'un ensemble de variables donne toutes les informations nécessaires sur la distribution.

À partir de l'équation 4.3 et .44, on peut voir que la fonction de probabilité d'un réseau bayésien est donnée en spécifiant un ensemble d'hypothèses d'indépendance conditionnelles ainsi qu'un ensemble de tableau des probabilités conditionnelles (TPC), qui spécifient les probabilités antérieures de tous les nœuds racine et les probabilités conditionnelles de tous les nœuds intermédiaires et les nœuds feuilles en prenant en considération toutes les combinaisons possibles de leurs parents.

Reprenons l'Exemple 1 : la Fiabilité d'un système de détection :

Un système de détection répond par une alerte à la détection d'une panne intervenant sur une machine donnée. Soient A l'événement « l'alerte est donnée », et B l'événement « le système est en panne », vérifiant les probabilités conditionnelles suivantes :

$$P(A|B) = 0,99 \text{ et } P(A|\bar{B}) = 0,002.$$

$$P(B|A) \text{ a été calculée précédemment, } P(B|A) = 0,83$$

Le problème que se pose le service de sécurité est le suivant : si l'alerte est donnée, quelle est la probabilité pour qu'elle corresponde à une panne, sachant qu'une panne survient avec une probabilité égale à 0,01 ?

Il s'agit de calculer $P(B|A)$ égal à :

$$\frac{P(A|B)P(B)}{P(B)P(A|B) + P(\bar{B})P(A|\bar{B})} = \frac{0,99 \times 0,01}{0,01 \times 0,99 + 0,99 \times 0,002} \approx 0,83.$$

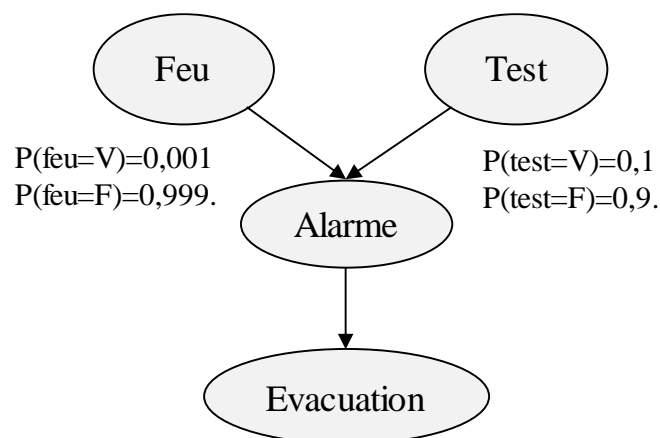


Figure 4.4 Réseau bayésien d'un système de détection.

Et les tables des probabilités conditionnelles (TPC) pour les variables alarme et évacuation sont illustrés dans les [Tableaux 4.1](#) et [4.2](#).

Tableau 4.1 TPC du nœud alarme.

Noeuds Racines		Alarme		
Feu	Test	V	F	diagramme à barres
V	V	0,9	0,1	
	F	0,8	0,2	
F	V	0,8	0,2	
	F	0,01	0,99	

Tableau 4.2 TPC du nœud Evacuation.

Noeuds Racines		Evacuation		
Alarme		V	F	diagramme à barres
V		0,9	0,1	
F		0,001	0,999	

4.2.3. Inférence

L'utilisation essentielle des réseaux bayésiens est donc de calculer des probabilités conditionnelles d'événements reliés les uns aux autres par des relations de cause à effet. Cette utilisation s'appelle inférence [GUE 18], [HAM 08], [NAI 07], [COR 03], [MUR 02]. La correspondance qui existe entre la structure graphique et la structure probabiliste associée va permettre de ramener l'ensemble des problèmes de l'inférence à des problèmes de théorie des graphes.

D'une manière générale, tout calcul portant sur la distribution de probabilité associée à un réseau bayésien relève de l'inférence. Certains types de calcul ont traditionnellement une plus grande importance, parce qu'ils peuvent correspondre à des utilisations pratiques.

C'est vrai en particulier du calcul de la probabilité d'une variable conditionnée à un ensemble d'observations. Ce type d'inférence, appelée aussi mise à jour des probabilités, est essentiel dans des applications de diagnostic, où l'on doit reconsidérer son appréciation de la situation en fonction d'une ou plusieurs nouvelles observations.

Le problème de l'inférence est uniquement un problème de calculs. Il n'y a aucun problème théorique ; en effet, la distribution de probabilité étant entièrement définie, on peut (en principe) tout calculer.

4.2.4. Méthodes de simplification du réseau

Le nombre d'entrées dans les tableaux des probabilités conditionnelles d'un réseau bayésien peut facilement devenir important parce qu'il croît de manière exponentielle avec le nombre de parents dans le réseau [Tableau 4.1](#), [4.2](#), pour une variable de m états et n parents, il est égal à m^n . Comme solution il faut simplifier l'hypothèse, par exemple en cherchant la corrélation entre certaines variables et remplacer les unes par les autres. Ceci peut aider à la réduction des nombres de case dans les Tableaux de probabilité conditionnelle. Parmi ces hypothèses est d'utiliser la porte logique 'ou' qui permet au nombre de probabilités des variables spécifiées de croître de manière linéaire avec le nombre de ses parents.

4.2.5. Réseaux Bayésiens Dynamiques

Les RB simple sont considérés comme étant un modèle discret. Récemment, de nombreux travaux de recherche [ZAI 12], [NAI 07], [MUR 02] ont été élaborés pour élargir la définition des réseaux Bayésiens afin de les rendre beaucoup plus important. Les réseaux bayésiens peuvent, par exemple, prendre en considération la continuité dans le temps : la probabilité qu'une variable change d'état, dépend du temps dans le cas où les paramètres du système changent dans le temps. Dans la littérature, il existe plusieurs définitions des réseaux bayésiens dynamiques d'une manière général on peut dire que c'est les RB qui incorporent des caractéristiques temporelles. Les réseaux dynamiques sont considérés comme un cas général des réseaux temporels où le terme dynamique fait référence à tout changement auquel le système est soumis en tant que changement d'état.

4.2.6. Utilisation des Réseaux Bayésiens

L'utilisation pratique d'un réseau bayésien peut être envisagée au même titre que celle d'autres modèles [NAI 07] : réseau de neurones, arbre de décision, modèle d'analyse de données (régression linéaire), arbre de défaillances, modèle logique. Naturellement, le choix de la méthode fait intervenir différents critères, comme la facilité, le coût et le délai de mise en œuvre d'une solution. En dehors de toute considération théorique, les aspects suivants des réseaux bayésiens les rendent, dans de nombreux cas, préférables à d'autres modèles :

- ✓ La possibilité de rassembler et de fusionner des connaissances de diverses natures dans un même modèle : retour d'expérience, expertise, observations.
- ✓ La représentation graphique d'un réseau bayésien est explicite, intuitive et compréhensible par un non-spécialiste, ce qui facilite à la fois la validation du modèle, ses évolutions éventuelles et surtout son utilisation.

- ✓ Un réseau bayésien est polyvalent : on peut se servir du même modèle pour évaluer, prévoir, diagnostiquer, ou optimiser des décisions, ce qui contribue à rentabiliser l'effort de construction du réseau bayésien.
- ✓ Il existe aujourd'hui de nombreux logiciels pour saisir et traiter des réseaux bayésiens. Ces outils présentent des fonctionnalités plus ou moins évoluées : apprentissage des probabilités, apprentissage de la structure du réseau bayésien, possibilité d'intégrer des variables continues, et de décision, etc.

4.2.7. Limites des Réseaux Bayésiens

- ✓ Un recul encore insuffisant pour l'apprentissage : la technique des réseaux bayésiens n'a pas immédiatement intégré l'ensemble de la problématique de l'apprentissage, comme cela avait été le cas des réseaux neuronaux. Aujourd'hui, l'essentiel de la littérature sur l'apprentissage avec des réseaux bayésiens ignore le problème de la capacité de généralisation d'un modèle, et des précautions que cela implique au moment de la construction du modèle. La prise en compte de ce problème peut s'effectuer par le choix du critère de recherche ou de distance des distributions de probabilité.
- ✓ Utilisation des probabilités : L'utilisation des graphes de causalités est, une approche très intuitive. Il reste cependant que la notion de probabilité, est, au contraire, assez peu intuitive. Il est en effet assez facile de construire des paradoxes fondés sur des raisonnements probabilistes. Les modèles déterministes, formulés en termes d'entrées et de sorties, comme les modèles de régression, les réseaux de neurones, ou les arbres de décision, même s'ils peuvent être réinterprétés dans le cadre d'un formalisme probabiliste, restent d'un abord plus facile.
- ✓ Lisibilité des graphes : En effet, même si la connaissance manipulée dans les réseaux bayésiens, ou extraites des données par les algorithmes d'apprentissage associés est lisible puisque représentée sous forme de graphes, elle reste moins lisible que celle représentée par un arbre de décision, par exemple, surtout si ce graphe présente un grand nombre de nœuds. Notons aussi que l'information représentée par le graphe est la structure des causalités. Les probabilités ne sont pas représentables, et on n'a donc pas d'idée, à la simple lecture du graphe, de l'importance d'un arc donné.
- ✓ Les variables continues : L'essentiel des algorithmes développés pour l'inférence et l'apprentissage dans les réseaux bayésiens, aussi bien que les outils disponibles sur le marché pour mettre en œuvre ces algorithmes utilisent des variables discrètes.

En effet, la machinerie des algorithmes d'inférence est essentiellement fondée sur une algèbre de tables de probabilités. De même, les algorithmes d'apprentissage modélisent en général les distributions de probabilité des paramètres contenus dans les tables du réseau, c'est-à-dire de probabilités discrètes. Même s'il est théoriquement possible de généraliser les techniques développées aux variables continues, il semble que la communauté de recherche travaillant sur les réseaux bayésiens n'a pas encore vraiment intégré ces problèmes. Cela pénalise cette technologie, en particulier pour des applications de data mining où variables continues.

- ✓ La complexité des algorithmes : La généralité du formalisme des réseaux bayésiens aussi bien en termes de représentation que d'utilisation les rend difficiles à manipuler à partir d'une certaine taille. La complexité des réseaux bayésiens ne se traduit pas seulement en termes de compréhension par les utilisateurs. Les problèmes sous-jacents sont pratiquement tous de complexité non polynomiale, et conduisent à développer des algorithmes approchés, dont le comportement n'est pas garanti pour des problèmes de grande taille.

4.3. Réseaux bayésiens pour l'analyse quantitative des risques

4.3.1. Utilisation des réseaux bayésiens en analyse des risques :

Les réseaux bayésiens ont été initié tout d'abord dans le domaine de l'intelligence artificielle [COR 03], puis élargi dans les autres domaines scientifiques, en particulier dans le domaine de l'analyse des risques pour la gestion des événements incertains, la détection et le diagnostic des défaillances des systèmes complexes [WEB 12], [LAM 10], [LAM 09], [KAL 09], [HAM 08], [SIN 06], [PRO 03].

La [Figure 4.5](#) montre que l'utilisation des réseaux bayésien dans le domaine de l'analyse des risques est de 26% et la fiabilité des systèmes est de 61%. Il y a une très grande importance accordée à cette approche pour le traitement des données issues des approches de la sûreté de fonctionnement [BEL 16], [BOU 13], [DEM 09] ce qui renforce notre démarche dans cette thèse.

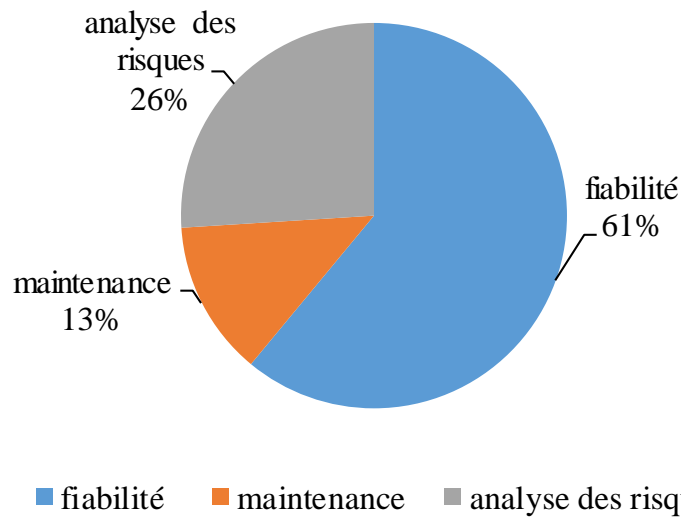


Figure 4.5 Taux d'utilisation des réseaux bayésiens en sûreté de fonctionnement

La tendance des publications des travaux de recherche sur les réseaux bayésiens liées à l'analyse des risques dans les revues internationales et les articles les plus important dans le temps jusqu'à 2008 sont montrés dans les Figures 4.6 et 4.7 comme suite :

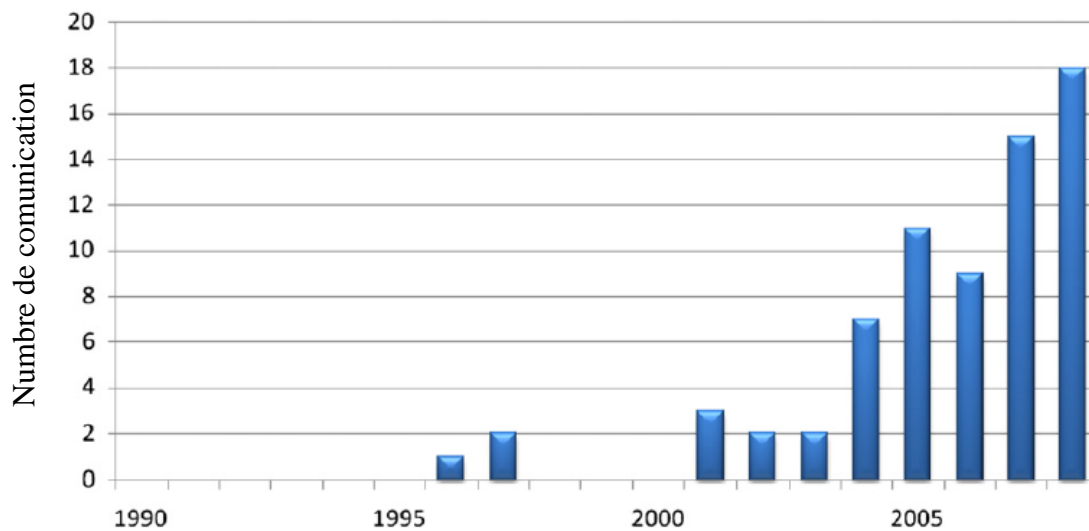


Figure 4.6 Tendance d'utilisation des réseaux bayésiens dans l'analyse des risques

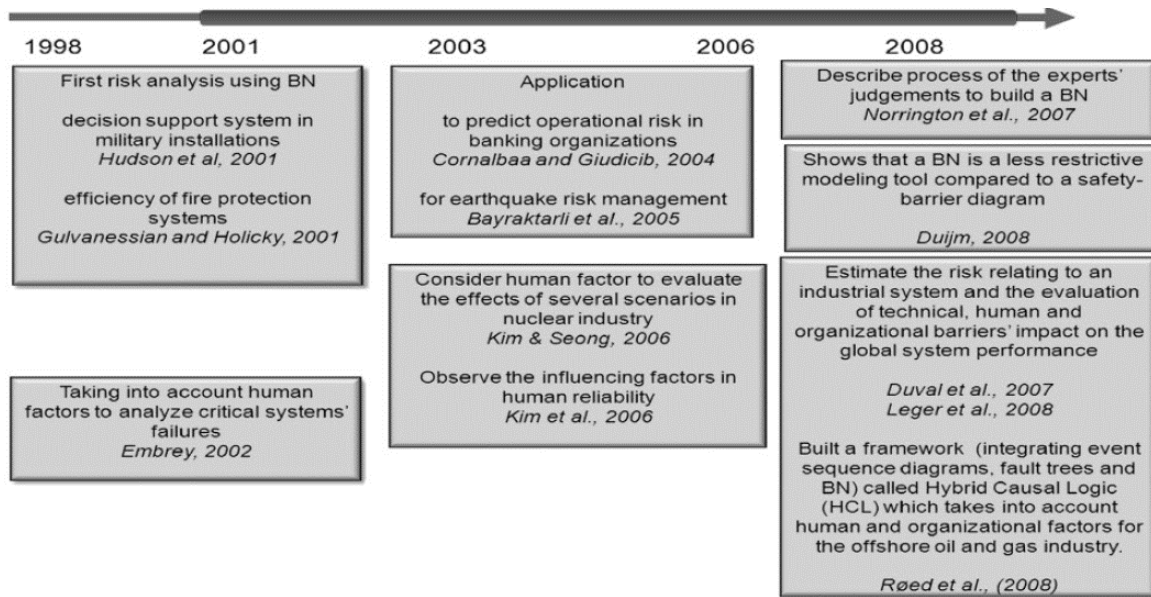


Figure 4.7 Les publications les plus cités sur les réseaux bayésiens liées à l'analyse des risques jusqu'à 2008

4.3.2. Interprétation de AdD en RB

Plusieurs travaux de recherche cités dans le [Tableau 4.1](#), ont démontrés la similitude entre l'arbre de défaillance et les réseaux bayésiens afin d'établir des algorithmes capables de convertir l'arbre de défaillance issue des méthodes classique vers les réseaux bayésiens parmi les méthodes les plus efficaces et les plus utilisées dans le domaine d'intelligence artificiel. Afin de promouvoir un outil d'aide à la décision en temps réel pour des études de sûreté de fonctionnement plus approfondies. Ces travaux montrent comment un AdD peut être converti en un RB et que toutes les analyses et étapes dans le sens des coupes minimales effectuées sur un modèle AdD peuvent être présentées dans un RB [FEN 13], [LAM 10], [SIN 06]. En plus de cela, certaines nouvelles analyses sont faites par le biais des RB telles que le calcul de la probabilité a posteriori d'un système sachant que des composants sont défaillants. Par conséquent, n'importe quel AdD correspond à un RB et toute technique appliquée à un AdD peut être réalisée dans un RB, mais ça nécessite certaines solutions de modélisation [BIB, 01].

Tableau 4.3 Travaux de recherche sur le passage de l'arbre de défaillance vers les réseaux bayésiens

Référence	Domaine / Cas d'application	Méthodologie de travaille
[GUE 18]	L'inférence bayésienne pour l'obtention des facteurs d'importance probabilistes pour un systèmes déluge à eau	<ul style="list-style-type: none"> ✓ AdD d'un systèmes déluge à eau ; ✓ Convertir l'AdD en RB pour l'obtention de l'outil d'aide à la décision; ✓ L'inférence bayésienne ;

	convertir l'arbre de défaillance issue des méthodes classique vers les réseaux bayésiens	<ul style="list-style-type: none"> ✓ Obtention des FIP en terme de posteriori et les comparer avec les résultats obtenus par modèle mathématique; ✓ RB pour la mise à jour des données.
[DON 16]	Modélisation des taux de défaillance par réseaux bayésiens cas d'une turbine dans le domaine nucléaire	<ul style="list-style-type: none"> ✓ Modélisation des taux de défaillance par Arbre de défaillance, ✓ Convertir les données apriori en réseaux bayésiens, ✓ Un outil utile dans l'évaluation dynamique des risques à partir des données apostériori.
[CAI 13]	Maintenance préventive et l'évaluation de la fiabilité et la disponibilité par réseau bayésien obtenu à partir de l'arbre de défaillance cas de la plateforme de forage en mer	<ul style="list-style-type: none"> ✓ Transformation de l'arbre des défaillances en un réseau bayésien ✓ Les dépendances et la relations cause à effet ✓ Démonstration de l'application par l'étude du cas ✓ Effectuer à la fois l'analyse prédictive et le diagnostic par RB ✓ Détection des causes de défaillance par RB
[KHA2 13]	Implémentation d'un réseau bayésien à partir de l'AdD pour évaluer et analyser les risques d'une plateforme de forage en mer	<ul style="list-style-type: none"> ✓ Introduction d'un algorithme de RB innovant pour modéliser l'AdD, ✓ Une technique robuste pour modéliser un système dynamique pour mettre à jour les données, ✓ Mise à jour et adaptation des données.
[KHA 11]	Algorithme de passage de l'arbre de défaillance vers le réseau bayésien d'un procédé de gaz	<ul style="list-style-type: none"> ✓ Fondamentaux sur arbres des défaillances et réseaux bayésiens ✓ Modélisation de l'étude de cas ✓ comparaison entre les résultats des deux méthodes

4.3.2.1. Convertir l'AdD en RB

A partir des travaux de recherche cités dans le [Tableau 4.3](#) un algorithme d'obtention d'un RB à partir d'un AdD est proposé ci-dessous avec une simplification présentée dans la [Figure 4.8](#) dans cet Algorithme il est supposé que le AdD n'aura que des portes logique « ou », « et » et « k -sur- n », le RB résultant sera binaire et ces variables représenteront les états des composants d'un système et les deux valeurs qu'elles pourront prendre seront désignées par faux « F » pour l'état de fonctionnement et par vrai « V » pour l'état défaillant. Cependant, l'algorithme peut être généralisé à n'importe quel AdD.

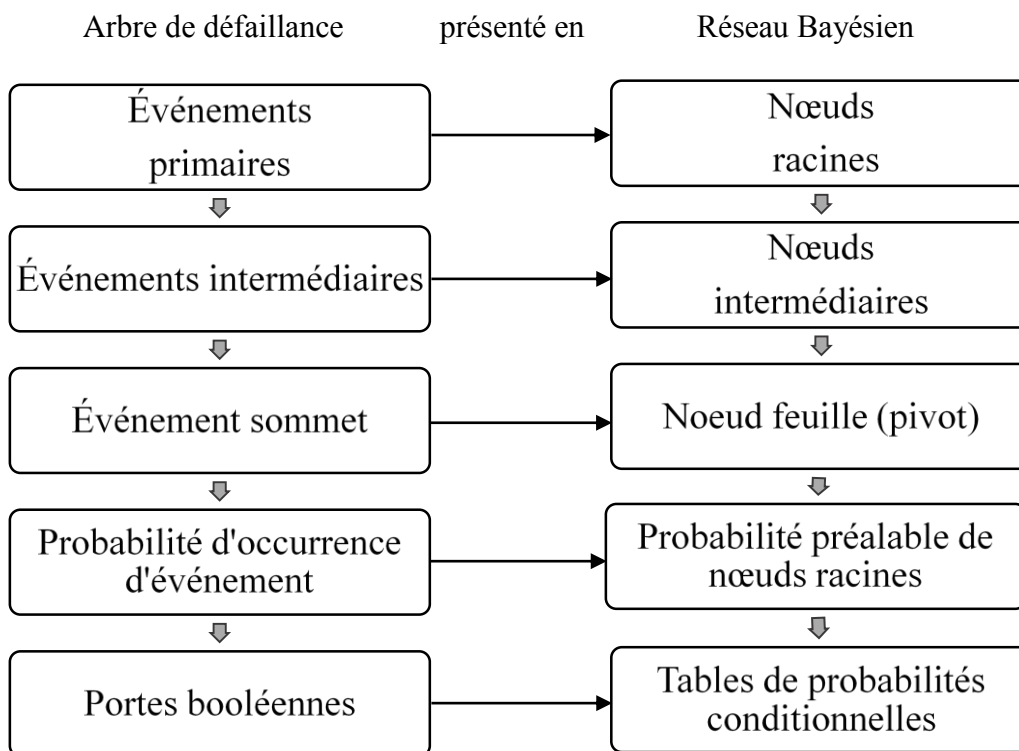


Figure 4.8 Organigramme représentant un algorithme simplifié pour représenter un AdD en RB

En ce qui concerne la partie qualitative du RB:

1. Chaque événement de base de l'AdD est converti en un nœud racine (parent) dans le RB;
2. Pour chaque nœud pivot 'feuille' du BN correspondant à un événement sommet ou intermédiaire désigné par la porte logique dans l'AdD selon l'emplacement, en particulier la dernière porte logique et l'événement sommet finale de AdD sera étiquetée en tant que nœud de défaillance;
3. Les nœuds du RB doivent être connectés entre eux selon l'arrangement des portes logique de l'AdD.

Les [Figures 4.9](#) et [4.10](#) montrent comment la structure d'un AdD simple est convertie RB.

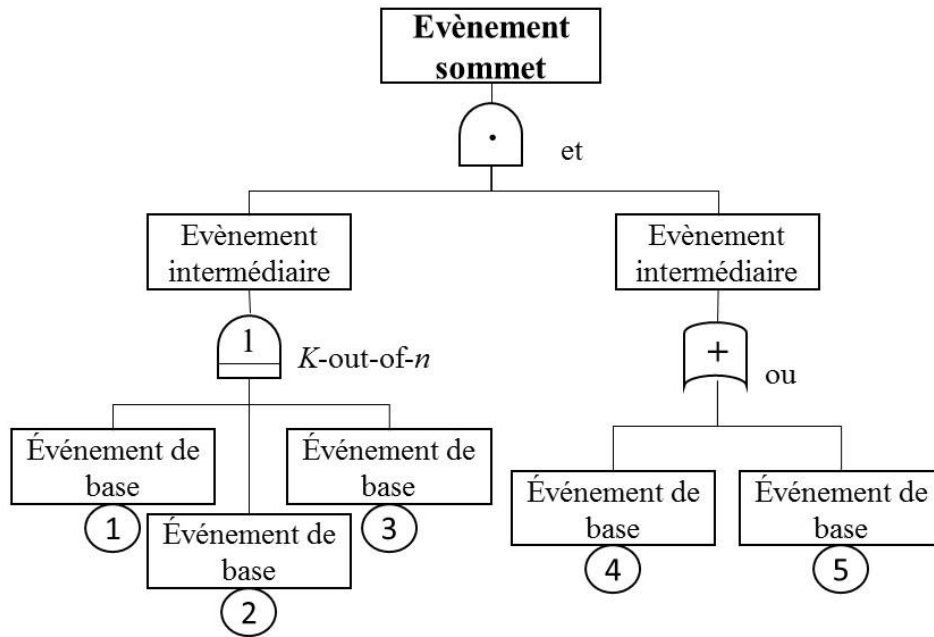


Figure 4.9 Exemple de Structure d'AdD

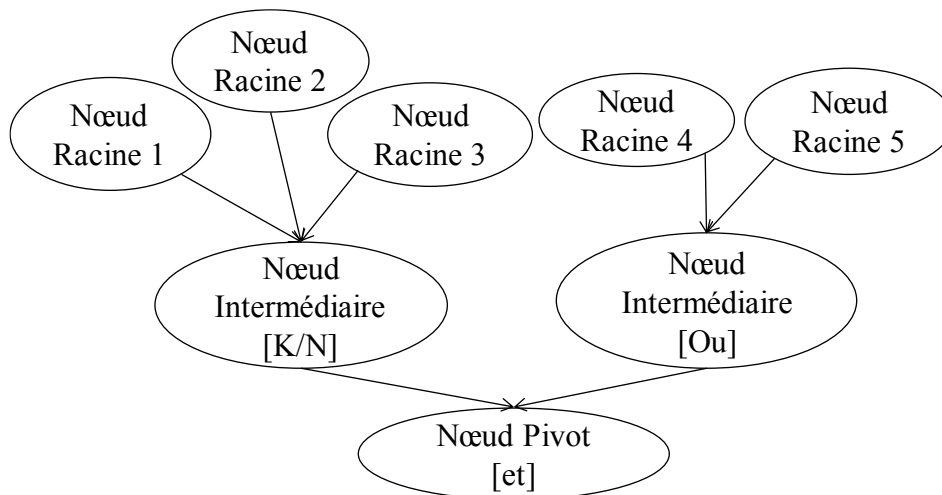


Figure 4.10 Structure du réseau bayésien obtenu à partir de la Figure 4.9

En ce qui concerne la partie quantitative (probabilité) du RB:

1. Pour chaque nœud racine du RB la même probabilité antérieure de l'évènement de base correspondant dans le AdD est attribuée;
2. Chaque porte logique 'ou', 'et', 'k-sur-n' dans l'AdD correspond à une table de probabilité conditionnelle équivalente dans le RB.

Les Tableaux 4.4, 4.5 et 4.6 présentent les tables de probabilité conditionnelles des portes logique 'ou', 'et', 'k-sur-n' respectivement.

La méthode de conversion peut être étendue aux AdD avec d'autres portes et les CPT des réseaux correspondants suivront les tables logiques des portes.

Tableau 4.4 TPC de la porte logique « Ou »

Nœud Racine 1	Nœud Racine 2	P(Nœud Intermédiaire [Ou]=0)	P(Nœud Intermédiaire [Ou]=1)
0	0	1	0
0	1	0	1
1	0	0	1
1	1	0	1

Tableau 4.5 TPC de la porte logique « et »

Nœud Intermédiaire [K/N]	Nœud Intermédiaire [Ou]	P(Nœud Pivot [Et]=0)	P(Nœud Pivot [Et]=1)
0	0	1	0
0	1	1	0
1	0	1	0
1	1	0	1

Tableau 4.6 TPC de la porte logique « 2 sur 3 »

Nœud Racine 3	Nœud Racine 4	Nœud Racine 5	P(Nœud Intermédiaire [K/N]=0)	P(Nœud Intermédiaire [K/N]=1)
0	0	0	1	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	0	1

4.3.2.2. RB obtenu à partir de AdD avec des événements répétés

Les événements de base qui apparaît plusieurs fois dans l'AdD (événements répétés), peuvent être représentés dans les RB en créant simplement un seul nœud pour les événements de base répétés et en le reliant avec plusieurs arcs vers les nœuds correspondant aux événements répétés.

Dans la Figure 4.11, l'événement de base A apparaît deux fois dans l'AdD en tant que sortie des portes EI1 et EI 2.

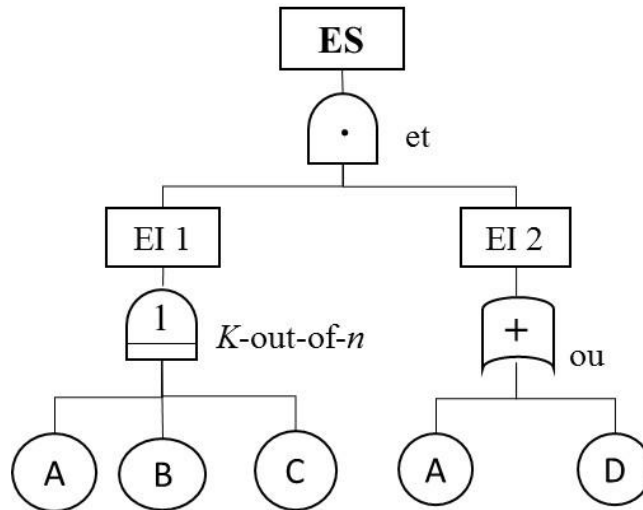


Figure 4.11 Arbres de défaillance avec un événement répété

Le RB correspondant à l'AdD dans la Figure 4.11 est présenté dans la Figure 4.12 avec le nœud A qui apparaît qu'une seul fois liées avec 2 arcs un vers EI 1 et l'autre vers EI 2.

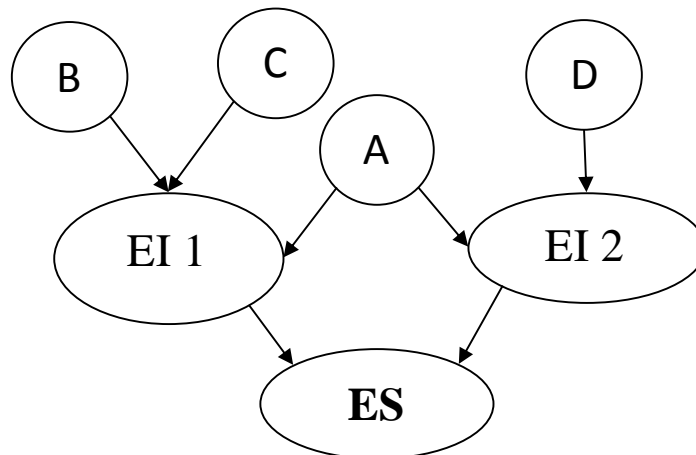


Figure 4.12 Réseau bayésien avec nœud répété

Lorsqu'un AdD a de nombreux événements répétés, le RB correspondant peut prendre une structure graphique dans laquelle les arcs se croisent de manière à rendre la compréhension visuelle plus simple pour les réseaux les plus compliqués. La même procédure peut être

appliquée pour un AdD avec des branches répétées, le RB correspondant aura pour résultat des nœuds avec plus d'un lien, comme présenté dans les Figure 4.13 et 4.14.

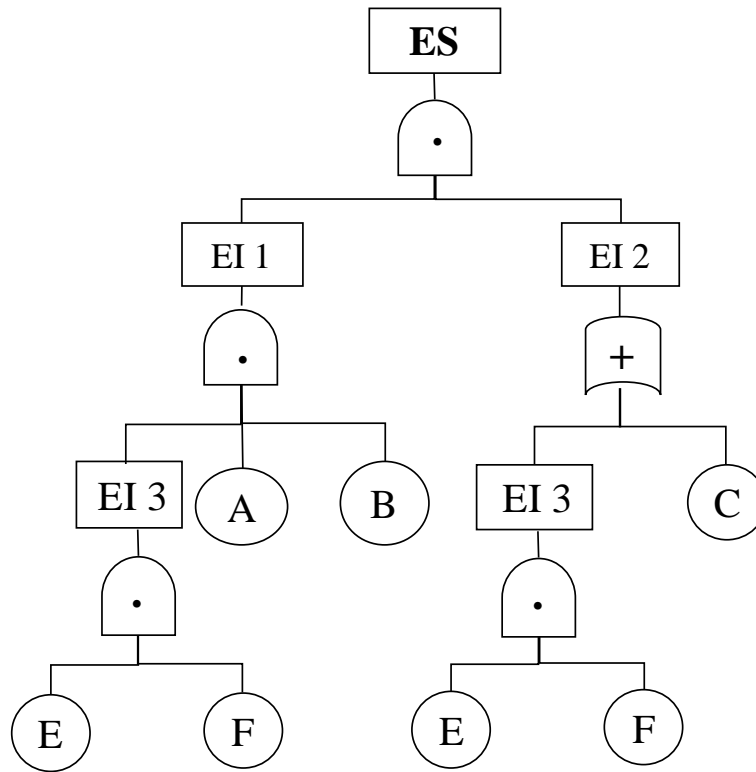


Figure 4.13 Arbre de défaillance avec une branche répétée

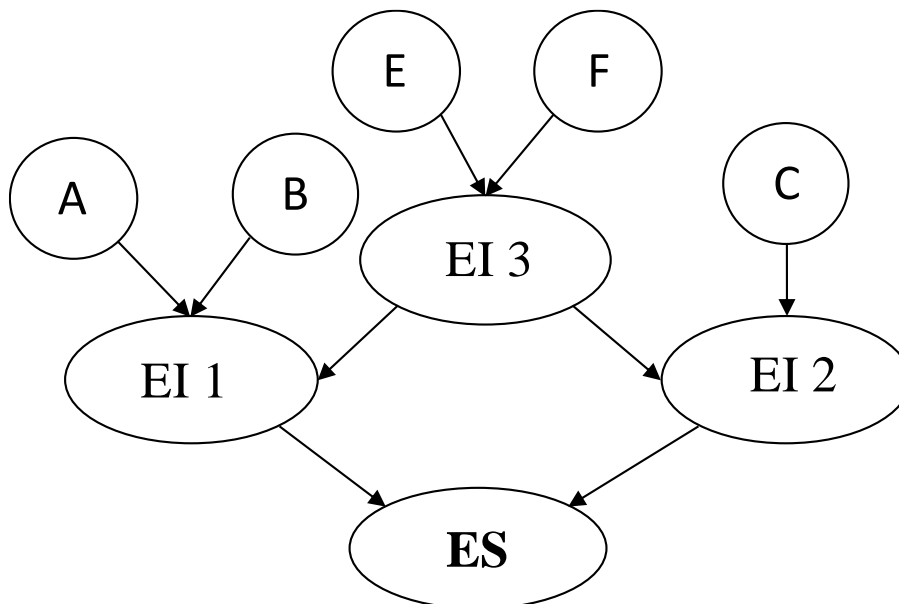


Figure 4.14 Réseau bayésien avec une branche répétée

4.3.2.3. L'inférence sur le RB obtenue à partir de AdD

Dans l'étude d'indisponibilité l'événement sommet dans l'AdD correspond à la probabilité à priori du nœud désigné nœud de défaillance dans le RB (la probabilité à posteriori est obtenue à partir de l'inférence dans le réseau) et c'est la même procédure pour les événements intermédiaire (sous système). Dans un AdD, les calculs d'indisponibilité sont obtenus à partir des coupes minimales, par contre dans les RB ils peuvent être obtenus par le concept d'inférence bayésienne. La règle de mise à jour des probabilités est donnée par la forme $P(H | e)$:

$$P(H | e) = \frac{P(e | H) \cdot P(H)}{P(e)} \quad (4.5)$$

$P(H)$ probabilité a priori, et $P(e | H)$, la probabilité que e se produise lorsque H est vraie, H représente la défaillance (ou bien les variables du sous-système) et l'évidence est l'ensemble vide, $e = \emptyset$. La probabilité à posteriori peut également être calculée dans un RB [FEN 13], [LAM 09], en prenant en considération un seul composant, un sous-ensemble de composants (sous-système) ou pour tous les composants, à l'exception de ceux auxquels des évidences ont été attribuées.

Quand la défaillance est donnée comme évidence, la probabilité à posteriori de chaque composant est une information de la criticité de chacun des composants et la probabilité posteriori d'un sous-système et une information de la criticité du sous-système qui est l'origine de la défaillance du système.

4.3.3. Facteur d'importance probabiliste en RB

Les facteurs d'importance probabilistes sont des mesures très importantes pour évaluer le rôle des composants qui contribuent dans l'occurrence de la défaillance du système. Par l'attribution d'une valeur numérique à chaque composant en termes de probabilité. Il serait facile de les classer selon leur criticité vis-à-vis l'évènement à étudier soit sommet ou bien intermédiaire afin de nous aider dans l'identification des parties critiques à prendre en considération dans le système. Ils peuvent être probabilistes ou déterministes selon s'ils impliquent ou non la probabilité du composant.

A partir du raisonnement de l'inférence sur les RB obtenus par AdD et les définitions des facteurs d'importance probabiliste en paragraphe § 2. Nous pouvons constater que le facteur de Birnbaum peut être obtenu à partir de l'équation 2. En termes de probabilité à posteriori par inférence sur le RB.

Et de ce fait, l'équation du facteur d'importance probabiliste de Birnbaum (Marginale) s'écrit de la forme :

$$I_i^B(t) = p_{(s=yes | i=yes)}(t) - p_{(s=yes | i=no)}(t) \quad (4.6)$$

Par conséquent, le facteur d'importance probabiliste Critique s'écrit de la forme :

$$I_i^{Cr}(t) = \frac{[p_{(s=yes | i=yes)}(t) - p_{(s=yes | i=no)}(t)] \cdot p_i(t)}{p_s(t)} \quad (4.7)$$

Avec : $p_{(s=yes | i=yes)}(t)$: la probabilité que le système est défaillant sachant que le composant 'i' est défaillant a l'instant 't' (a priori)

$p_{(s=yes | i=no)}(t)$: la probabilité que le système est défaillant sachant que le composant 'i' est en marche a l'instant 't' (posteriori).

$p_i(t)$: La probabilité du composant 'i' à l'instant 't'

et $p_s(t)$: La probabilité Système 's' à l'instant 't'.

4.4. Conclusion

Dans Ce chapitre un aperçu de littérature sur les réseaux bayésiens en générale d'une part et les réseaux bayésien pour l'analyse quantitative des risques d'autre part a été présenté.

Le réseau bayésien étant considéré comme une méthode d'analyse probabilistes des systèmes et ses composants, il a été fréquemment utilisé pour une étude plus approfondie pour son efficacité visuelle et conceptuelle afin de représenter les relations entre les défaillances et les pannes d'un système.

Le réseau bayésien a été choisi comme étant notre démarche d'aide à la décision pour les intérêts suivant :

Permet d'obtenir une connaissance enrichie, dont l'incertitude est plus faible : où la probabilité a posteriori représente la nouvelle connaissance pour l'analyste;

Ces applications dans l'industrie grâce au principe d'actualisation dynamique des connaissances, utilisé en particulier pour l'actualisation des bases de données sur les défaillances.

La possibilité de convertir l'arbre de défaillance en réseau bayésiens plus facilement et établir des analyses plus approfondies en utilisant des probabilités a priori obtenues par les méthodes d'analyse classiques, les bases des données, le retour d'expérience et le jugement d'experts.

L'inférence dans les réseaux bayésiens peut représenter les défaillances et pannes observés et les probabilités à posteriori permettent d'identifier les causes possibles. Ces probabilités peuvent être réutilisées comme probabilités de connaissance (à priori) pour une mise à jour du réseau.

Ainsi, ce chapitre comporte les aspects théoriques ainsi que notre contribution dans l'interprétation des facteurs d'importance dans les réseaux Bayésiens à partir desquels seront élaborées des méthodes destinées à l'étude de notre cas réels dans le domaine de l'analyse des risques des systèmes.

Chapitre V

FDMA du système déluge dans la zone de stockage du GPL

Sommaire du chapitre :

5.1. Introduction	70
5.2. Identification des Systèmes à étudier	70
5.2.1. Zone de stockage du GPL	70
5.2.1.1. Stockage sous pression	70
5.2.1.2. Scénarios et phénomènes dangereux dans la zone de stockage de GPL	72
5.2.1.3. Synthèse :	74
5.2.2. Le système déluge à eau comme barrière de sécurité	74
5.2.2.1. Description du système déluge à eau	74
5.2.2.2. Équipements et fonctionnement du système déluge à eau	74
5.3. Données d'étude de fiabilité du système déluge	76
5.4. Etude FDMA du système déluge à eau	77
5.4.1. Analyse des composants	77
5.4.2.1. AMDE des composants	77
5.4.2.2. Simulation de Monté Carlo	79
5.4.2.3. Fiabilité et disponibilité des composants	82
5.4.2.4. Analyse du système	92
5.4.2.4.1. Développement de l'arbre de défaillance	92
5.4.2.4.2. Fiabilité et disponibilité des sous-systèmes et du système	93
5.4.2.4.3. Coupes minimales et leurs importances	97
5.4.2.4.4. Facteurs d'importances probabilistes	98
5.5. Conclusion	101

5.1. Introduction

Dans ce chapitre, la modélisation d'un système déluge a été établie pour l'évaluation des performances relatives à la sûreté de fonctionnement. Où nous proposons à titre de référence l'étude du système déluge à eau installé comme étant une barrière de sécurité au niveau de la zone de stockage du GPL du projet ZCINA à Hassi Messaoud.

Les zones de stockage sont parmi les endroits où les scénarios les plus catastrophiques s'occurent, et ça comporte un produit fini destiné à la commercialisation car le GPL demeure l'un des piliers de l'économie en Algérie, un dispositif de prévention / intervention d'un très haut niveau de fiabilité, de disponibilité, de maintenabilité et de sécurité doit être assuré.

A cet effet, une méthodologie pour l'évaluation de la sûreté de fonctionnement du système déluge à eau est mise en œuvre. En premier lieu, une description de la zone de stockage du GPL et un aperçu sur les accidents les plus catastrophiques avec leurs probabilités d'occurrences obtenus grâce à l'analyse par arbre de défaillance afin de mettre en évidence le danger qui doit être maîtrisé par le système déluge à eau. Par la suite une étude de la fiabilité, disponibilité, maintenabilité et sécurité du système déluge à eau et mise en œuvre selon l'organigramme présenté en [Figure 5.1](#) avec comme principal but d'établir une analyse de fiabilité de chaque composant du système, les sous-systèmes clés dans le fonctionnement du système déluge et la contribution de chaque composant dans l'indisponibilité du système.

Les résultats obtenus comme synthèse de ce chapitre seront utilisés comme étant les données apriori pour l'élaboration d'un outil d'aide à la décision par les réseaux bayésiens dans le chapitre suivant.

5.2. Identification des Systèmes à étudier

5.2.1. Zone de stockage du GPL

5.2.1.1. Stockage sous pression

La zone de stockage du projet LPG ZCINA Hassi Messaoud comporte 4 sphères de stockage sous pression [Figure 5.2](#) d'une capacité totale de $500m^3$ contenant le GPL récupéré du débutaniseur (la dernière chaîne de liquéfaction dans le train de séparation). Stocké sous-pression de 15 à 21 *barg* et une température qui dépasse les $40^{\circ}c$ le GPL serai par la suite acheminé par 2 pompes centrifuge pour être expédié vers la station de pompage hors complexe.

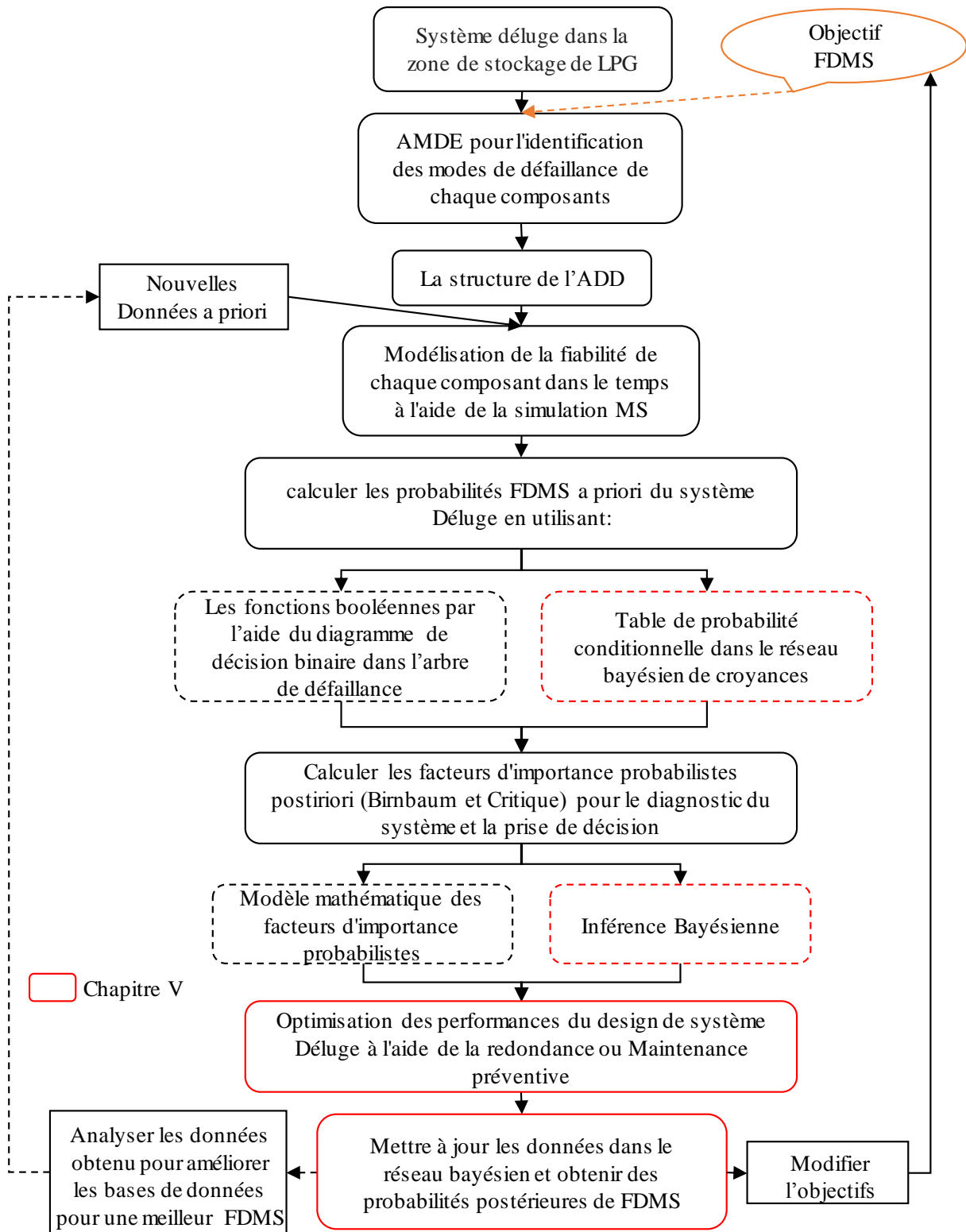


Figure 5.1 Organigramme représentant la démarche de l'évaluation de la sûreté de fonctionnement du système

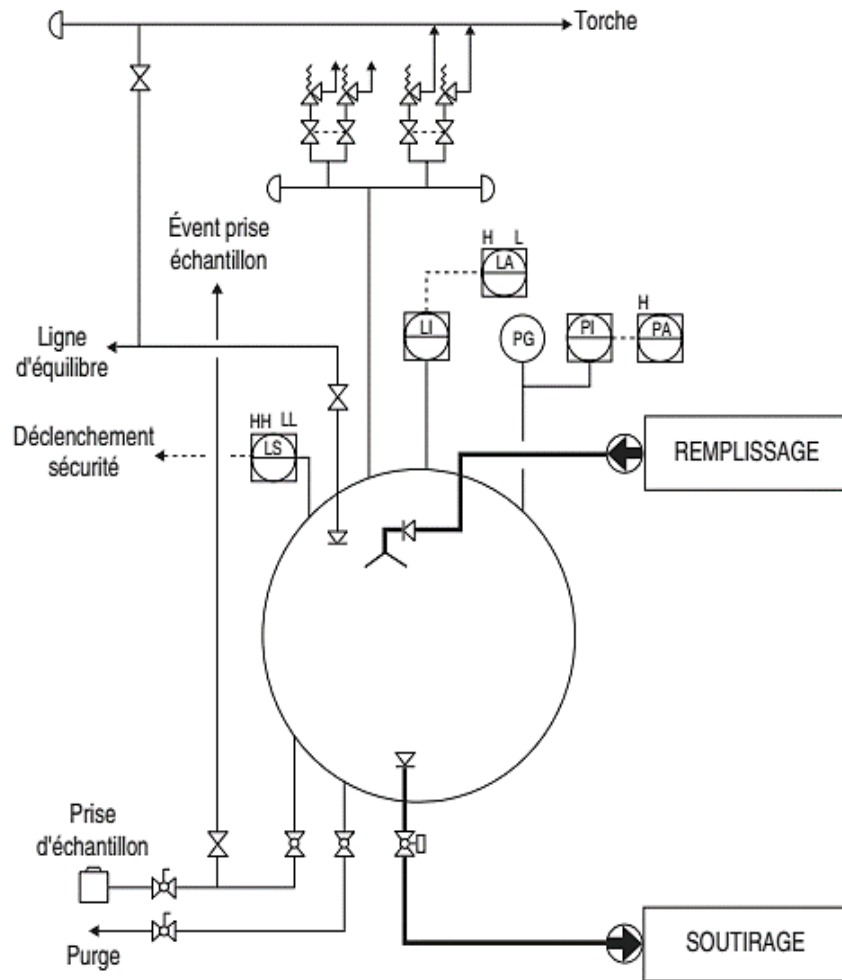


Figure 5.2 Schéma pour décrire les éléments importants composants une sphère de stockage du GPL

5.2.1.2. Scénarios et phénomènes dangereux dans la zone de stockage de GPL

Suite aux résultats des études HAZOP et HAZID établis par des bureaux d'études, la principale cause, dite évènement initiateur, est la perte de confinement par rupture, grande fuite, moyenne fuite ou bien petite fuite de la/les sphère(s) avec des fortes probabilités d'être suivi d'ignition immédiate, Ignition retardée ou bien carrément une explosion [MAN 05], [OLF 04]. Le [Tableau 5.1](#) présente les probabilités d'occurrence de ces derniers. Comme conséquence des scénarios et phénomènes dangereux catastrophiques inhérents tels que (feu de nappe, feu de chalumeau, Ball de feu, explosion de nuage de vapeur VCE) [ALS 14], [MAN 05] peuvent être le déclenchement du phénomène de BLEVE ainsi que l'effet domino [LAB 12], [ABD11], [DAR 10], [MAN 05], [SAN 05], [GUI 92]. La [Figure 5.3](#) présente l'arbre d'évènement développé comme étant notre 1^{ère} démarche d'analyse quantitative des risques pour obtenir les probabilités d'occurrence en [Tableau 5.2](#) des scénarios catastrophiques les plus redoutés.

Tableau 5.1 Probabilités d'occurrence des évènements qui peuvent survenir suite à une perte de confinement au niveau de la zone de stockage du GPL. [MAN 05], [OLF 04]

	Ignition immédiate	Ignition retardée	Explosion
Rupture 2.56 E-6/an	0.7	0.7	0.4
Grande fuite 4.40 E-6/an	0.7	0.7	0.4
Moyenne fuite 4.40 E-6/an	0.5	0.2	0.3
Petite fuite 2.48 E-4/an	0.2	0.06	0.2

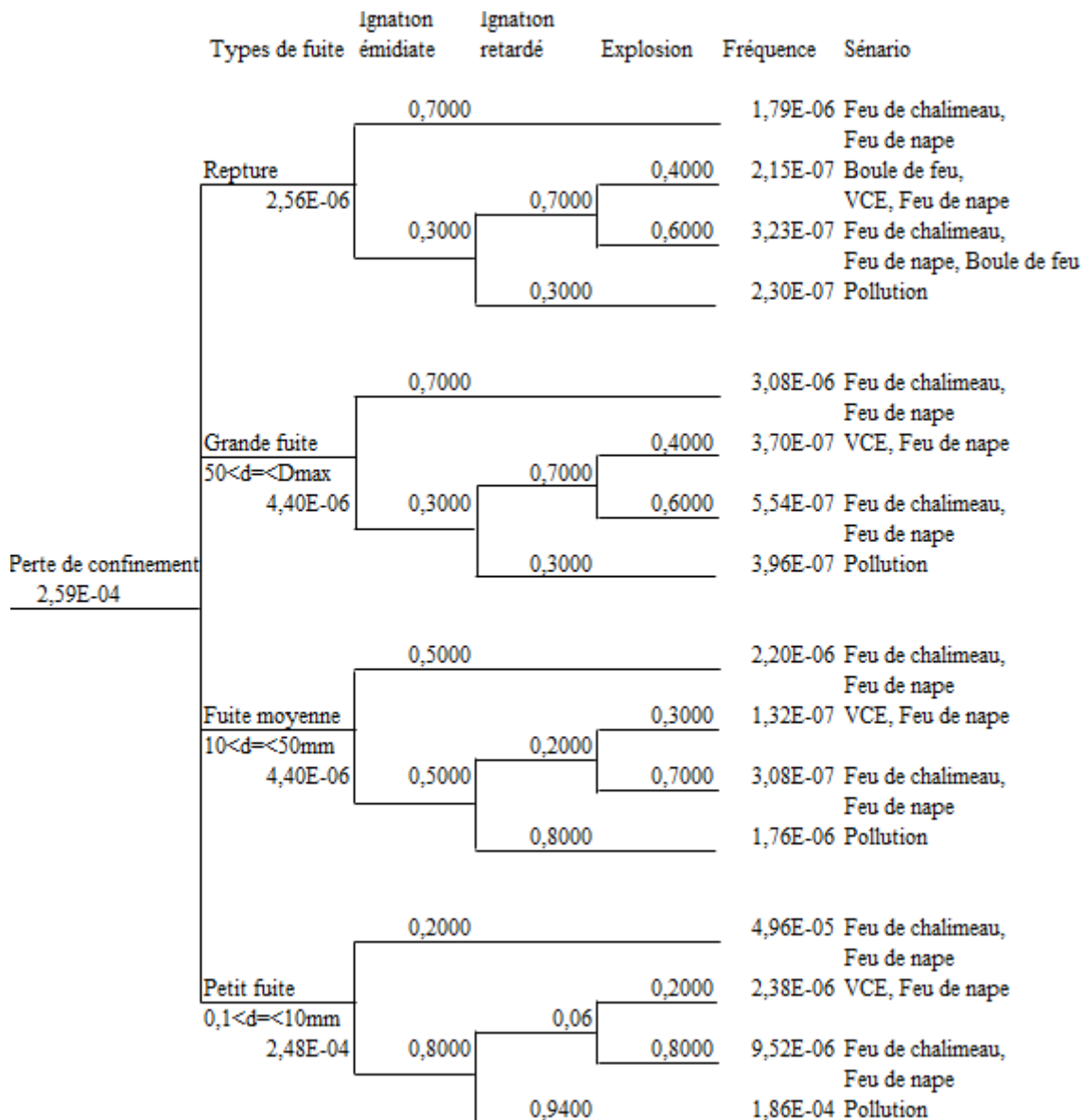


Figure 5.3 Arbre d'évènement des scénarios catastrophiques dans la zone de stockage de GPL

Tableau 5.2 Fréquences d'occurrences des Scénarios catastrophiques dans la zone de stockage du GPL

Scénario catastrophique	Fréquence d'occurrence /an
Feu de nape (flaque de feu)	7.05E-5
Feu de chalimeau (Feu de torche)	6.74E-5
Boule de feu	2.12E-6
VCE	3.10E-6
Pollution	1.89E-4

5.2.1.3. Synthèse :

A partir de l'analyse par Arbre de défaillance, il a été constaté que les fréquences d'occurrence des scénarios catastrophiques sont minimales mais toujours probables et leurs survenus peuvent engendrer des graves dégâts sur l'homme, sur les installations et l'environnement avoisinant causant de graves pertes économiques. À cet effet, il ne faut pas négliger la totale sécurité au niveau de ces zones de stockage, d'où l'importance d'un dispositif de sécurité performant qui peut assurer la prévention ainsi que l'intervention afin de diminuer les dégâts.

5.2.2. Le système déluge à eau comme barrière de sécurité

5.2.2.1. Description du système déluge à eau

Le complexe pétrolier de GPL se trouve au voisinage de plusieurs autres complexes et près de la ville de Hassi Messaoud où les températures sont souvent élevées. De ce fait, le système déluge à eau [Figure 5.4](#) joue plusieurs rôles importants [GUE 18], [NOL 14], [BEL 07], [ROB 04], [VAN 00], [GUI 92], parmi lesquels il est supposé fournir, à la demande, par un système de vote composé de 2 out-of 3 détecteurs, de l'eau à une pression contrôlée à la zone de stockage de LPG afin de réduire la charge calorifique d'un incendie, le flux de chaleur sur les installations ainsi que la création d'un rideau d'eau pour éviter / limiter la propagation d'un incendie [INC 10].

Cependant, le système déluge à eau est un système qui assure ces fonctions à partir du réseau anti incendie général du complexe pétrolier.

5.2.2.2. Équipements et fonctionnement du système déluge à eau

L'usine GPL ZCINA dispose d'un système d'eau incendie comprenant deux réservoirs de stockage d'eau incendie, une pomperie incendie et un réseau de distribution d'eau incendie maillé et enterré.

L'eau provenant du puits et de l'extérieur du site est stockée dans deux réservoirs d'une capacité de 14 000 m³ avec une autonomie de 12 chacun. Le système pomperie comporte plusieurs pompes redondantes [JEN 07] calculé pour le scénario le plus défavorable. Le dimensionnement est considéré pour la demande en eau correspond à un feu sur une sphère de stockage de GPL. Ce scénario de feu nécessite un débit d'eau de 930 m³/h, afin d'assurer ce débit d'eau {deux pompes jockey (2x100%) 30 m³/h à 8 barg, deux pompes électriques (2x50) 550m³/h à 10 barg et une pompe diesel (1*100) 1100m³/h à 10barg}. La 1^{ère} pompe jockey marche à plein temps pour maintenir le réseau sous pression, les autres pompes interviennent soit automatiquement par le système Feu et gaz en cas de détection de feu confirmée par 2 détecteurs parmi les 3 ou bien par le transmetteur de pression en cas de basse pression dans le réseau selon des étapes bien définies ou bien manuellement par l'opérateur à partir de la salle de contrôle ou bien sur site. En même temps que le système de détection feu et gaz envoi le signal aux pompes, il actionne aussi la vanne déluge (électrovanne à émission) pour que l'eau puisse passer vers les buses du système déluge (sprinkler [LAK 10], [NEI 07]). Afin de maintenir le niveau de pression dans l'anneau principal, des dispositifs de pression sont installés.

La Figure 5.5 montre une image explicative simplifiée des importants composants du système déluge à eau.

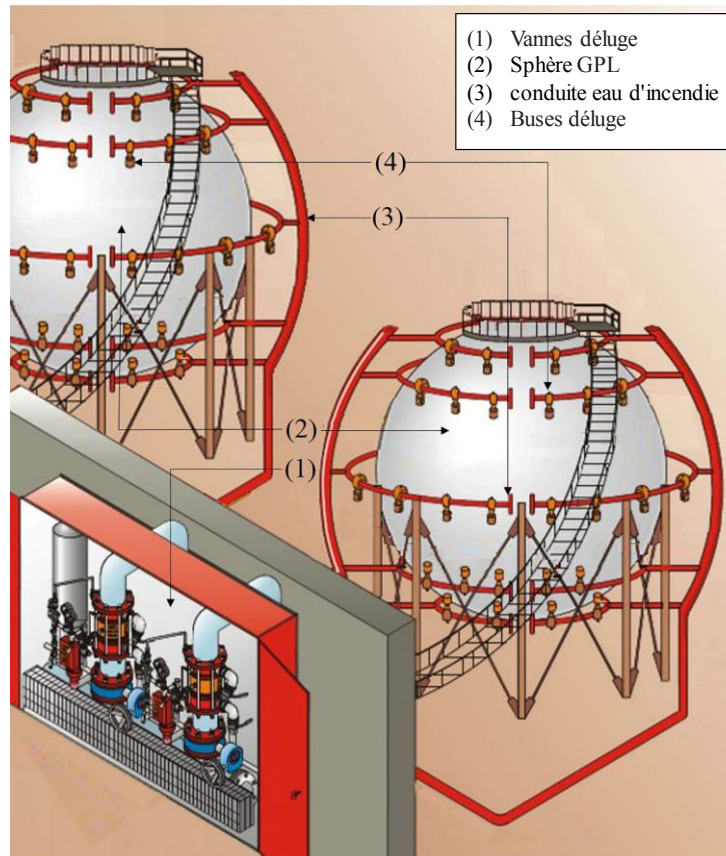


Figure 5.4 Système déluge à eau installé sur une sphère de GPL

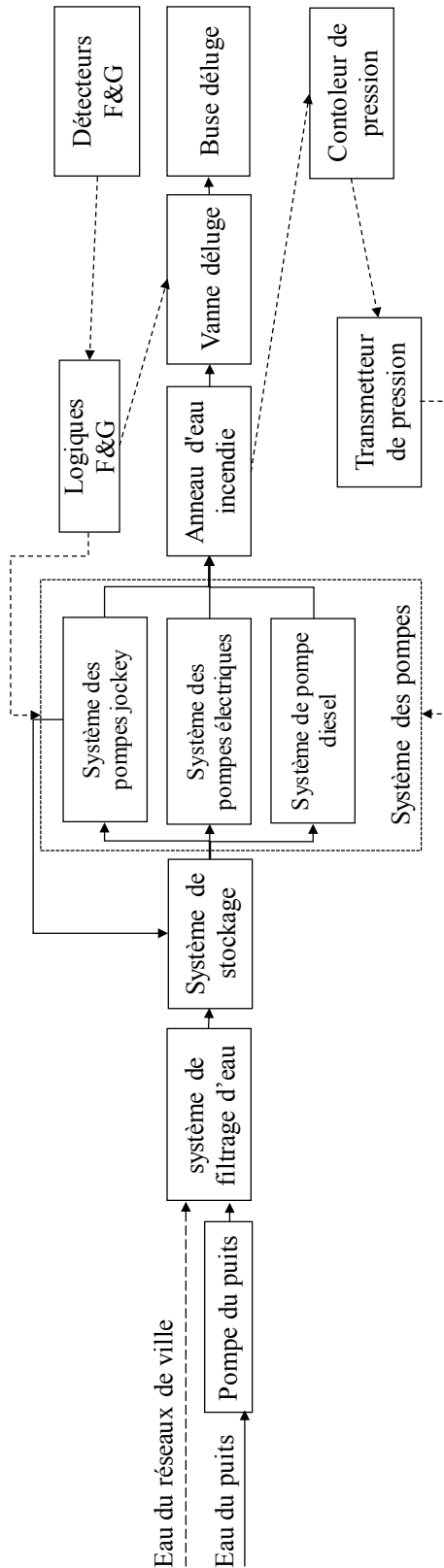


Figure 5.5 Schéma simplifié des équipements du système déluge à eau

5.3. Données d'étude de fiabilité du système déluge

Les données des paramètres de fiabilité utiles pour la réalisation de ce travail (taux de défaillance, écart type, taux de réparation, ...) ont été sélectionnées selon les modes de

défaillance des équipements du système déluge à eau à partir de la base de donnée [MAN 05], [SIN 02] regroupées dans le [Tableau 5.3](#) qui suit en fonction des modèles de fiabilité caractérisant chaque composant qui fera objet d'étude dans ce qui suit.

Tableau 5.3 Données de fiabilité des composants du système de déluge d'eau [MAN 05], [SIN 02]

Nœud	Composant	Paramètres	
		$(\lambda, \sigma), \tau, t_0$ (SPT)	$(\lambda, \sigma), \mu, \tau, t_0$ (EPT)
N1	La vanne déluge ne s'ouvre pas à la demande	P(1)=5.223E-3	
N2	Blocage de la buse ou débit réduit	P(2)=1.0E-6	
N3, N4, N5	Détecteur de flamme 1, 2, 3 /	(5.9E-7, 5.9E-7), 3.39E5, 4	
N6, N9 / N12, N15 / N18	Défaillance de la pompe jockey 1, 2 / électrique 1, 2 / diesel	(1.7E-6, 2.48E-6), 2E-2, 1.471E5, 1.471E5	
N7, N10, N13, N16, N31	Défaillance du moteur électrique 1, 2, 3, 4, 5	(1.473E-6, 1.123E-5), 1.054E-2, 1.697 E4, 1.697 E4	
N8	Défaillance du capteur de pression	(5.3E-6, 7.55E-6), 3.774E4, 48	
N11, N14, N17, N19	La pompe ne démarre pas à la demande	P(11, 14, 17, 19,)=2.84E-3	
N20	Défaillance du moteur diesel	(1.466E-5, 1.274E-5), 0.1639, 1.705E4, 1.705E4	
N21	Rupture du Bac de stockage A	P(21)=2.89E-7	
N22	Blocage de la vanne manuelle en position fermée	(5.074E-5, 5.074E-5), 8.403E-2, 4.927E3, 4.927E3	
N23	Erreur humaine	P(23)=0.01	
N24, N25	Filtre A / B défaillant	(3.805E-5, 3.805E-5), 6.897E-2, 6.57E3	
N26, N29	Vanne Glob 1 / 2 défaillante	(6.34E-6, 1.996E-5), 3.704E-2, 3.943E4, 3.943E4	
N27	Défaillance du capteur de niveau	(9.2E-7, 1.26E-6), 2.174E5, 48	
N28, N33	La vanne automatique 1 / 2 ne s'ouvre pas	(5.93E-6, 5.93E-6), 0.1667, 42160, 42160	
N30	Défaillance de la pompe du puits	(1.026E-5, 9.32E-6), 6.258E-3, 2.437E4, 2.437E4	
N32	La pompe du puits ne démarre pas à la demande	P(32)= 6E-3	

5.4. Etude FDMA du système déluge à eau

5.4.1. Analyse des composants

5.4.1.1. AMDE des composants

Une Analyse des modes de défaillance et de leurs effets (AMDE) de chaque composant du système a été requise pour définir les modes de défaillance des composants et sélectionner ceux qui feront l'objet d'une étude de sûreté de fonctionnement approfondie.

Comme étant les tableaux générés par l'analyse par AMDE contiennent un nombre très important de données, un extrait de ce tableau est présenté en [Tableau 5.4](#) avec quelques composants pour le but d'expliquer la démarche d'analyse par AMDE.

Tableau 5.4 Extrait d'AMDE de quelques composants du systèmes déluge a eau

Phase opérationnelle:									
Compo sant	Mode de Défaillance	Causes de Défaillance	Effets des Défaillances			Sauvegardes ou Détections	Recommandations	Notes	
			Local (sous- système)	Réseau anti- incendie	La zone de Stockage GPL				
N1	Ne s'ouvre pas	Bloquée fermée (rouille, calcaire, systèmes solénoïde (électromécaniqu e) ne fonctionne	Pas de passage d'eau	La partie déluge de la zone de stockage ne fonctionne pas	Pas de protection	Systèmes de détection des flammes	Maintenance préventive et testes régulières	Systèmes de détection des flammes marche	
			Passage d'eau réduit	La partie déluge de la zone de stockage ne fonctionne temporairement pas assez de pression	protection limité	capteur de pression	Inspection des équipes		
N2	Colmatées	Rouille, calcaire	Le rideau d'eau ne protège pas tous les équipements	la partie déluge de la zone de stockage ne fonctionne temporairement pas assez correctement	Zone peut protégé	/	Inspection, utiliser les larges diamètres de pulvérisation pour minimiser le colmatage	le nombre des buse installé est important d'où l'influence est minime	

Synthèse :

Une sélection des composants selon des modes de défaillance les plus influenceurs sur le bon fonctionnement du système déluge à eau a été établie, pour une analyse probabiliste beaucoup plus approfondie en passant par l'étude FDMS de chaque équipement suivie d'une étude de système par le biais de l'arbre de défaillance.

5.4.1.2. Simulation de Monté Carlo

Les données sélectionnées à partir de OREDA [SIN 02] représentent des écarts types importants suite aux différentes conditions (emplacement de l'équipement, sa qualité, son fonctionnement ...) de récolte des données, cependant la simulation de Monté Carlo comme étant un modèle établi pour l'étude de continuité dans le temps de la fiabilité d'un système ainsi que par la propagation d'incertitude sur les résultats par le principe d'échantillonnage, elle a permis l'obtention des résultats convergents.

Les approximations des résultats en temps continu sont obtenues sur le résultat de chaque composant et ainsi de suite jusqu'à l'obtention du résultat final en utilisant le modèle de distribution normal en équation (5.1), où l'estimation du taux de défaillance est donnée à la fois sous l'hypothèse multi-échantillon et sous l'hypothèse d'ensemble de données homogènes. L'incertitude du taux de défaillance λ est présentée sous la forme d'un intervalle de confiance de 90% couvrant 90% de la variation entre les échantillons multiples, de sorte que la valeur réelle est : $Pr(\lambda_{5\%} \leq \lambda < \lambda_{95\%}) = 90\%$ comme recommandé par la base de données OREDA [SIN 02].

$$f_{\mu,\sigma}(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\left(\frac{(t-\mu)^2}{2\sigma^2}\right)} \quad (5.1)$$

Sachant que : ' μ ' est la moyenne du taux de défaillance et ' σ ' l'écart type

Plusieurs essais avec des nombres d'échantillons différents sur la probabilité d'indisponibilité ainsi que sur l'écart type à des axes de temps prédéfinis (1 ans, 5ans et 10ans) ont été établis sur le modèle afin de définir le nombre d'échantillons minimal à partir duquel les résultats convergent. Les [Figures 5.6, 5.8 et 5.10](#) représentent la variation de l'indisponibilité du système par rapport au nombre d'échantillons et les [Figures 5.7, 5.9 et 5.11](#) représentent la variation de l'écart type du système par rapport au nombre d'échantillons.

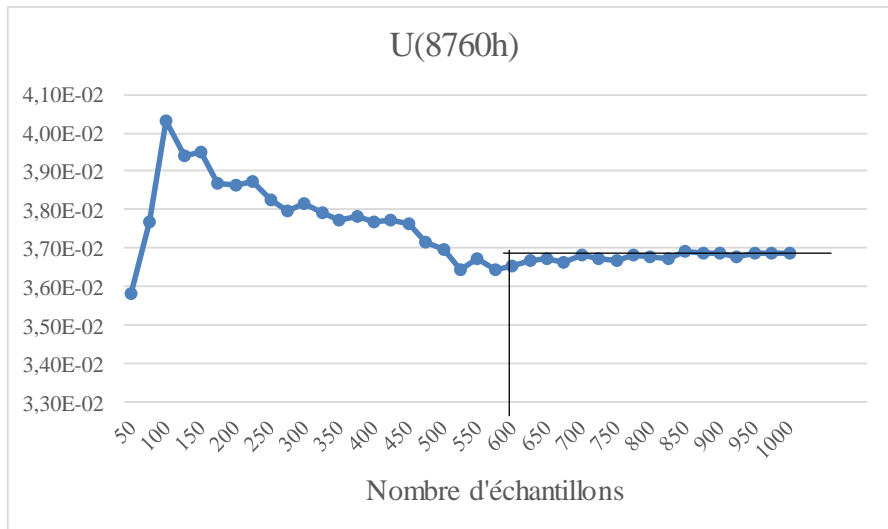


Figure 5.6 Variation de l'indisponibilité du système a $t= 8760h$ par rapport au nombre d'échantillons

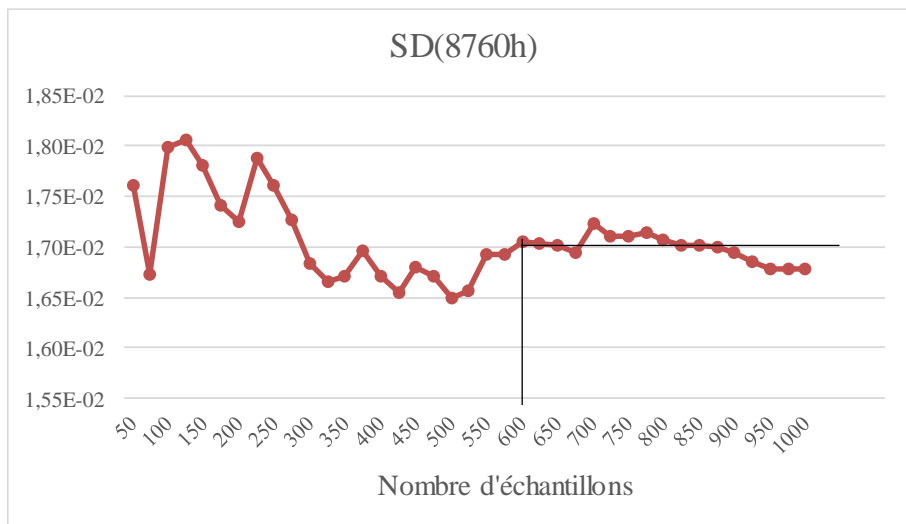


Figure 5.7 Variation de l'écart type du système a $t= 8760h$ par rapport au nombre d'échantillons

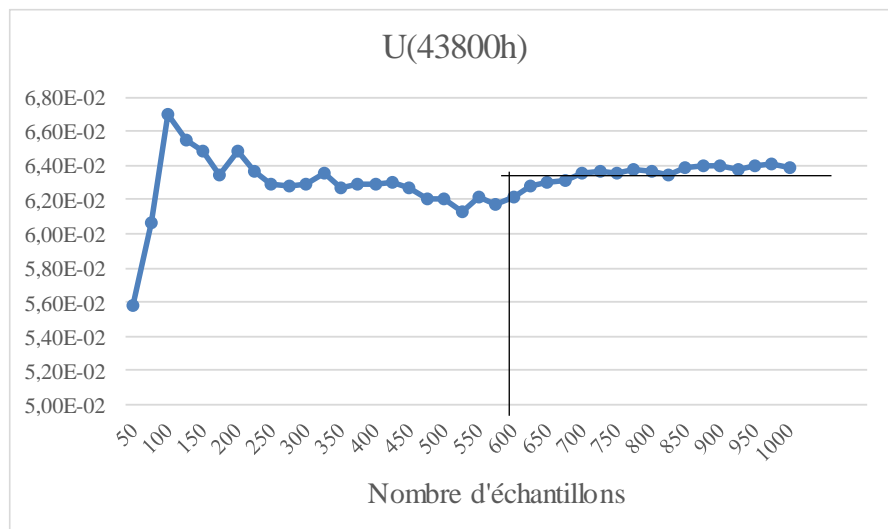


Figure 5.8 Variation de l'indisponibilité du système a $t= 43800h$ par rapport au nombre d'échantillons

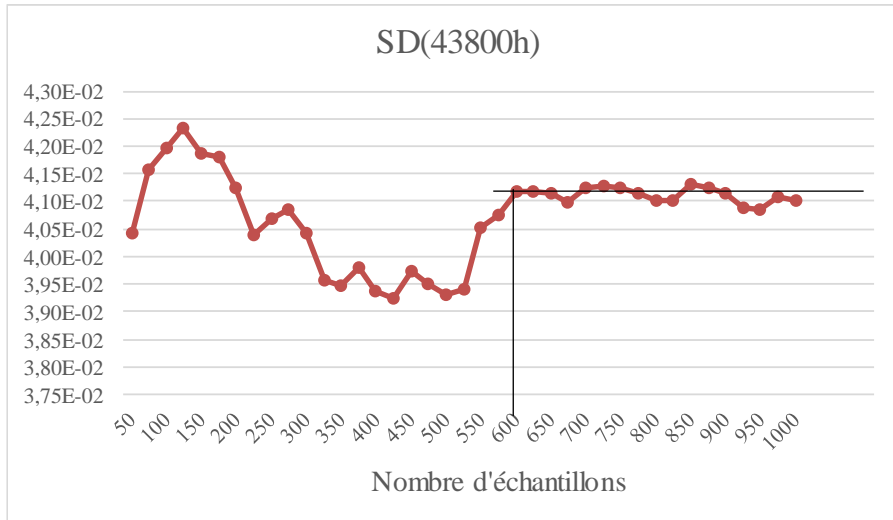


Figure 5.9 Variation de l'écart type du système a t= 43800h par rapport au nombre d'échantillons

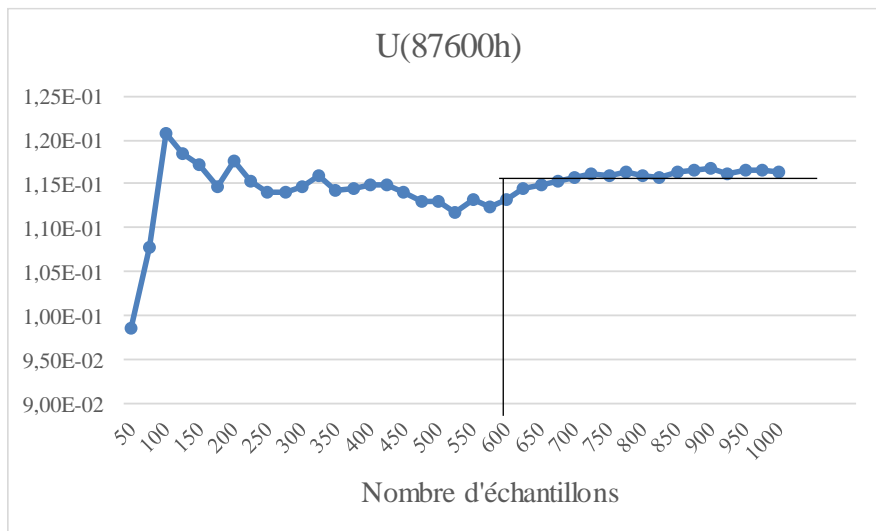


Figure 5.10 Variation de l'indisponibilité du système a t= 87600h par rapport au nombre d'échantillons

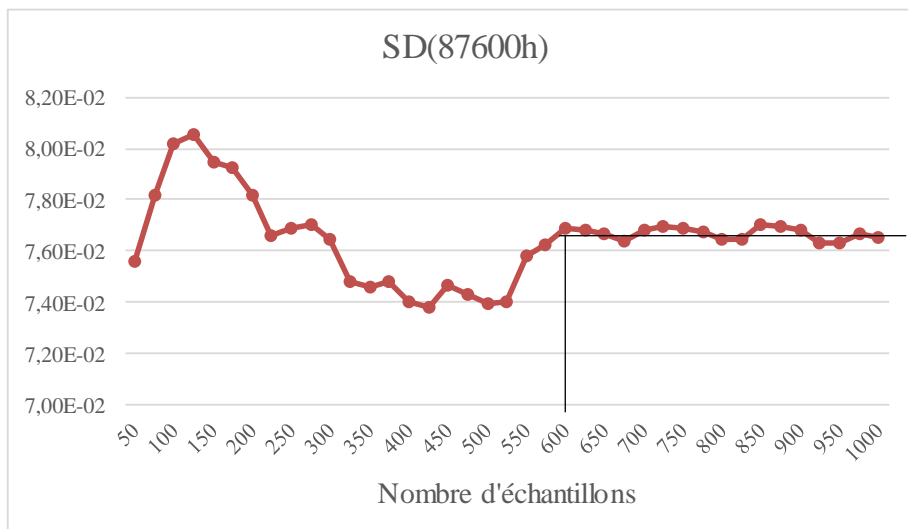


Figure 5.11 Variation de l'écart type du système a t= 87600h par rapport au nombre d'échantillons

Synthèse : Le nombre d'échantillons retenus pour toutes les simulations de fiabilité qui vont suivre, obtenue à partir des Figures de 5.6 jusqu'au 5.11, est de 600 échantillons, la valeur minimale à partir de laquelle les résultats convergent sachant que le temps de simulation est considérable avec un nombre plus élevé.

5.4.1.3. Fiabilité et disponibilité des composants

- **Composants avec probabilité Constante**

- ✓ Vanne déluge : comme étant une nouvelle technologie récemment installée dans les complexes industriels, elle n'a pas été couverte par les bases de données et à partir des avis d'experts et de plusieurs études, la probabilité de défaillance d'une vanne déluge est estimée à $P=5.223E-3$.
- ✓ Buses d'eau (sprinklers) : représentent un nombre important, installées sur les équipements afin de couvrir toute la zone à protéger et leurs probabilités de défaillance est vraiment rare estimée à $P=1.0E-6$.
- ✓ Bac de stockage d'eau : La rupture d'un bac de stockage dépend de l'infrastructure sur laquelle repose ce bac et des matériaux de construction, selon le cas d'étude la valeur de rupture du bac est de $P=2.89E-7$.

- **Composants électroniques**

Les composants électroniques installés sur le système sont des équipements d'une très grande importance car ils commandent le système selon un raisonnement logique et la disponibilité du système déluge à eau dépend du bon fonctionnement de ces équipements.

Comme étant des équipements testés non réparables, le modèle mathématique du teste périodique simple (TPS) (5.2) obtenu à partir de l'équation générale (2.8) modélise la disponibilité du système ainsi que la fiabilité rapprochée.

$$U(t) = \begin{cases} 1 - e^{-\lambda.t}, & \text{if } t < t_0 \\ 1 - e^{-\lambda.[(t-t_0) \bmod \tau]}, & \text{otherwise} \end{cases} \quad (5.2)$$

Où ' λ ' est le taux de défaillance, ' τ ' période de test (intervalle de temps entre deux tests consécutifs) et ' t_0 ' temps du 1er teste. $1 - e^{-\lambda.t} \cong \lambda.t$ if $\lambda.t < 10\%$

Le modulaire arithmétique de cette expression exponentielle est utilisé pour représenter un composant qui tombe en panne selon une loi de distribution exponentielle et dont on constate la panne lors d'un test périodique. Le changement d'équipement s'effectue ensuite de façon instantanée.

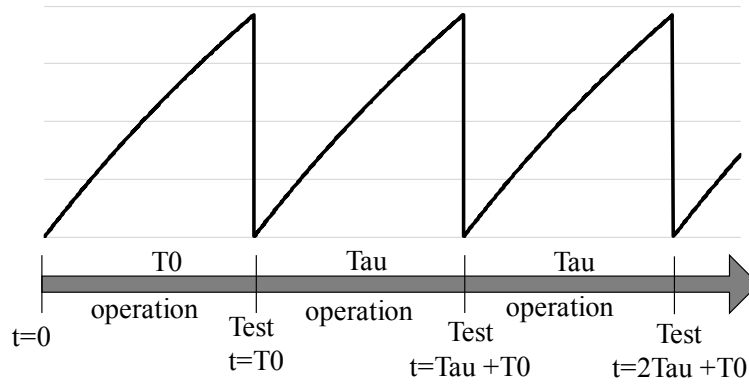


Figure 5.12 Modèle d'indisponibilité représentant la durée de vie d'un composant par teste périodique simple

Les résultats concernant les métriques de la sûreté de fonctionnement (MTTF, MDT, MUT et MTBF) de chaque composant ainsi que de la disponibilité et fiabilité approximative sont obtenus pour chaque composant.

✓ Détecteur de flamme

Tableau 5.5 Métriques de la sûreté de fonctionnement du détecteur de flamme

MTTF	MDT	MUT	MTBF
1,730E+06	4,861E+04	1,764E+06	1,813E+06

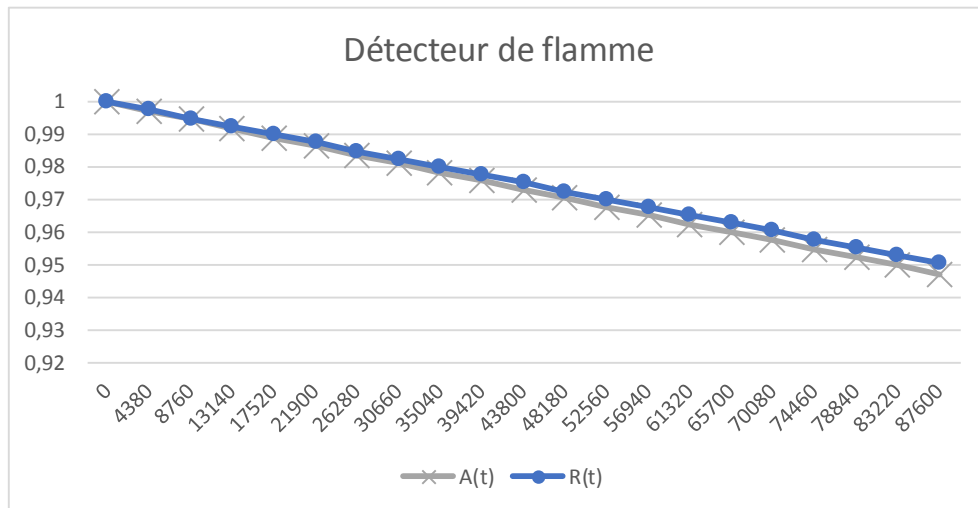


Figure 4.13 Disponibilité et fiabilité du détecteur de flamme

Tableau 5.6 Résumé de disponibilité et de fiabilité du détecteur de flamme

$A(t)_{\text{moy}}$	$A(87600\text{h})$	$R(t)_{\text{moy}}$	$R(87600\text{h})$
0,973	0,947	0,975	0,951

✓ Capteur de pression

Tableau 5.7 Métriques de la sûreté de fonctionnement du capteur de pression

MTTF	MDT	MUT	MTBF
1,942E+05	2,210E+04	2,137E+05	2,358E+05

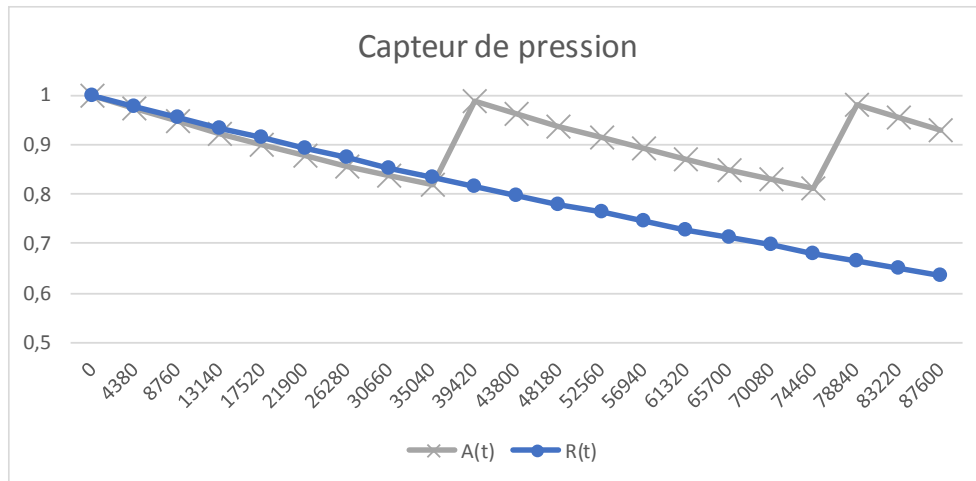


Figure 5.14 Disponibilité et fiabilité du capteur de pression

Tableau 5.8 Résumé de disponibilité et de fiabilité du capteur de pression

A(t) _{moy}	A(87600h)	R(t) _{moy}	R(87600h)
0,905	0,929	0,805	0,637

✓ Capteur de niveau

Tableau 5.9 Métriques de la sûreté de fonctionnement du capteur de niveau

MTTF	MDT	MUT	MTBF
1,12E+06	5,11E+04	1,10E+06	1,15E+06

Tableau 5.10 Résumé de disponibilité et de fiabilité du capteur de niveau

A(t) _{moy}	A(87600h)	R(t) _{moy}	R(87600h)
0,956	0,914	0,962	0,925

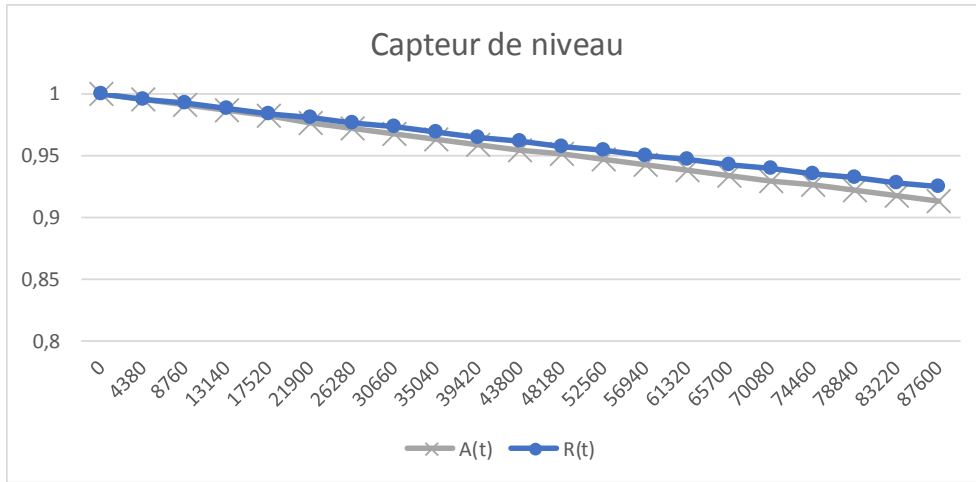


Figure 5.15 Disponibilité et fiabilité du capteur de niveau

Synthèse : à partir des résultats obtenus pour les 3 équipements on constate que le temps jusqu'à la 1ère défaillance est plus important par rapport au temps de simulation d'où les composants sont relativement plus fiables sur l'intervalle de (temps de simulation 10ans) et que la disponibilité et la fiabilité est la même que ce soit pour les détecteurs de flamme (Figure 5.13) ou bien le capteur de niveau (Figure 5.15). Par contre le capteur de pression représente une courte durée entre les défaillances par rapport aux 2 autres composant d'où on remarque que la disponibilité est supérieure à la fiabilité parce que après chaque test si l'équipement est défaillant il sera changé et considéré comme étant disponible à nouveau (Figure 5.14).

- **Composants mécaniques et électromécanique**

Les composants mécaniques et électromécaniques du système sont des équipements qui marchent en interaction entre eux et avec tous les équipements du système afin d'assurer un bon fonctionnement du système.

Comme étant ces équipements testés et réparables, le modèle mathématique du test périodique étendu (TPE) (5.3) obtenu à partir de l'équation générale (2.8) modélise la disponibilité du système ainsi que la fiabilité rapprochée.

$$U(t) = \begin{cases} \frac{\lambda}{\lambda + \mu} \cdot (1 - e^{-(\lambda + \mu) \cdot t}), & \text{if } t < t_0 \\ \frac{\lambda}{\lambda + \mu} \cdot (1 - e^{-(\lambda + \mu) \cdot [(t - t_0) \bmod \tau]}), & \text{otherwise} \end{cases} \quad (5.3)$$

Où 'λ' est le taux de défaillance, 'μ' taux de réparation (une fois qu'un test a mis en évidence la panne) 'τ' période de test (intervalle de temps entre deux tests consécutifs) et 't₀' temps du 1er test. $\lambda/(\lambda + \mu) \cdot (1 - e^{-(\lambda + \mu) \cdot t}) \cong \lambda/(\lambda + \mu)$ si $t = 4/5$ de MTTR ou $\cong \lambda/\mu$ si $\lambda \ll \mu$

Le modulaire arithmétique de cette expression exponentielle est utilisé pour représenter un composant qui tombe en panne selon une loi de distribution exponentielle et dont on constate

la panne lors d'un test périodique. La phase de réparation est ensuite modélisée par une exponentielle de paramètre μ

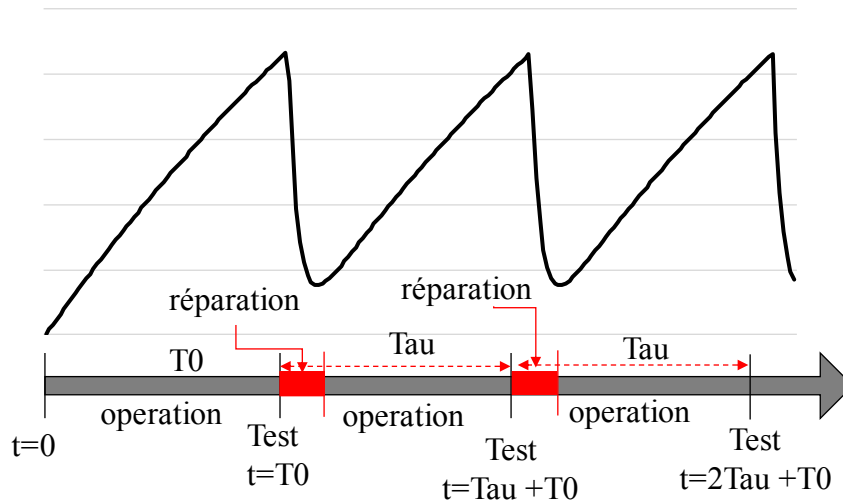


Figure 5.16 Modèle d'indisponibilité représentant la durée de vie d'un composant par test périodique étendu

✓ Pompe anti incendie

Tableau 5.11 Métriques de la sûreté de fonctionnement de la pompe anti incendie

MTTF	MDT	MUT	MTBF
6,059E+05	5,584E+04	6,430E+05	6,989E+05

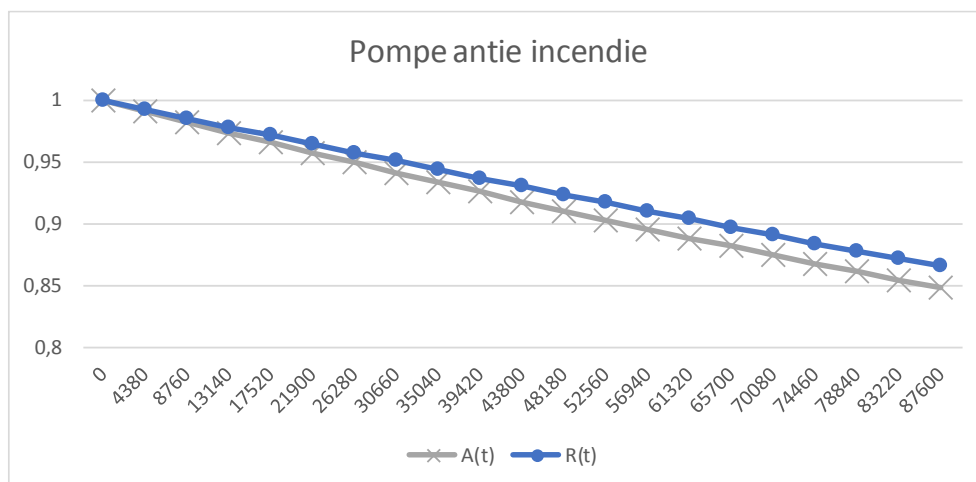


Figure 5.16 Disponibilité et fiabilité de la pompe anti incendie

Tableau 5.12 Résumé de disponibilité et de fiabilité de la pompe anti incendie

A(t) _{moy}	A(87600h)	R(t) _{moy}	R(87600h)
0,920	0,848	0,931	0,865

✓ Moteur électrique

Tableau 5.13 Métriques de la sûreté de fonctionnement du moteur électrique

MTTF	MDT	MUT	MTBF
6,059E+05	5,748E+04	6,620E+05	7,194E+05

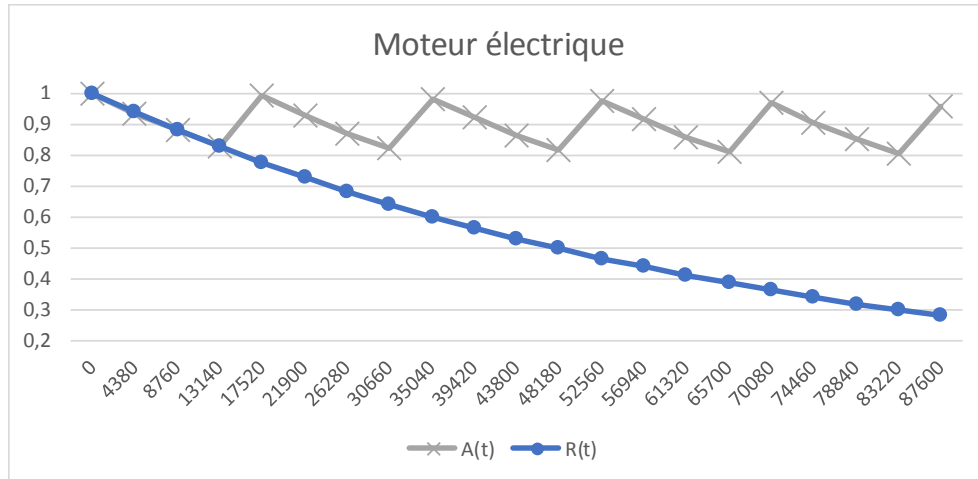


Figure 5.17 Disponibilité et fiabilité du moteur électrique

Tableau 5.14 Résumé de disponibilité et de fiabilité du moteur électrique

$A(t)_{\text{moy}}$	$A(87600\text{h})$	$R(t)_{\text{moy}}$	$R(87600\text{h})$
0,896	0,960	0,566	0,281

✓ Moteur Diesel

Tableau 5.15 Métriques de la sûreté de fonctionnement du moteur diesel

MTTF	MDT	MUT	MTBF
6,942E+04	9,159E+03	7,256E+04	8,172E+04

Tableau 5.16 Résumé de disponibilité et de fiabilité du moteur diesel

$A(t)_{\text{moy}}$	$A(87600\text{h})$	$R(t)_{\text{moy}}$	$R(87600\text{h})$
0,897	0,965	0,568	0,283

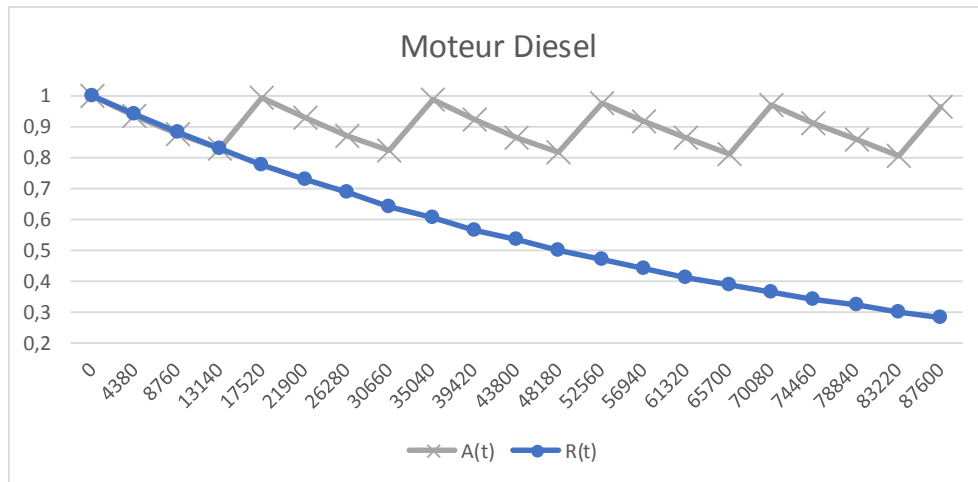


Figure 5.18 Disponibilité et fiabilité du moteur diesel

✓ Vanne manuelle

Tableau 5.17 Métriques de la sûreté de fonctionnement de la vanne manuelle

MTTF	MDT	MUT	MTBF
2,011E+04	4,029E+03	2,171E+04	2,574E+04

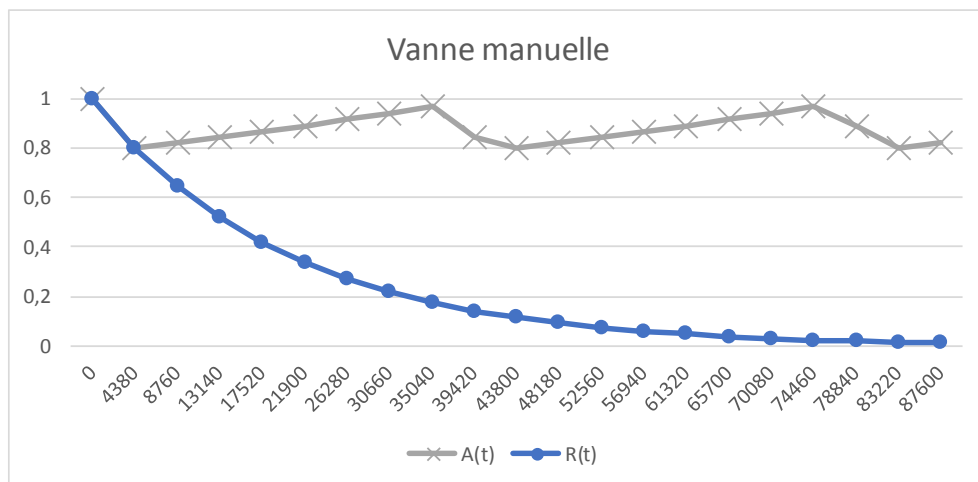


Figure 5.19 Disponibilité et fiabilité de la vanne manuelle

Tableau 5.18 Résumé de disponibilité et de fiabilité de la vanne manuelle

A(t) _{moy}	A(87600h)	R(t) _{moy}	R(87600h)
0,823	0,878	0,013	0,228

✓ Filtre d'eau

Tableau 5.19 Métriques de la sûreté de fonctionnement du filtre d'eau

MTTF	MDT	MUT	MTBF
2,682E+04	5,796E+03	3,085E+04	3,665E+04

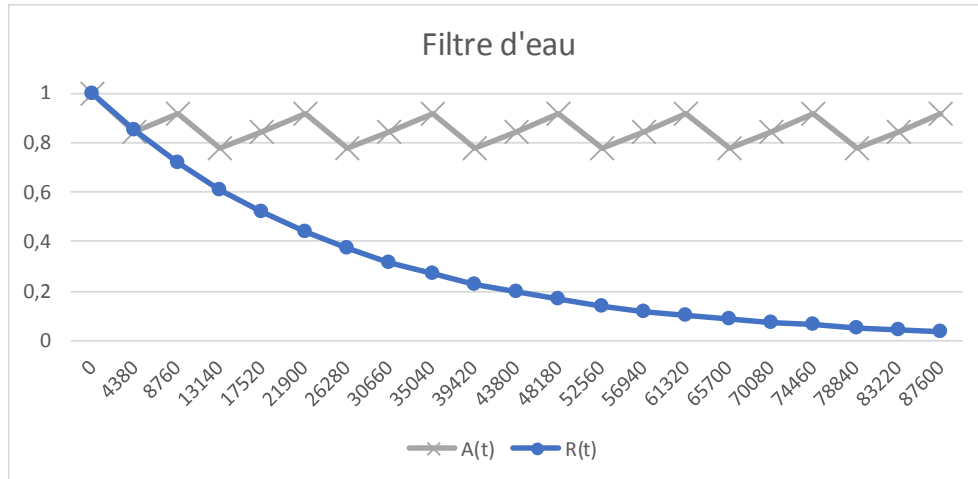


Figure 5.20 Disponibilité et fiabilité du filtre d'eau

Tableau 5.20 Résumé de disponibilité et de fiabilité du filtre d'eau

$A(t)_{\text{moy}}$	$A(87600\text{h})$	$R(t)_{\text{moy}}$	$R(87600\text{h})$
0,853	0,917	0,295	0,038

✓ Vanne globe

Tableau 5.21 Métriques de la sûreté de fonctionnement de la vanne globe

MTTF	MDT	MUT	MTBF
1,683E+05	8,032E+04	4,257E+05	5,061E+05

Tableau 5.22 Résumé de disponibilité et de fiabilité de la vanne globe

$A(t)_{\text{moy}}$	$A(87600\text{h})$	$R(t)_{\text{moy}}$	$R(87600\text{h})$
0,833	0,912	0,780	0,594

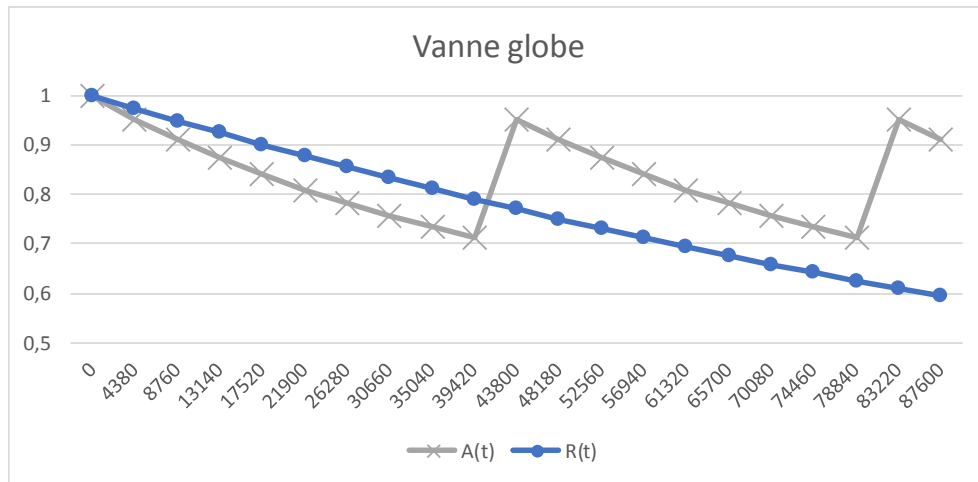


Figure 5.21 Disponibilité et fiabilité de la vanne globe

✓ Vanne automatique

Tableau 5.23 Métriques de la sûreté de fonctionnement de la vanne automatique

MTTF	MDT	MUT	MTBF
1,721E+05	2,405E+04	1,895E+05	2,136E+05

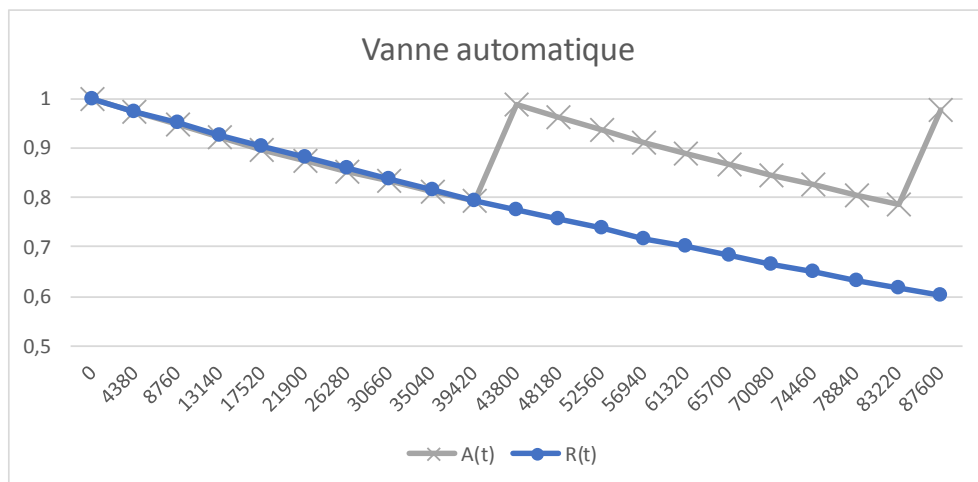


Figure 5.22 Disponibilité et fiabilité de la vanne automatique

Tableau 5.24 Résumé de disponibilité et de fiabilité de la vanne automatique

A(t) _{moy}	A(87600h)	R(t) _{moy}	R(87600h)
0,886	0,980	0,784	0,601

✓ Pompe de puit

Tableau 5.25 Métriques de la sûreté de fonctionnement de la pompe du puit

MTTF	MDT	MUT	MTBF
9,927E+04	1,298E+04	1,058E+05	1,188E+05

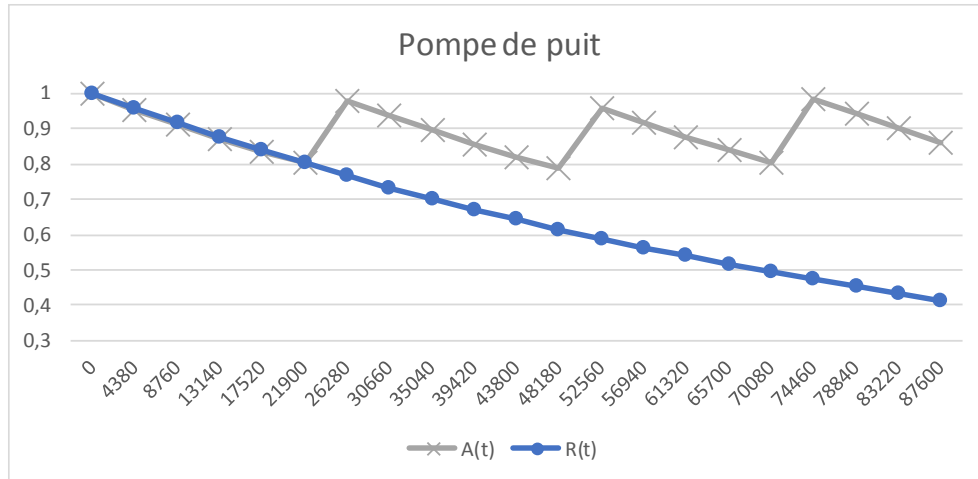


Figure 5.23 Disponibilité et fiabilité de la pompe du puit

Tableau 5.26 Résumé de disponibilité et de fiabilité de la pompe du puit

A(t) _{moy}	A(87600h)	R(t) _{moy}	R(87600h)
0,891	0,862	0,664	0,414

Synthèse :

Les résultats obtenus par la simulation de fiabilité sur les équipements mécaniques et électromécaniques ont montré d’une manière générale que la fiabilité et la disponibilité sont équivalentes avant le premier test, la disponibilité augmente de nouveau suite à l’opération de maintenance. Par contre, la fiabilité est toujours en diminution d’où on peut dire que la disponibilité est supérieure à la fiabilité après les réparations apportées aux équipements ce qui est normal (par ce qu’un équipement maintenu est considéré comme étant disponible mais moins fiable qu’un nouveau.)

Les résultats de la pompe anti incendie représentés en [Figure 5.16](#) ne montrent aucune augmentation de la disponibilité par rapport aux autres équipements [Figure 5.17](#) jusqu’au [5.23](#). Cela est dû au temps jusqu’à la 1ère défaillance de la pompe qui est important par rapport au temps de la simulation c’est pour cela que la pompe est relativement fiable vis-à-vis des autres composants.

Par comparaison entre les composants mécaniques ou bien électromécaniques par rapport aux composants électroniques on constate que durant le temps de simulation de 10ans les équipements électromécaniques sont plus fiables et c'est dû au fonctionnement de chaque équipement, la conception de l'équipement et surtout son emplacement sur terrain (environnement avoisinant).

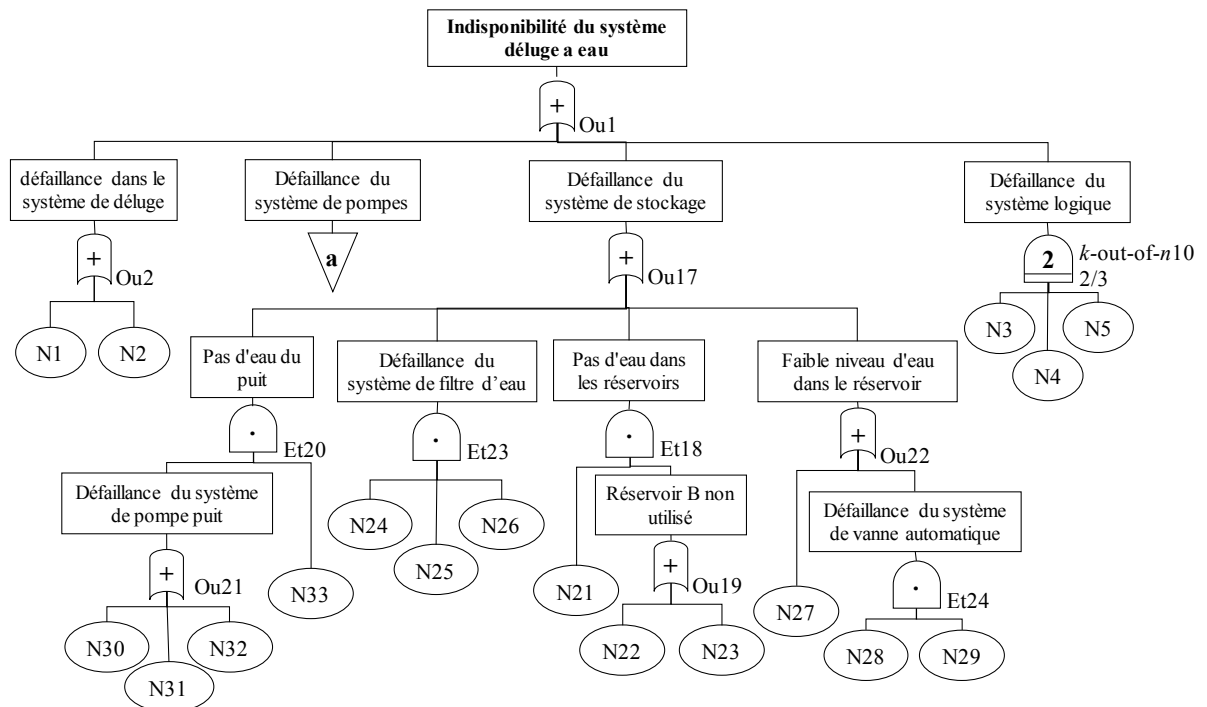
5.4.1.4. Analyse du système

5.4.1.4.1. Développement de l'arbre de défaillance

Le développement de la structure de l'arbre de défaillance a été établi comme le montre la Figure 5.24 selon la littérature présentée en §3.3.2 et en concordance avec la Figure 5.5.

La structure pour l'étude d'indisponibilité du système déluge à eau se base essentiellement sur 4 sous-systèmes. Pour clarifier la structure complexe : la défaillance du système déluge (caractérisée par la vanne déluge et les buses d'eau), la défaillance du système des pompes (caractérisée par les différentes pompes en redondance, leurs moteurs et capteur de pression), la défaillance du système de stockage (caractérisée par l'arrivée d'eau jusqu'au bac de stockage) ou bien par défaillance du système de détection des flammes (caractérisée par les détecteurs de flamme). Ces 4 sous-systèmes contribuent directement sur l'occurrence de l'événement sommet et sont connectés avec ce dernier via une porte 'ou'.

Les composants des sous-systèmes sont répertoriés dans le Tableau 5.3 et sont connectés par les portes logiques 'et', 'ou' et 'k-sur-n',



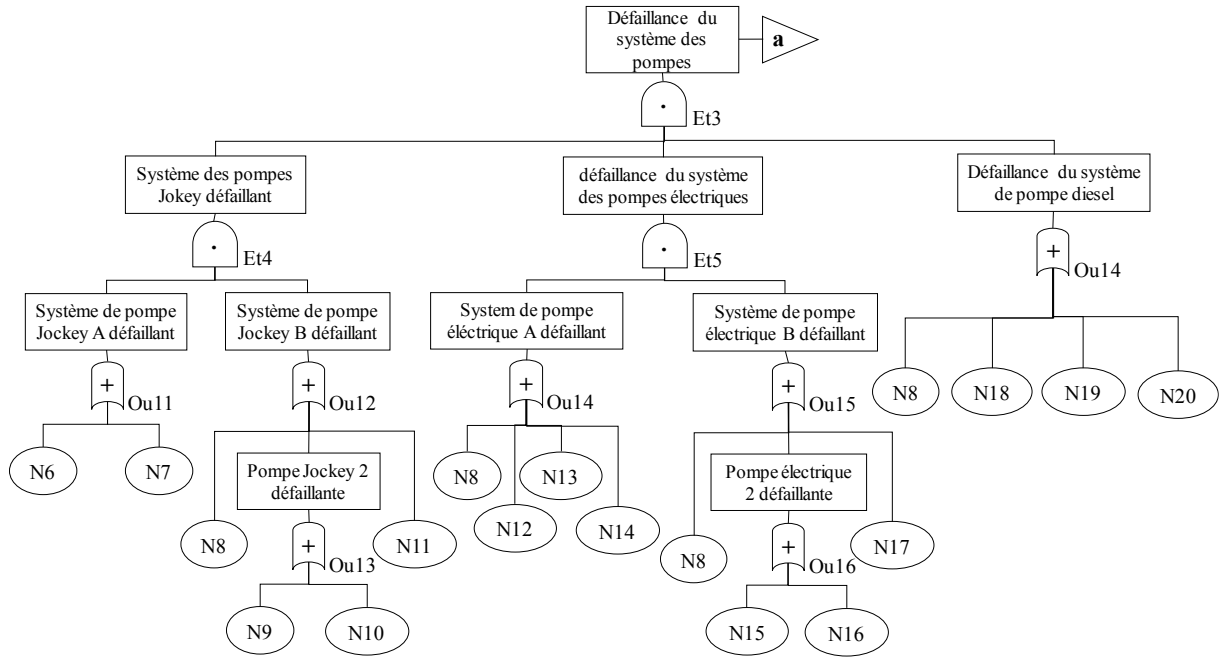


Figure 5.24 La structure de l'arbre de défaillance du système déluge à eau avec l'extension de la défaillance du sous-système des pompes en (a), où les événements de base sont énumérés dans le [Tableau 5.3](#)

5.4.1.4.2. Fiabilité et disponibilité des sous-systèmes et du système

✓ Système logique

Tableau 5.27 Métriques de la sûreté de fonctionnement du système logique de détection

MTTF	MDT	MUT	MTBF
1,163E+07	3,179E+04	1,135E+07	1,138E+07

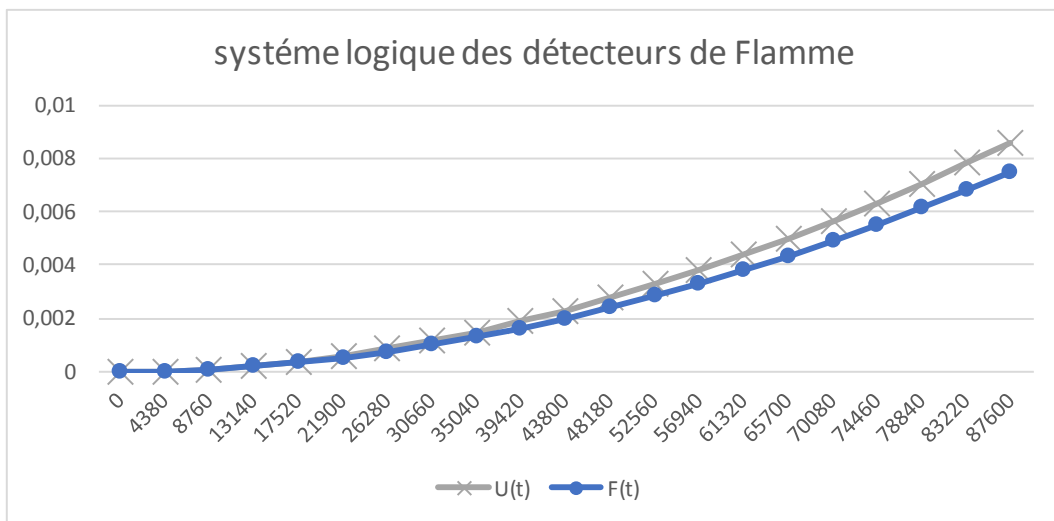


Figure 5.25 Indisponibilité et défiabilité du système logique de détection

Tableau 5.28 Résumé de disponibilité et de fiabilité du système logique de détection

A(t) _{moy}	A(87600h)	R(t) _{moy}	R(87600h)
0,997	0,991	0,997	0,997

✓ Système de pompage

Tableau 5.29 Métriques de la sûreté de fonctionnement du système de pompes

MTTF	MDT	MUT	MTBF
4,715E+05	9,061E+03	4,783E+05	4,873E+05

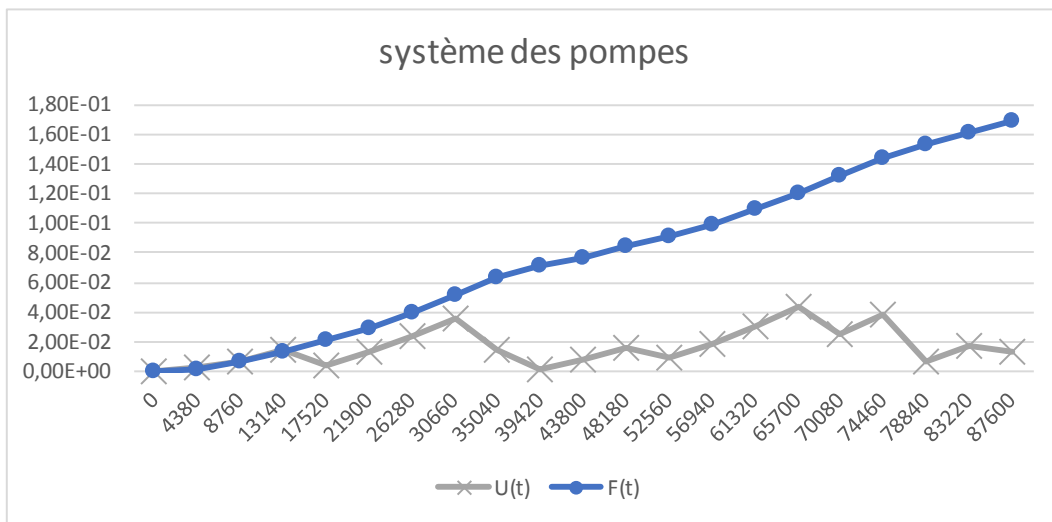


Figure 5.26 Indisponibilité et défiabilité du système de pompes

Tableau 5.30 Résumé de disponibilité et de fiabilité du système logique de détection

A(t) _{moy}	A(87600h)	R(t) _{moy}	R(87600h)
0,981	0,987	0,922	0,830

✓ Système de stockage

Tableau 5.31 Métriques de la sûreté de fonctionnement du système de stockage

MTTF	MDT	MUT	MTBF
1,480E+05	1,698E+04	1,653E+05	1,823E+05

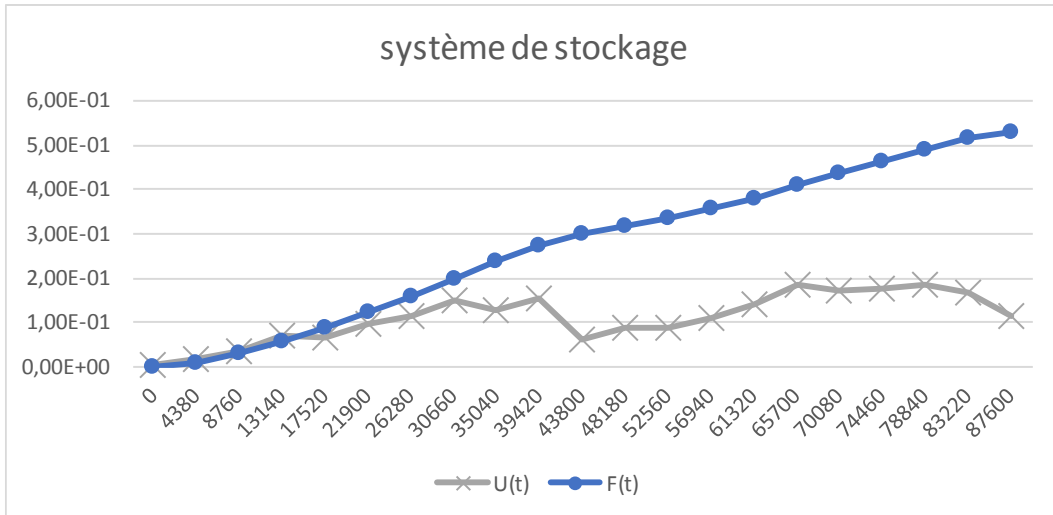


Figure 5.27 Indisponibilité et défiabilité du système de stockage

Tableau 5.32 Résumé de disponibilité et de fiabilité du système de stockage

A(t) _{moy}	A(87600h)	R(t) _{moy}	R(87600h)
0,907	0,911	0,774	0,553

✓ Système déluge à eau

Tableau 5.33 Métriques de la sûreté de fonctionnement du système déluge

MTTF	MDT	MUT	MTBF
1,159E+05	1,560E+04	1,225E+05	1,381E+05

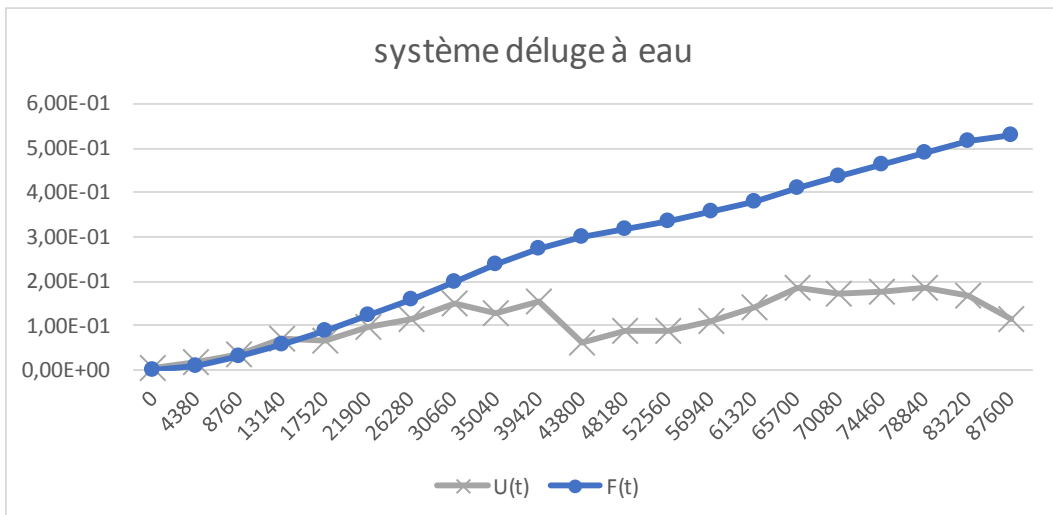


Figure 5.28 Indisponibilité et défiabilité du système déluge à eau

Tableau 5.34 Résumé de disponibilité et de fiabilité du système déluge

A(t) _{moy}	A(87600h)	R(t) _{moy}	R(87600h)
0,887	0,887	0,728	0,530

Synthèse : à partir des résultats obtenus par simulation sur les sous-systèmes ainsi que le système en [Figure 5.26](#), [5.27](#) et [5.28](#), il a été remarqué malgré la fiabilité des composants durant les 10ans s'est réduite, mais leurs fonctionnements en interaction dans le système, a fait que la fiabilité des sous-systèmes jusqu'à la fiabilité du système est considérable suite aux redondances des équipements ou bien les bypass. Les probabilités de défaillance des événements intermédiaires et l'indisponibilité du système déluge à eau installé dans la zone de stockage du GPL sont calculées par l'expression booléenne obtenue à l'aide de BDD. Les résultats d'indisponibilité du système obtenus à l'aide du logiciel GRIF® [GRI 18] sur une durée de mission de 87 600 h par simulation DDB et la simulation de MC ont été présentés au long de l'analyse de sureté de fonctionnement. Le [Tableau 5.35](#) résume les probabilités de chaque évènement intermédiaire à l'instant t=87 600h.

Le temps de simulation de 87 600h a été utilisé dans les calculs en tenant compte du fait que le système déluge à eau est disponible sur demande, quels que soient les scénarios, pour les raisons suivantes :

1. Redondance des composants importants, si le 1er composant est en phase de réparation, le 2ème le remplace ;
2. Essais périodiques et dispositifs de maintenance [LIN 02] ;
3. Phase de réparation, lorsque la défaillance est détectée, les composants soient retournés comme s'ils étaient dans leur état d'origine.

L'importance du système déluge a fait que malgré sa disponibilité moyenne de 88,7% avec une fiabilité approximative moyenne de 72,8% il faut prévoir une optimisation des performances du design pour le but d'augmenter encore plus la disponibilité sur tout pour une barrière de prévention/intervention tel que le système déluge à eau.

A cet effet, plusieurs méthodes et modèles mathématiques ont pour but de trouver les coupes minimales ainsi que les composants qui contribuent à l'indisponibilité du système.

Tableau 5.35 évènement intermédiaire et sous-systèmes

Nœud	Nom	U(t=87600h)
Ou1	Indisponibilité du système déluge à eau	0.1132
Ou2	Défaillance du système déluge	5.2210E-3
Et3	Défaillance du système de pompes	1.2764E-2
Et4	Le système de pompes Jockey défaillant	4.3972E-2
Et5	Défaillance du système de pompes électriques	0.1008
Ou6	Défaillance du système de pompe diesel	0.2481
KsurN10	Défaillance du système logique de détection de flamme	8.6211E-3
Ou11	Système de pompe Jockey A défaillant	0.1797
Ou12	Système de pompe Jockey B défaillant	0.2453
Ou13	Pompe jockey 2 défaillante	0.1881
Ou14	Système de pompe électrique A défaillant	0.2474
Ou15	Le système de pompe électrique B ne démarre pas	0.2393
Ou16	Pompe électrique 2 défaillante	0.1811
Ou17	Défaillance du système de stockage	8.9160E-2
Et18	Pas d'eau dans les réservoirs	5.3194E-8
Ou19	Réservoir B non utilisé	0.1841
Et20	Pas d'eau du puits	3.6516E-3
Ou21	Le système de pompe puits défaillant	0.1823
Ou22	Faible niveau d'eau dans le réservoir	8.5331E-2
Et23	Défaillance du système de filtrage	5.6092E-4
Et24	Défaillance du système de vannes automatique	1.8535E-3

5.4.1.4.3. Coupes minimales et leurs importances

La structure de l'arbre de défaillance comme étant complexe, elle représente 177 coupes minimales où là plupart des coupes minimales sont d'ordre 5 avec 3 coupes d'ordre 1 qui contribuent à 79.93% dans l'indisponibilité du système [Tableau 5.36](#). Ces 3 coupes doivent être prises en considération pour qu'elles ne soient pas les principaux composants qui contribuent le plus à l'indisponibilité du système. Parmi ces 3 coupes il y'a les buses d'eau, leur probabilité d'occurrence est vraiment faible à cause de leurs nombres importants, donc on s'intéressera beaucoup plus aux autres composants soit le capteur de niveau ainsi que la vanne déluge ainsi que d'autres composants qui contribuent dans d'autres coupes avec des ordres (niveaux) différents et qui seront déterminés par les modèles mathématiques beaucoup plus approfondis.

Tableau 5.36 nombre de coupes minimales et leurs contributions dans l'événement sommet avec exemple d'indisponibilité de la grande coupe minimale dans chaque ordre à t = 87600 h

Ordre	Nombre	Probabilité de produits	Exemples	
			Produits	Probabilité de produits
1	3	79.93%	N27	7.739E-02
2	11	19.66%	N6,N8	8.575E-03
3	1	0.33%	N24,N25,N26	3.434E-04
5	162	0.07%	N6,N9,N12,N15,N18	5.071E-05

5.4.1.4.4. Facteurs d'importances probabilistes

Suite à une analyse détaillée des données obtenues par les approches précédentes, 4 composants ont été retenus pour étudier leurs contributions dans l'indisponibilité du système par le modèle facteur d'importance probabiliste marginale par l'équation 5.3 ainsi que facteur d'importance probabiliste critique par l'équation 5.4. Ces 4 composants sont 'la vanne déluge, capteur de pression, capteur de niveau et la vanne automatique moyenne'.

$$I_i^B(t) = p_{(s|i)}(t) - p_{(s|\bar{i})}(t) \tag{5.3}$$

$$I_i^{CR}(t) = \frac{p_i(t)}{p_s(t)} \times I_i^B(t) \text{ for } i = 1, 2, \dots, n \tag{5.4}$$

Les résultats obtenus par les facteurs d'importances probabilistes à l'instant t= 8760h Figure 4.29 et 4.31 ainsi que ceux obtenus à l'instant t= 87600 Figure 4.30 et 4.32 montrent que chaque équipement influence sur le système à des axes de temps définis selon la disponibilité de l'équipement. D'où on ne peut pas prendre des décisions bien déterminées que si on calcule les facteurs d'importances en fonction du temps.

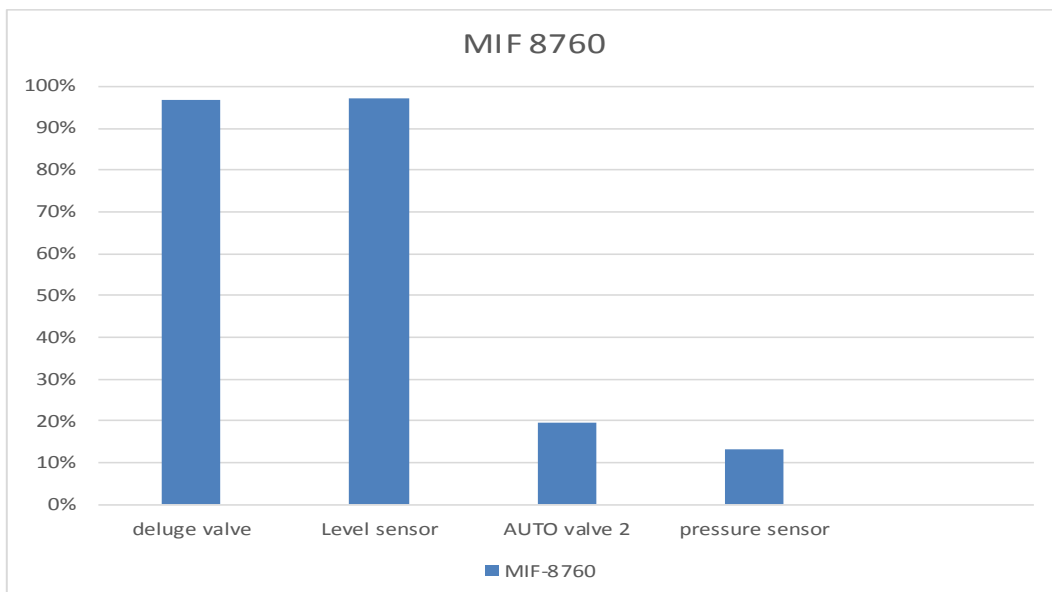


Figure 5.29 Facteur d'importance marginale à 8760h

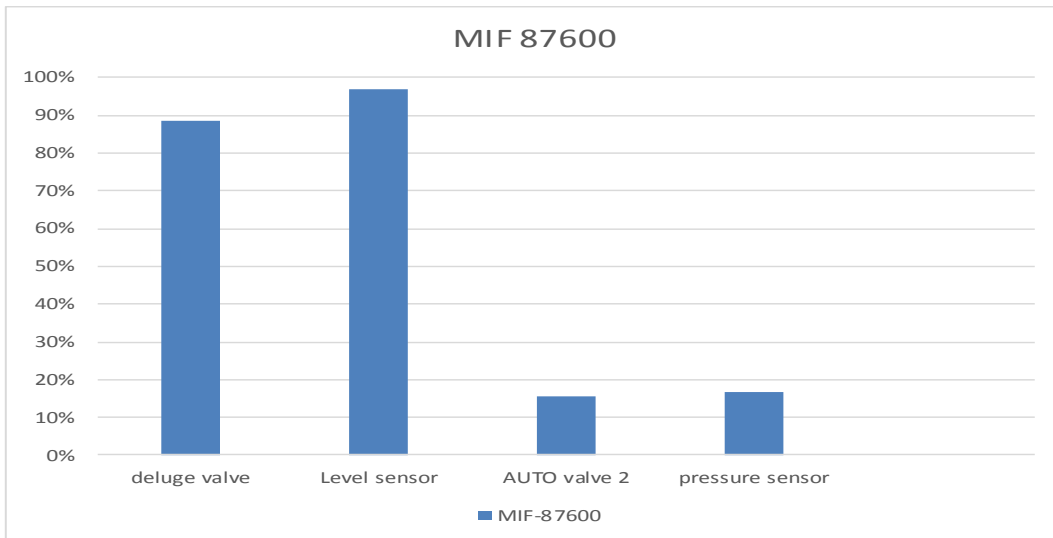


Figure 5.30 Facteur d'importance marginale à 87600h

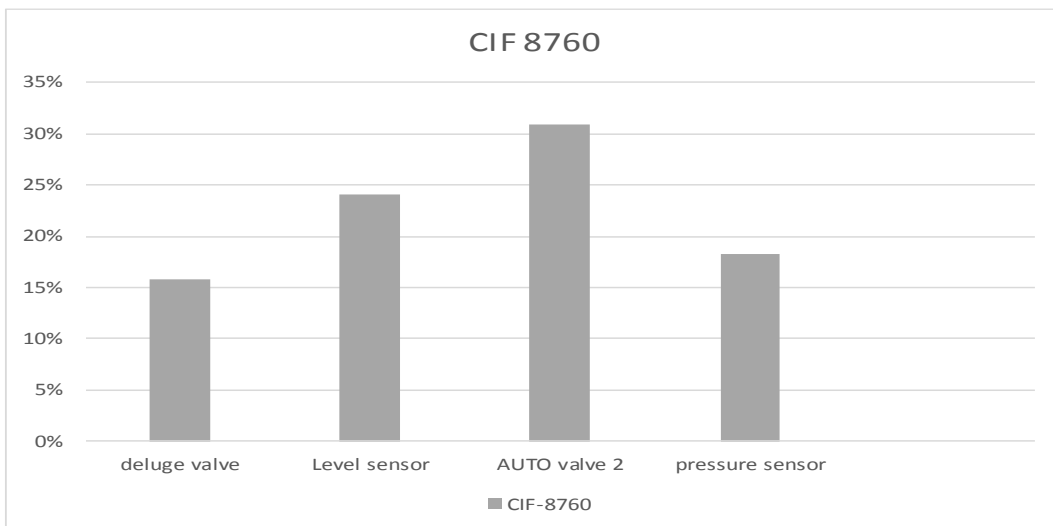


Figure 5.31 Facteur d'importance critique à 8760h

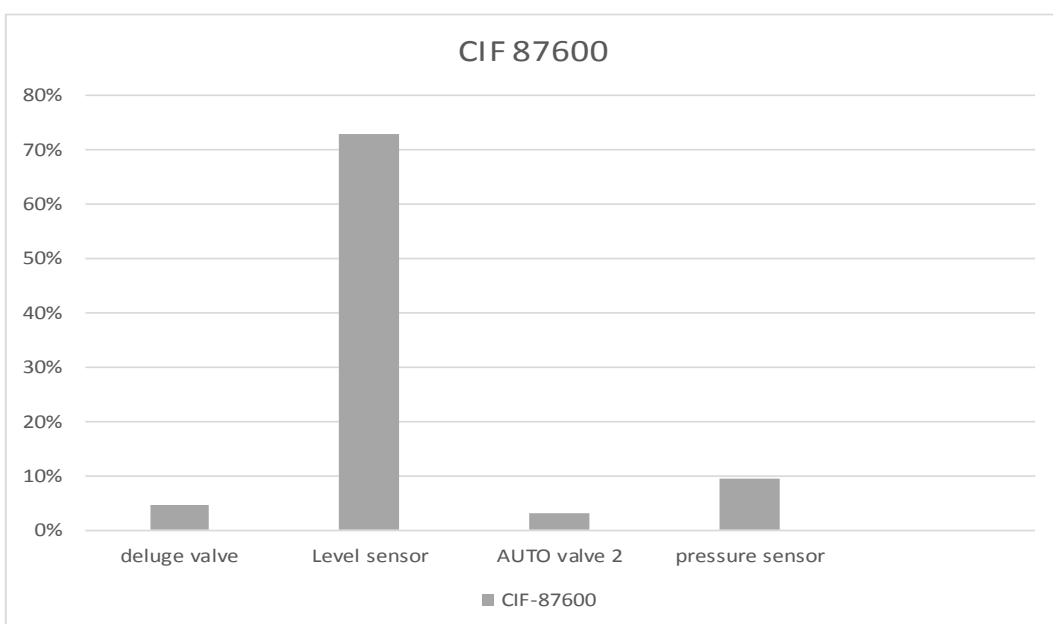


Figure 5.32 Facteur d'importance Critique à 87600h

Suite au calcul des facteurs d'importances en fonction du temps les résultats obtenus sont représentés en Figure 5.33 et comparés par l'évolution de l'indisponibilité du système afin de déterminer à quel instant l'équipement, s'il est défaillant, il mettra le système en situation de fonctionnement critique. A partir de la Figure 5.33 on remarque que la vanne déluge est le composant le plus critique durant le démarrage du système et comme le système ne comporte qu'une seule vanne déluge la défaillance de démarrage de la vanne à la demande peut suspendre le fonctionnement du système d'où de graves conséquences peuvent se générer en cas d'accident catastrophique. D'autre part on peut constater que le capteur de niveau qui a une courte durée de vie par rapport aux autres équipements peut donner une fausse information sur le niveau d'eau et ainsi se retrouver avec un bac de stockage vide. En plus de cela l'ensemble de défaillance de ces équipements clés peut aussi être critique sur le bon fonctionnement du système déluge à eau.

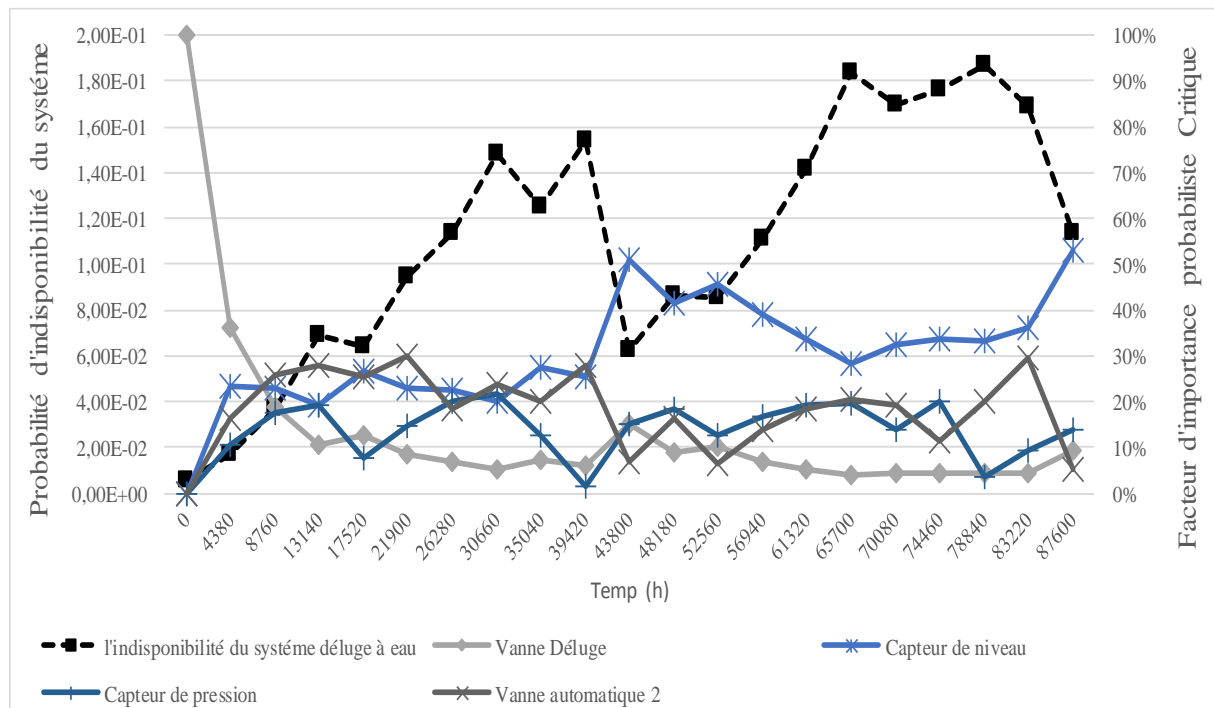


Figure 5.33 Facteur d'importance Critique des composants comparé par leur influence sur l'indisponibilité du système

Synthèse : l'analyse par facteur d'importance probabiliste joue un rôle très important pour prendre les décisions adéquates notamment sur l'optimisation des performances du design. Par contre, c'est toute une procédure de calcul de tous les équipements du système. Certains équipements présentent un très haut niveau de fiabilité mais leurs défaillances peuvent aussi être néfastes sur la disponibilité du système. À cet effet, il est nécessaire de s'orienter vers des méthodes beaucoup plus performantes pour une très bonne aide à la décision qui prend en

considérations tous les équipements même ceux avec un haut niveau de fiabilité. Ces méthodes se doivent aussi être dynamiques pour une meilleure prise en compte de l'évolution temporelle.

5.5. Conclusion

Dans ce chapitre, nous avons déterminé les scénarios catastrophiques qui surviennent dans la zone de stockage du GPL par la méthode d'arbre d'événement, les probabilités obtenues par cette méthode nous ont permis de proposer l'utilisation d'une démarche pour l'analyse d'un dispositif de sécurité performant qui peut assurer la prévention ainsi que l'intervention afin de diminuer les dégâts dans ces zones. Ce dispositif est le système déluge à eau qui a été étudié en détail par les méthodes d'analyse prévisionnelle de la sûreté de fonctionnement, il a fait l'objet d'une analyse par AMDE pour déterminer les modes de défaillance ainsi que leurs causes et effets pour chaque composant, ces résultats nous ont permis de regrouper les données essentielles pour l'étude de fiabilité. Par la suite une analyse de fiabilité et de disponibilité pour chaque composant a été établie pour faciliter l'analyse du système.

L'étude du système déluge à eau ainsi que ses sous-systèmes a été établie par l'utilisation de l'arbre de défaillance afin d'obtenir des résultats qui seront utilisés comme étant des données à priori dans le chapitre suivant pour établir un réseau bayésien d'aide à la décision en temps réel.

Des facteurs d'importance probabiliste ont été calculés par des modèles mathématiques à la fin de ce chapitre afin de les comparer avec les résultats obtenus dans le chapitre suivant.

Chapitre VI

Modèle d'aide à la décision pour les systèmes déluge

Sommaire du chapitre:

6.1. Introduction	103
6.2. Réseau bayésien du système déluge a eau	103
6.2.1. Structure du RB à partir de l'AdD.	103
6.2.2. Comparaison des résultats par les différentes méthodes	104
6.3. Inférence bayésienne pour l'aide à la décision	105
6.3.1. Exemple d'inférence établie sur le réseau	105
6.3.2. Facteurs d'importance obtenus par l'inférence bayésienne	106
6.4. Optimisation des performances du design par processus décisionnel	109
6.4.3. FDMS du nouveau design	111
6.5. Conclusion	116

6.1. Introduction

Les résultats exposés dans ce chapitre expriment le processus décisionnel apporté sur un système déluge à eau installé dans une zone de stockage de GPL. Ce processus décisionnel est développé par l'approche Bayésienne utilisée comme outil stochastique de modélisation de la fiabilité des systèmes. Ainsi, l'analyse de la fiabilité du système par cette approche permet de contrôler la dérive éventuelle des paramètres de fiabilité des composants par l'inférence bayésienne dans le but de maîtriser les risques industriels. Cette analyse basée sur la théorie de Bayes permet d'intégrer les connaissances subjectives des experts et ainsi d'obtenir un processus décisionnel portant sur des événements rares ou incertains.

6.2. Réseau bayésien du système déluge à eau

6.2.1. Structure du RB à partir de l'Add.

Le réseau bayésien a été développé pour analyser l'indisponibilité du système de déluge avec un modèle probabiliste plus performant comme le montre la Figure 6.1 à partir de l'arbre de défaillance présenté dans la Figure 5.24 et en correspondance avec l'algorithme décrit en §4.3.2.

Tous les événements de base dans l'arbre de défaillance sont convertis en nœuds parents. Les nœuds logiques (pivot) sont obtenus à l'aide de la table de probabilités conditionnelles. Où il y'a comme états oui et non.

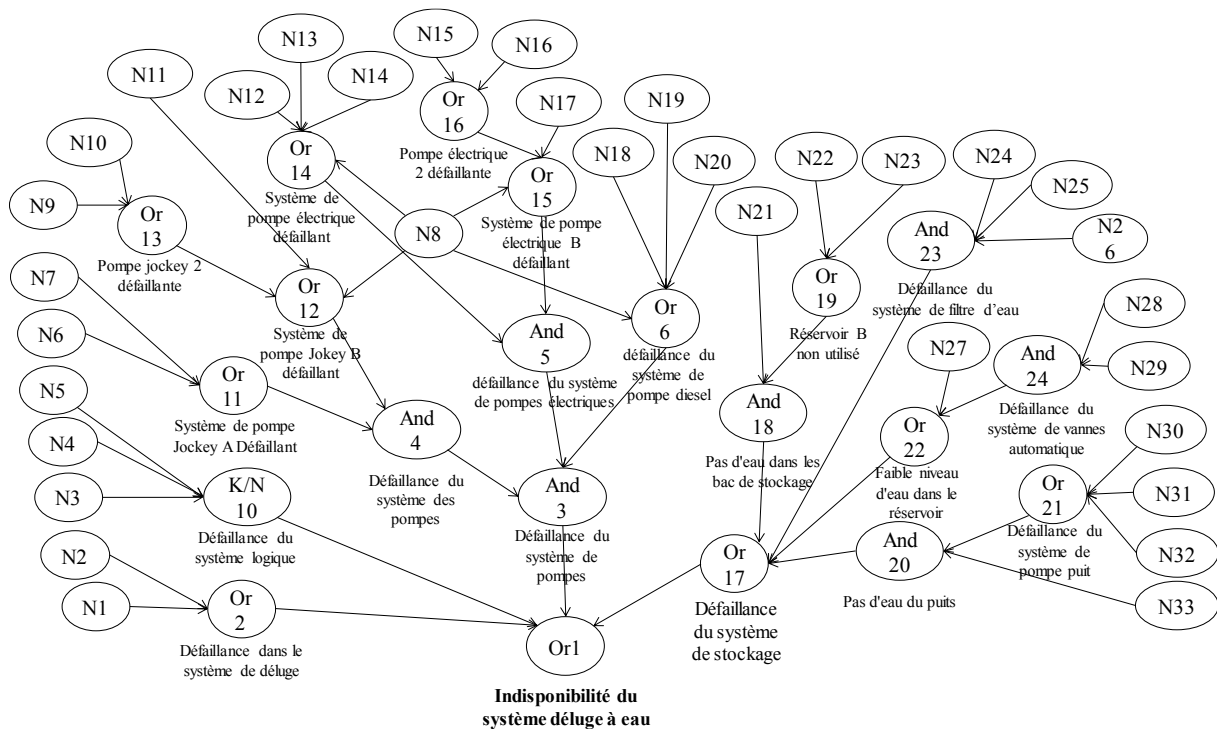


Figure 6.1 Structure du réseau bayésien de l'indisponibilité du système déluge à eau, où les nœuds parents sont présentés dans le Tableau 5.3

6.2.2. Comparaison des résultats par les différentes méthodes

Comme 1^{ère} analyse par les réseaux bayésiens, on a calculé l'indisponibilité du système déluge en termes de tables de probabilité conditionnelle selon les portes logiques correspondantes, en prenant en considération les résultats obtenus par l'analyse de sûreté de fonctionnement (probabilité de défaillance dans le temps) comme étant des données a priori. Ensuite, ces résultats sont comparés avec les résultats obtenus par la simulation de Monté Carlo ainsi que ceux obtenus par simple calcul en fonction de l'arbre développé par le diagramme de décision binaire. Ces résultats ont pour principal objectif la validation du modèle établi par les réseaux bayésiens en utilisant le logiciel AgenaRisk ® [AGE 18]. Les résultats obtenus par ces 3 approches sont représentés sur la [Figure 6.2](#)

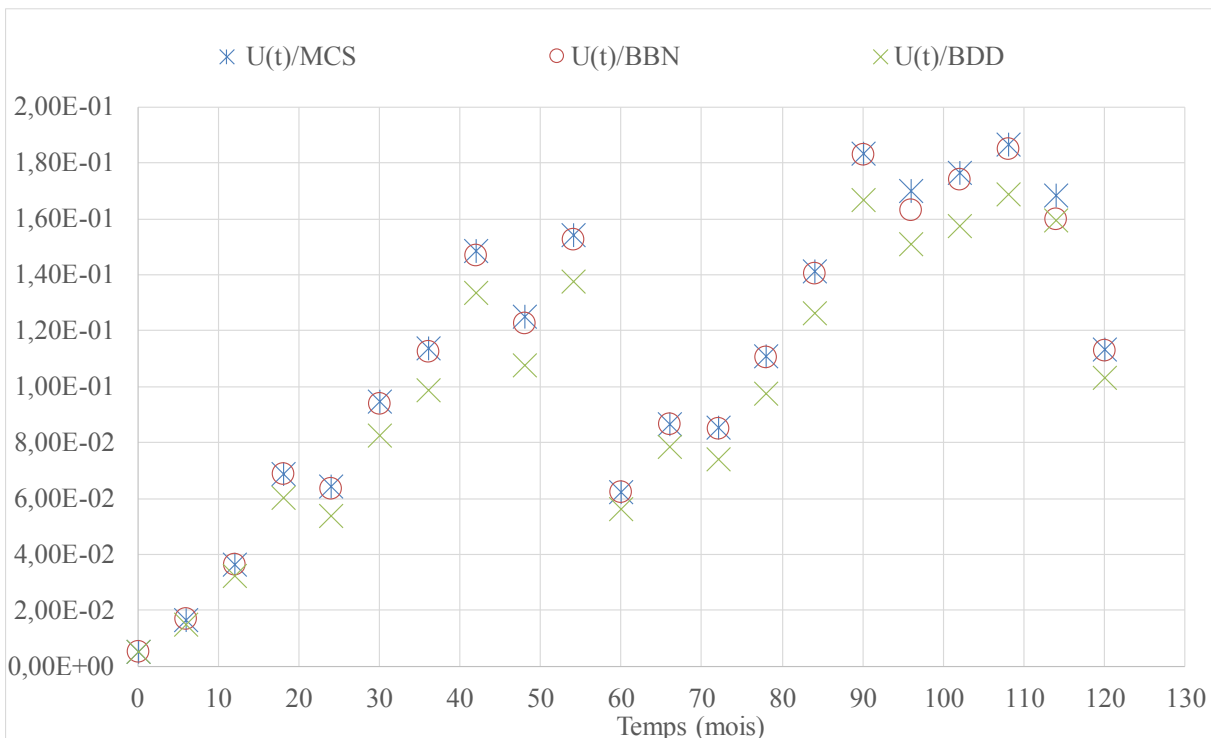


Figure 6.2 l'indisponibilité du système déluge par différentes méthodes

Synthèse : On remarque que l'analyse par réseau bayésien et par la simulation de Monté Carlo sont identiques à part quelques points avec l'erreur quadratique moyenne entre les résultats de simulation d'environ 6,78273E-06 et cela est dû aux données a priori utilisées pour l'analyse par réseau bayésien calculé avec la propagation d'incertitude. Par contre, les résultats obtenus par le diagramme de décision binaire sont relativement proches aux autres résultats d'où on peut conclure que notre réseau bayésien est performant pour une utilisation avancée comme étant un outil dynamique d'aide à la décision.

6.3. Inférence bayésienne pour l'aide à la décision

Le processus qui conduit à décider d'une action met en œuvre un ensemble d'opérations convergentes, sur un groupe d'information plus ou moins important et pertinent, en s'appuyant sur un ensemble de connaissances, dans un environnement déterminé afin d'obtenir un résultat.

Les facteurs d'importance, en plus des données du système, peuvent être considérés comme l'ensemble d'informations nécessaires pour construire la connaissance qui sera utilisée pour la prise de décision. Le facteur d'importance marginale est utilisé pour classer les composants représentant l'augmentation maximale du risque lorsque les composants sont défectueux en comparaison avec lorsque ces composants fonctionnaient.

4 Composants sont sélectionnés par le facteur d'importance marginale comme étant les composants les plus influents sur l'indisponibilité du système 'vanne déluge, capteur de niveau, vanne automatique 2 et capteur de pression'. Les facteurs d'importance critiques sont calculés sur un intervalle de temps de 87 600h pour analyser plus précisément le comportement de chaque composant au-delà de leur MTTF afin d'établir des décisions particulièrement adaptées.

Pour prendre la bonne décision en assurant un haut niveau de FDMS en temps réel, il est très important d'obtenir ces facteurs d'importance à l'aide des réseaux bayésiens.

Après avoir constaté que les facteurs d'importance calculés en temps réel dans le chapitre précédent peuvent être obtenus facilement en termes de posteriori par simple inférence dans le réseau bayésien. On a réécrit les équations 4.4 et 4.5 simplifiées en termes d'inférence bayésienne

Pour qu'elles soient :

$$I_i^B(t) = p_{(s=yes | i=yes)}(t) - p_{(s=yes | i=no)}(t) \quad (6.1)$$

$$I_i^{Cr}(t) = \frac{[p_{(s=yes | i=yes)}(t) - p_{(s=yes | i=no)}(t)] \cdot p_i(t)}{p_s(t)} \quad (6.2)$$

6.3.1. Exemple d'inférence établie sur le réseau

L'exemple suivant en [Figure 6.3](#) illustre l'inférence bayésienne sur le réseau et son influence sur le résultat final avec une évidence de tolérance égale à 1% avec des scénarios «vrais» ou «faux». La probabilité postérieure résultante est un facteur par lequel chaque nœud contribue à la défaillance du système. Les résultats de l'indisponibilité du système à $t = 87\ 600$ h, obtenus pour chaque scénario sachant que les composants sélectionnés sont en panne et / ou en état de fonctionnement. Il est observé que l'indisponibilité du système est de 11,28%, mais lorsque l'une des vannes déluge ou le capteur de pression sont en état de panne, le système est indisponible à 100% et lorsque le capteur de niveau est en état de panne, le système est indisponible de 25,30%. Cependant, ces déductions dans le réseau du système ont permis

d'identifier les composants qui influent directement sur l'indisponibilité du système et qui doivent être sélectionnés pour déterminer leurs réelles criticités sur le système.

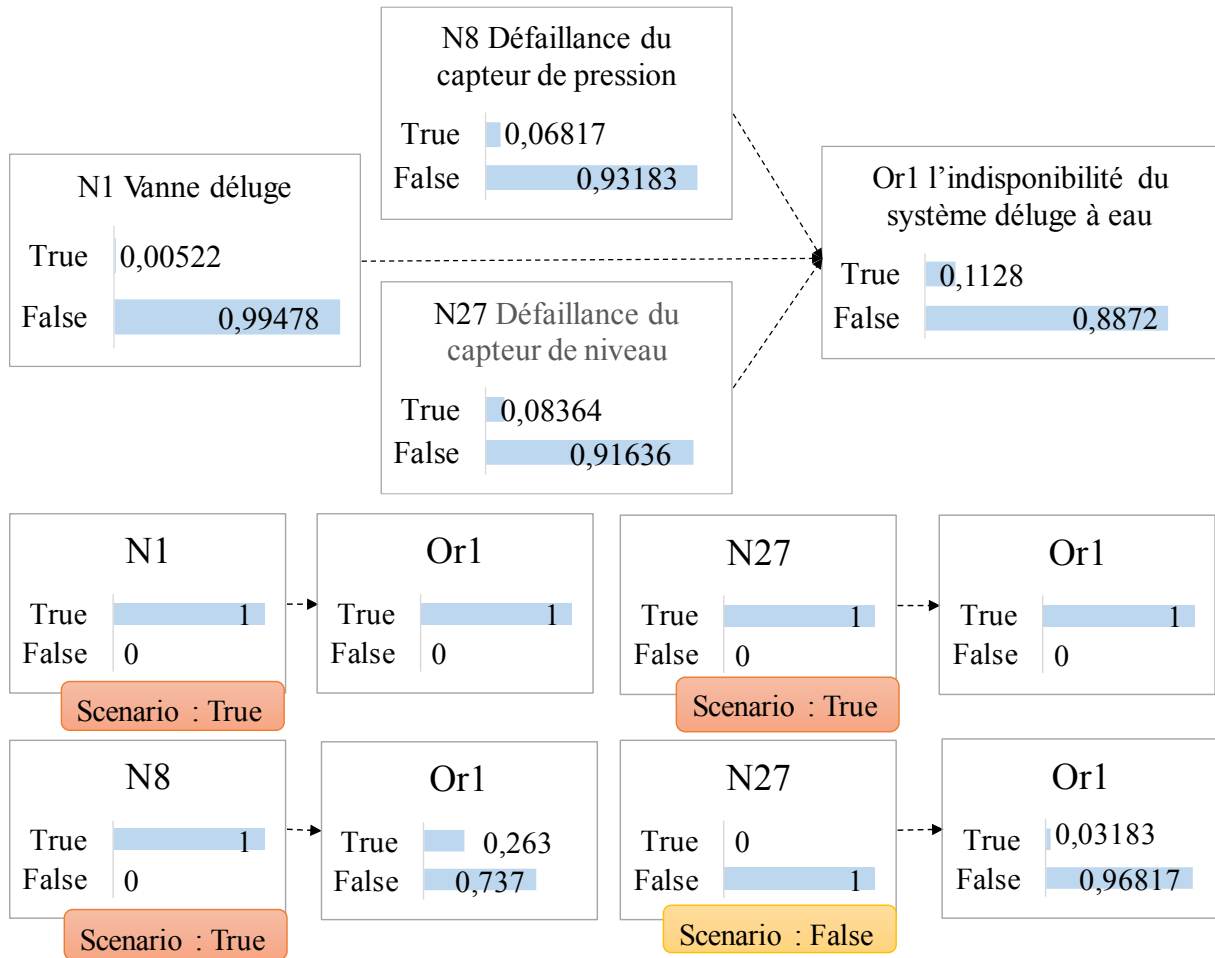


Figure 6.3 Exemple de la variation d'indisponibilité du système à $t = 87600$ h avant et après l'inférence bayésienne de quelques composants.

6.3.2. Facteurs d'importance obtenus par l'inférence bayésienne

Les facteurs d'importance probabilistes sont obtenus à partir des résultats d'inférence et par l'utilisation de l'équation (6.1) pour facteur d'importance marginale et l'équation (6.2) pour le facteur d'importance critique.

Les résultats des facteurs d'importance obtenus a posteriori par le réseau bayésien, pour les quatre composants sélectionnés, sont présentés et validés avec les résultats obtenus à l'aide de l'analyse en chapitre 4 par le diagramme de décision binaire. L'erreur relative est également calculée entre les deux méthodes. On peut observer dans les Tableaux 6.1, 6.2, 6.3 et 6.4 que les valeurs du facteur d'importance marginale obtenues par les deux approches pour chacun des composants dans le temps sont identiques. Cependant, dans le cas du facteur d'importance critique, les différences entre les deux méthodes sont relativement faibles dans certains composants, tels que capteur de niveau Tableau 6.1 avec une erreur relative moyenne de 2,37%

et capteur de pression [Tableau 6.2](#) avec 3,15%. Une différence importante est observée dans les autres composants avec 10,69% pour la vanne de déluge [Tableau 6.3](#) et 10,85% pour la vanne automatique 2 [Tableau 6.4](#). Les explications pratiques de ces différences sont liées aux erreurs relatives des valeurs d'indisponibilité du système obtenues en [Figure 6.2](#) qui sont utilisées pour calculer le facteur d'importance dans l'équation (6.2). La position du composant dans le réseau et la valeur après inférence dans le réseau bayésien sont également prises en compte.

Tableau 6.1 Comparaison des facteurs d'importance pour le capteur de niveau

Time	$I_i^B(t)$		$I_i^{Cr}(t)$		
	BDD	RB	BDD	BBN	RE
0	9.948E-01	9.948E-01	0	0	
4380	9.876E-01	9.876E-01	2.648E-01	2.640E-01	0.32%
8760	9.716E-01	9.722E-01	2.416E-01	2.394E-01	0.91%
13140	9.430E-01	9.440E-01	1.885E-01	1.848E-01	2.00%
17520	9.530E-01	9.535E-01	2.843E-01	2.682E-01	5.65%
21900	9.250E-01	9.267E-01	2.252E-01	2.196E-01	2.49%
26280	9.111E-01	9.118E-01	2.235E-01	2.156E-01	3.55%
30660	8.780E-01	8.802E-01	1.854E-01	1.849E-01	0.26%
35040	9.085E-01	9.094E-01	2.716E-01	2.607E-01	4.01%
39420	8.823E-01	8.824E-01	2.314E-01	2.282E-01	1.42%
43800	9.801E-01	9.806E-01	6.919E-01	6.876E-01	0.62%
48180	9.577E-01	9.592E-01	5.317E-01	5.290E-01	0.52%
52560	9.647E-01	9.650E-01	6.177E-01	5.883E-01	4.75%
56940	9.410E-01	9.424E-01	4.978E-01	4.779E-01	4.00%
61320	9.120E-01	9.146E-01	4.016E-01	3.914E-01	2.55%
65700	8.700E-01	8.731E-01	3.116E-01	3.059E-01	1.84%
70080	8.904E-01	8.978E-01	3.748E-01	3.741E-01	0.17%
74460	8.880E-01	8.902E-01	3.794E-01	3.685E-01	2.88%
78840	8.819E-01	8.820E-01	3.708E-01	3.619E-01	2.41%
83220	8.998E-01	9.129E-01	4.196E-01	4.554E-01	7.85%
87600	9.671E-01	9.682E-01	7.295E-01	7.178E-01	1.60%
RE = 2.37%					

Tableau 6.2 Comparaison des facteurs d'importance pour le capteur de pression

Time	$I_i^B(t)$		$I_i^{Cr}(t)$		
	BDD	RB	BDD	BBN	RE
0	0	0	0	0	
4380	6.947E-02	7.055E-02	1.047E-01	1.073E-01	2.54%
8760	1.302E-01	1.321E-01	1.826E-01	1.814E-01	0.67%
13140	1.811E-01	1.835E-01	2.049E-01	1.965E-01	4.14%
17520	4.045E-02	3.873E-02	5.844E-02	5.844E-02	0.01%
21900	1.002E-01	9.985E-02	1.272E-01	1.245E-01	2.16%

26280	1.545E-01	1.547E-01	2.013E-01	1.889E-01	6.18%
30660	1.982E-01	1.994E-01	2.248E-01	2.124E-01	5.51%
35040	7.314E-02	7.016E-02	1.034E-01	1.002E-01	3.16%
39420	1.238E-01	1.221E-01	7.410E-03	7.830E-03	5.33%
43800	1.923E-01	1.911E-01	1.046E-01	1.079E-01	3.10%
48180	2.366E-01	2.363E-01	1.607E-01	1.616E-01	0.55%
52560	1.106E-01	1.059E-01	1.015E-01	1.023E-01	0.77%
56940	1.633E-01	1.601E-01	1.537E-01	1.510E-01	1.77%
61320	2.075E-01	2.056E-01	1.888E-01	1.831E-01	3.02%
65700	2.412E-01	2.403E-01	1.999E-01	1.904E-01	4.75%
70080	1.314E-01	1.270E-01	1.271E-01	1.275E-01	0.29%
74460	1.818E-01	1.779E-01	1.958E-01	1.861E-01	5.00%
78840	2.158E-01	2.131E-01	2.196E-02	2.262E-02	2.91%
83220	2.600E-01	2.618E-01	6.516E-02	7.284E-02	10.53%
87600	1.677E-01	1.612E-01	9.381E-02	9.740E-02	3.69%
					RE = 3.15%

Tableau 6.3 Comparaison des facteurs d'importance pour la vanne déluge

Time	$I_i^B(t)$		$I_i^{Cr}(t)$		
	BDD	RB	BDD	BBN	RE
0	1	1	9.998E-01	9.998E-01	0%
4380	9.879E-01	9.884E-01	3.480E-01	3.075E-01	11.62%
8760	9.671E-01	9.686E-01	1.575E-01	1.386E-01	11.98%
13140	9.340E-01	9.362E-01	8.164E-02	7.120E-02	12.79%
17520	9.393E-01	9.414E-01	9.207E-02	7.745E-02	15.88%
21900	9.073E-01	9.109E-01	5.818E-02	5.068E-02	12.90%
26280	8.893E-01	8.922E-01	4.801E-02	4.144E-02	13.69%
30660	8.529E-01	8.575E-01	3.406E-02	3.046E-02	10.58%
35040	8.783E-01	8.820E-01	4.357E-02	3.757E-02	13.77%
39420	8.489E-01	8.521E-01	3.292E-02	2.921E-02	11.27%
43800	9.384E-01	9.428E-01	8.839E-02	7.921E-02	10.39%
48180	9.126E-01	9.182E-01	6.163E-02	5.539E-02	10.12%
52560	9.148E-01	9.197E-01	6.548E-02	5.646E-02	13.78%
56940	8.882E-01	8.943E-01	4.861E-02	4.233E-02	12.93%
61320	8.568E-01	8.643E-01	3.634E-02	3.218E-02	11.44%
65700	8.134E-01	8.215E-01	2.626E-02	2.347E-02	10.62%
70080	8.287E-01	8.411E-01	2.955E-02	2.691E-02	8.92%
74460	8.227E-01	8.304E-01	2.809E-02	2.494E-02	11.22%
78840	8.133E-01	8.193E-01	2.588E-02	2.313E-02	10.62%
83220	8.257E-01	8.445E-01	2.769E-02	2.758E-02	0.41%
87600	8.834E-01	8.919E-01	4.564E-02	4.129E-02	9.51%
					RE = 10.69%

Tableau 6.4 Comparaison des facteurs d'importance pour la vanne automatique 2

Time	$I_i^B(t)$		$I_i^{Cr}(t)$		
	BDD	RB	BDD	BBN	RE
0	5.970E-03	5.970E-03	0	0	
4380	1.077E-01	1.101E-01	1.859E-01	1.720E-01	7.51%
8760	1.940E-01	1.982E-01	3.092E-01	2.784E-01	9.95%
13140	2.647E-01	2.700E-01	3.387E-01	2.957E-01	12.71%
17520	1.694E-01	1.742E-01	3.111E-01	2.692E-01	13.48%
21900	2.424E-01	2.482E-01	3.646E-01	3.173E-01	12.99%
26280	1.309E-01	1.336E-01	2.019E-01	1.674E-01	17.10%
30660	2.037E-01	2.080E-01	2.672E-01	2.278E-01	14.73%
35040	1.124E-01	1.157E-01	1.958E-01	1.700E-01	13.18%
39420	1.895E-01	1.938E-01	2.926E-01	2.527E-01	13.64%
43800	2.727E-01	2.791E-01	4.824E-02	4.465E-02	7.43%
48180	3.307E-01	3.381E-01	1.537E-01	1.395E-01	9.24%
52560	6.195E-02	6.369E-02	4.984E-02	4.517E-02	9.37%
56940	1.466E-01	1.505E-01	1.287E-01	1.144E-01	11.14%
61320	2.168E-01	2.223E-01	1.911E-01	1.686E-01	11.76%
65700	2.714E-01	2.779E-01	2.233E-01	1.945E-01	12.89%
70080	1.934E-01	2.003E-01	2.015E-01	1.823E-01	9.52%
74460	8.928E-02	9.148E-02	1.043E-01	8.853E-02	15.16%
78840	1.663E-01	1.702E-01	2.027E-01	1.723E-01	15.01%
83220	2.421E-01	2.511E-01	3.459E-01	3.223E-01	6.83%
87600	1.575E-01	1.626E-01	2.970E-02	2.844E-02	4.24%
					RE = 10.85%

6.4. Optimisation des performances du design par processus décisionnel

Suite à l'analyse des résultats des facteurs d'importance obtenus par l'inférence bayésienne, des décisions d'optimisation des performances du design du système déluge à eau peuvent être prises en considération selon le modèle de décision en schéma de processus décisionnelle [Figure 6.4](#). Ces décisions seront interprétées dans le réseau bayésien initial comme étant des nouvelles données a priori pour but de mettre à jour les probabilités précédentes.

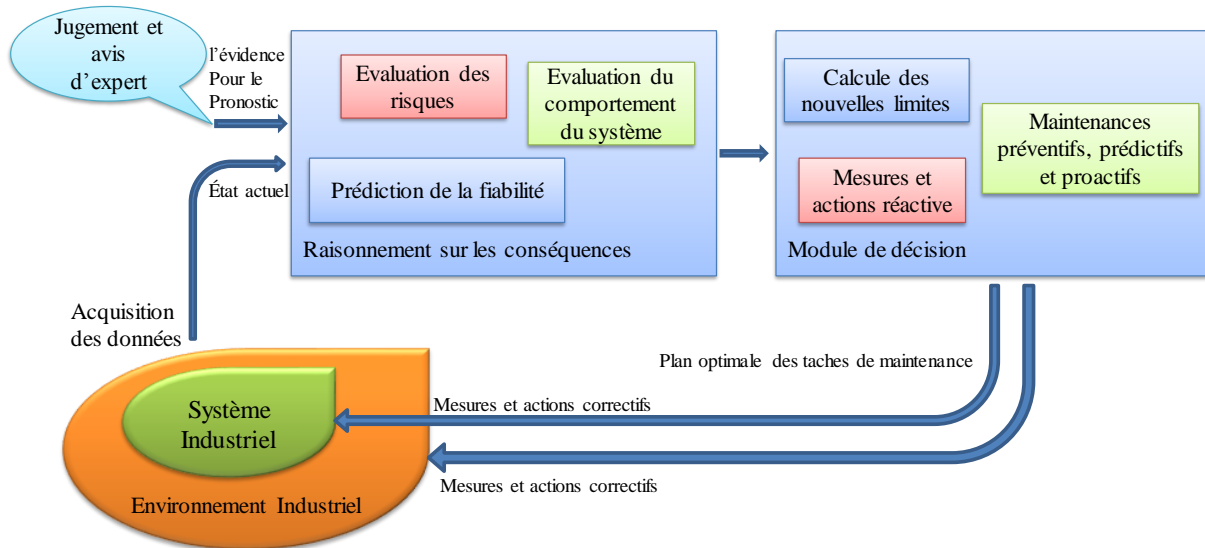


Figure 6.4 Processus décisionnel d'un système industriel

L'utilisation de ce processus décisionnel est établie sur les résultats des 4 composants présentés en tableaux 6.1, 6.2, 6.3 et 6.4. D'après leurs analyses il est clair que chaque composant contribue à l'indisponibilité du système à un intervalle de temps connu. Une redondance des composants «vanne de déluge, système de contrôle de pression et système de contrôle de niveau» est requise en créant de nouveaux nœuds en parallèle de ceux existants déjà dans le réseau ou tout simplement par une mise à jour des probabilités de ces nœuds. Par contre, la valeur de probabilité du nœud de la vanne automatique 2 est mise à jour en réduisant le temps de la maintenance préventive. Cette modification de conception doit être une cible principale pour augmenter la FDMS de notre système déluge à eau.

Le Tableau 6.5 résume les décisions prises sur les 4 composants.

Tableau 6.5 les décisions prises sur les 4 composants

Composant	Décision	Données initiales	Nouvelles données
Vanne déluge	Redondance (l'indisponibilité de la vanne déluge et l'indisponibilité du système)	$P= 5.233E-03$	$P=2.738E-05$
Capteur de pression	Redondance (défaillance du capteur de pression)	$\lambda= 5.300E-6$	$2 \times (\lambda= 5.300E-6)$

	et le non démarrage des pompes)		
Capteur de niveau	Redondance (la défaillance du capteur de niveau et le non remplissage des bacs de stockage)	$\lambda= 9.200E-7$	$2 \times (\lambda= 9.200E-7)$
Vanne automatique 2	Réduction du temps de la maintenance préventive	($\lambda= 5.930E-6,$ $T=4.216E4$)	($\lambda= 5.930E-6,$ $T=4.216E2$)

6.4.3. FDMS du nouveau design

Les décisions adoptées sur la conception du réseau nous ont permis d'obtenir de nouveaux résultats sur l'indisponibilité du système après chaque décision prise pour chaque composant. Les [Tableaux 6.6 – 6.9](#) montrent à quel intervalle de temps la décision a été adéquate et nous donnent le pourcentage de réduction d'indisponibilité pour chaque composant et à chaque intervalle de temps sélectionné. On peut constater que la vanne déluge contribue à 100% sur l'indisponibilité du système au démarrage mais suite à la décision de redondance, l'indisponibilité a diminué avec un grand pourcentage et du même principe, l'indisponibilité du système a diminué avec les autres composants.

Tableau 6.6 Résultats d'aide à la décision sur la vanne déluge

Temps	U(t)	Vanne déluge ne s'ouvre pas à la demande		
		FIC%	U'(t)	↓U%
0	5.221E-03	99.98	2.825 E-05	99.46
1600	7.773E-03	70.33	2.593E-03	66.64
1800	8.228E-03	66.86	3.051E-03	62.92
2400	9.770E-03	57.31	4.601E-03	52.91
3500	1.329E-02	43.23	8.141E-03	38.74
4000	1.519E-02	38.17	1.005E-02	33.84

5000	1.953E-02	30.06	1.441E-02	26.22
43000	5.796E-02	9.50	5.304E-02	8.49
52000	8.164E-02	6.88	7.685E-02	5.87
67000	1.871E-01	2.53	1.829E-01	2.24
67800	1.946E-01	2.41	1.904E-01	2.16
75000	1.822E-01	2.70	1.779E-01	2.36
76000	1.570E-01	3.24	1.526E-01	2.80
84000	1.763E-01	2.62	1.720E-01	2.44
87600	1.132E-01	4.56	1.086E-01	4.06

Tableau 6.7 Résultats d'aide à la décision sur le capteur de niveau

Temps	U(t)	Capteur de niveau défaillant		
		FIC%	U'(t)	↓U%
0	5.221E-03	0	5.221E-03	0.00
1600	7.773E-03	19.15	6.197E-03	20.28
1800	8.228E-03	20.55	6.452E-03	21.58
2400	9.770E-03	23.66	7.399E-03	24.27
3500	1.329E-02	26.21	9.844E-03	25.93
4000	1.519E-02	26.5	1.126E-02	25.87
5000	1.953E-02	26.16	1.464E-02	25.04
43000	5.796E-02	72.94	1.836E-02	68.32
52000	8.164E-02	64.18	3.509E-02	57.02
67000	1.871E-01	30.68	1.377E-01	26.40
67800	1.946E-01	29.5	1.451E-01	25.44
75000	1.822E-01	36.68	1.251E-01	31.34
76000	1.570E-01	44.67	9.469E-02	39.69
84000	1.763E-01	40.16	1.144E-01	35.11

87600	1.132E-01	72.95	4.105E-02	63.74
-------	-----------	-------	-----------	-------

Tableau 6.8 Résultats d'aide à la décision sur la vanne automatique 2

Temps	U(t)	Vanne automatique 2 ne s'ouvre pas		
		FIC%	U'(t)	↓U%
0	5.221E-03	0	5.221E-03	0
1600	7.773E-03	5.69	7.415E-03	4.61
1800	8.228E-03	6.73	7.700E-03	6.41
2400	9.770E-03	9.87	8.929E-03	8.61
3500	1.329E-02	15.13	1.143E-02	13.99
4000	1.519E-02	17.19	1.284E-02	15.44
5000	1.953E-02	20.62	1.607E-02	17.71
43000	5.796E-02	2.53	5.727E-02	1.18
52000	8.164E-02	3.98	7.871E-02	3.59
67000	1.871E-01	24.26	1.478E-01	20.99
67800	1.946E-01	24.69	1.530E-01	21.40
75000	1.822E-01	11.29	1.649E-01	9.47
76000	1.570E-01	16.50	1.352E-01	13.88
84000	1.763E-01	35.10	1.221E-01	30.77
87600	1.132E-01	2.97	1.103E-01	2.54

Tableau 6.9 Résultats d'aide à la décision sur le capteur de pression

Temps	U(t)	Capteur de pression défaillant		
		FIC%	U'(t)	↓U%
0	5.221E-03	0	5.221E-03	0
1600	7.773E-03	0.99	7.722E-03	0.66
1800	8.228E-03	1.11	8.139E-03	1.08
2400	9.770E-03	1.49	9.530E-03	2.45

3500	1.329E-02	2.17	1.264E-02	4.93
4000	1.519E-02	2.47	1.429E-02	5.94
5000	1.953E-02	3.08	1.805E-02	7.58
43000	5.796E-02	4.14	2.329E-02	0
52000	8.164E-02	3.24	5.824E-02	2.18
67000	1.871E-01	8.37	7.986E-02	8.29
67800	1.946E-01	15.78	1.716E-01	8.27
75000	1.822E-01	16.14	1.785E-01	8.52
76000	1.570E-01	19.24	1.667E-01	0
84000	1.763E-01	0.30	1.620E-01	0
87600	1.132E-01	5.16	1.779E-01	0.02

La [Figure 6.5](#) illustre la contribution de la prise de décision à l'optimisation des performances du système déluge à eau en temps continu pour mieux comprendre les [tableaux 6.6 - 6.10](#)

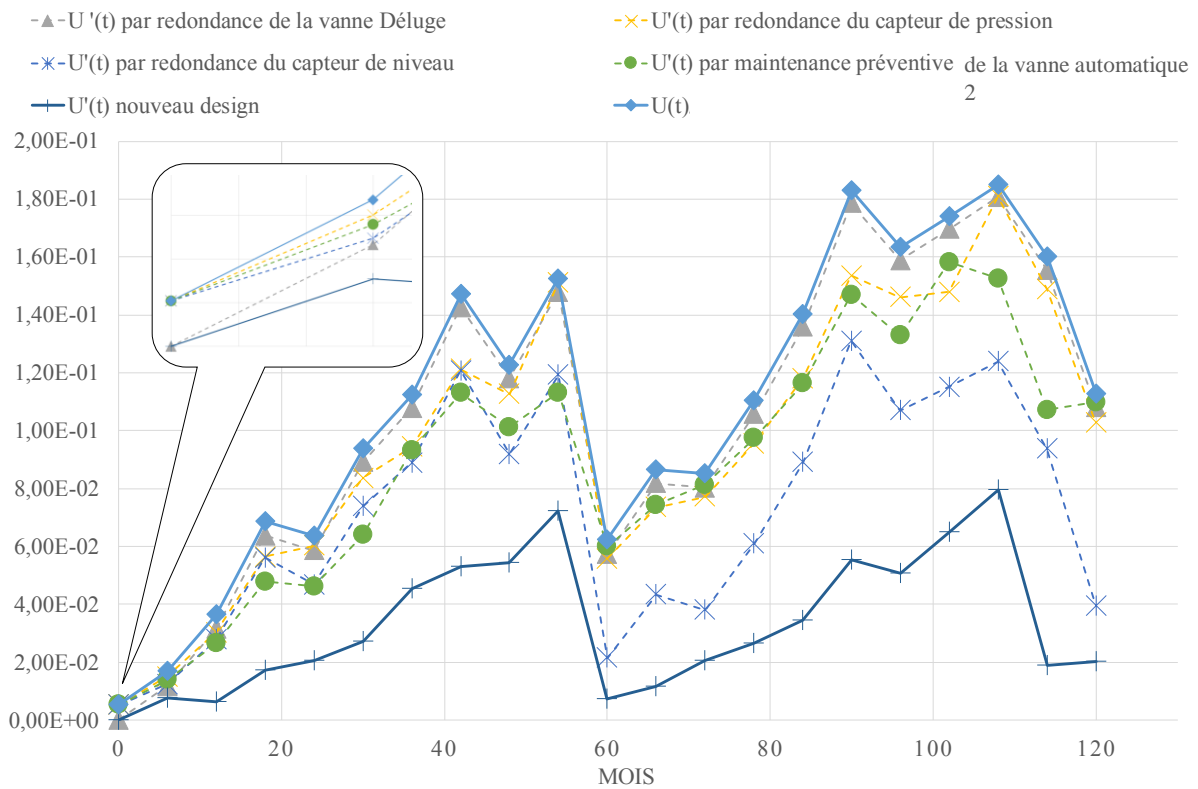


Figure 6.5 l'indisponibilité du système déluge à eau après optimisation du design.

Tableau 6.10 synthèse des résultats d'aide à la décision par réseau bayésien

Temps	U(t)	U'(t)	↓U%
0	5.221E-03	2.825E-05	99.46
1600	7.773E-03	4.000E-04	94.85
1800	8.228E-03	4.191E-04	94.91
2400	9.770E-03	8.258E-04	91.55
3500	1.329E-02	1.689E-03	87.29
4000	1.519E-02	2.314E-03	84.77
5000	1.953E-02	3.886E-03	80.10
43000	5.796E-02	6.058E-03	89.55
52000	8.164E-02	1.913E-02	76.57
67000	1.871E-01	5.225E-02	72.07
67800	1.946E-01	5.566E-02	71.40
75000	1.822E-01	7.097E-02	61.05
76000	1.570E-01	6.824E-02	56.53
84000	1.763E-01	3.229E-02	81.68
87600	1.132E-01	1.910E-02	83.12

Synthèse : l'inférence bayésienne pour le calcul des facteurs d'importance comme des résultats a posteriori nous a permis d'établir un outil d'aide à la décision dynamique. Cet outil facilite la simulation des décisions prises en mettant à jour les probabilités. Ces probabilités deviendront des nouvelles données a priori pour alimenter les bases des données afin de les utiliser pour de nouvelles études de sureté de fonctionnement similaires.

Dans notre étude de plus, la décision de redondance des vannes déluge joue un rôle très important dans la prévention des pannes du système à la demande. Ces nouvelles mises à jour sont très importantes pour alimenter les bases de données, spécialement concernant ces dispositifs récents. La redondance du système de pression est également l'un des éléments clés de cette optimisation, car elle contrôle le système de pompes et la décision de la mettre en redondance, elle joue un rôle important pour le bon fonctionnement de système des pompes.

6.5. Conclusion

On peut conclure que les résultats obtenus par l'utilisation du réseau bayésien correspondant à l'arbre de défaillance du système déluge à eau ont montré une vraisemblance avec une erreur minimale. En outre, le réseau bayésien utilise les informations a priori pour prendre une décision, il a pour objet la détermination de la fiabilité d'un système, tout en utilisant le concept de la probabilité. L'inférence bayésienne nous a permis d'obtenir les facteurs d'importance probabilistes avec une simplicité remarquable donnée en termes de posteriori qui ont été validés par l'approche mathématique présentée dans le chapitre précédent.

Le processus décisionnel développé par les réseaux bayésiens nous a permis d'établir les bonnes décisions pour une optimisation des performances du design du système déluge à eau en assurant un haut niveau de FDMS.

Chapitre VII

Conclusion Générale

Sommaire du chapitre:

7.1. Conclusion 118
7.2. Bilan..... 118
7.3. Perspectives 119

7.1. Conclusion

Les travaux de recherche présentés dans cette thèse ont porté sur la problématique d'utilisation de l'intelligence artificielle comme outil d'aide à la décision dans le domaine de la sûreté de fonctionnement des systèmes en général et des dispositifs de sécurité dans l'industrie pétrolière en particulier. En outre, une méthodologie d'élaboration d'un outil d'aide à la décision à partir des méthodes prévisionnelles de la sûreté de fonctionnement a été proposée. Cet outil est basé sur la présentation de l'arbre de défaillance par un réseau bayésien, une des approches les plus utilisées dans l'intelligence artificielle pour assurer un haut niveau de fiabilité, disponibilité, maintenabilité et sécurité d'un dispositif de sécurité (système déluge à eau) installé dans une zone de stockage de GPL.

7.2. Bilan

Nous avons d'abord présenté une revue de littérature générale sur l'avancée de la technologie dans le développement des méthodes d'aide à la décision dans le domaine de la gestion des risques industriels, cela nous a permis de mieux exprimer notre problématique.

Ensuite nous avons introduit l'analyse par sûreté de fonctionnement et son intérêt dans le contrôle de sécurité, d'amélioration de la disponibilité et de garantie de la fiabilité en tenant en considération la notion du coût. De plus, nous avons présenté les termes les plus rencontrés dans le domaine de la sûreté de fonctionnement tel que FDMS, Métriques de la Sûreté de Fonctionnement, Défaillance, Taux de défaillance et Taux de réparation. Nous avons présenté aussi les lois de probabilité appliquées dans la sûreté de fonctionnement et à la fin de cette partie une large partie a été consacrée aux notions du système en passant par sa structure, son fonctionnement, sa fiabilité et les données de fiabilité.

Nous avons évoqué les principales méthodes d'analyse prévisionnelle des risques tout en essayant de les situer selon leurs processus de raisonnement et d'application. Après avoir décelé les avantages et les limites des méthodes d'analyse choisies pour le développement de notre travail de recherche, nous avons trouvé intéressant de proposer ensuite les critères de choix d'une méthode d'analyse de risque.

La partie théorique de cette thèse a été finalisée par un long chapitre consacré à l'approche bayésienne appliquée en analyse des risques. Nous avons passé par la littérature sur les réseaux bayésiens en général d'une part et les réseaux bayésien pour l'analyse quantitative des risques d'autre part. Le passage de l'arbre de défaillance vers les réseaux bayésiens ainsi que l'utilisation de l'inférence bayésienne pour l'obtention des facteurs d'importances probabilistes représentent notre démarche d'aide à la décision développée pour répondre à la problématique.

Nous avons entamé la partie expérimentale de cette thèse par la détermination de la zone d'étude 'zone de stockage de GPL' ainsi que les scénarios catastrophiques qui surviennent dans cette zone, en suite la détermination du dispositif de sécurité performant qui peut assurer la prévention ainsi que l'intervention afin de diminuer les dégâts dans ces zones 'système déluge à eau'. Nous avons établi une étude approfondie par plusieurs méthodes d'analyse prévisionnelle de la sûreté de fonctionnement pour obtenir un maximum de résultats et de connaissances sur la fiabilité du système déluge à eau qui vont faire l'objet de données a priori pour notre modèle d'aide à la décision. Les facteurs d'importance probabilistes ont été calculés par des modèles mathématiques afin de valider par la suite les résultats de notre démarche.

Enfin, nous avons développé notre outil d'aide à la décision à partir des données a priori, il nous a permis d'obtenir les mêmes résultats que l'arbre de défaillance. Par l'aide de l'inférence bayésienne, nous avons obtenu les facteurs d'importance probabilistes et nous les avons comparés avec ceux obtenus par les modèles mathématiques. En outre, ce processus décisionnel développé par les réseaux bayésiens nous a permis d'établir les bonnes décisions pour une optimisation des performances de design du système déluge à eau en assurant un haut niveau de FDMS.

7.3. Perspectives

Ce thème de recherche laisse à explorer d'autres pistes en termes de développement des méthodes prévisionnelles de la sûreté de fonctionnement par l'intelligence artificielle afin d'établir des modèles d'aide à la décision dynamiques et performants, assurant une supervision en temps réel pour un haut niveau de FDMS des systèmes, à cet effet les principaux développements à entamer sont :

Générer des algorithmes par langage python qui permettent l'optimisation des performances des systèmes en séries et en parallèles à multi états par l'approche Monté Carlo-chaine de Markov MCMC [FIT 11]. Cela permettra d'établir un outil d'aide à la décision performant par les réseaux bayésiens et de le valider par les fonctions génératrices des probabilités (UGF) [LEV 05], [LEV 04].

S'intéresser d'avantage à l'aide à la décision en temps réel par réseaux bayésiens dynamique dans le domaine des systèmes instrumentés de sécurité (SIS/SIL).

Etablir une modélisation des scénarios catastrophiques des risques dans l'industrie pétrolière par les systèmes d'information géographique (SIG) et gérer ces données par des approches hybrides et dynamiques d'aide à la décision.

Bibliographie

[ABD 11] B. Abdolhamidzadeh, T. Abbasi, D. Rashtchian, and S. A. Abbasi, Domino effect in process-industry accidents – An inventory of past events and identification of some patterns, *J Loss Prev Process Ind.* 24(5) (2011), 575–593.

[AFN 88] Afnor, Recueil de normes françaises : “ Fiabilité, Maintenabilité et Disponibilité”. Ed Afnor-Ute. 1988.

[AGE 18] AgenaRisk <https://www.agenarisk.com> consulté 2018-12-03 23:05:06

[AIS 15] N. Aissani and I.H.M. Guetarni, “From Centralized Modelling to Distributed Design in Risk Assessment and Industrial Safety: Survey and Proposition,” *Service Orientation in Holonic and Multi-Agent Manufacturing*, T. Borangiu, A. Thomas, and D. Trentesaux, (Editors), Springer International Publishing, Cham (2015), pp. 125–134.

[AIS 17] N. Aissani, I.H.M. Guetarni, and S. Zebirate, Dynamic control for safety system multi-agent system with case-based reasoning, *Int J Reliab Saf.* 11(3/4) (2017), 238.

[ALS 14] A. Al-shanini, A. Ahmad, and F. Khan, Accident modelling and analysis in process industries, *J Loss Prev Process Ind.* 32 (2014), 319–334.

[BEL 07] K.M. Bell, NFPA 15: Standard for the Installation of Water Spray Fixed Systems for Fire Protection, National Fire Protection Association, USA 2007.

[BEL 16] Salima BELEULMI. Contribution à l’Analyse Bayésienne en Fiabilité des Systèmes Mécanique. Université des frères MENTOURI Constantine 2016.

[BIR 07] Alessandro Birolini, *Reliability Engineering Theory and Practice*, Springer, 2007

[BOB 01] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla, Improving the analysis of dependable systems by mapping fault trees into Bayesian networks, *Reliab Eng Syst Saf.* 71(3) (2001), 249–260.

[BOU 13] Anass BOUCHIBA. EVALUATION DE DYSFONCTIONNEMENT D'UN SYSTEME PAR APPROCHE BAYESIENNE : CAS DU SYSTEME FERROVIAIRE. Ecole doctorale d'Angers, Ecole doctorale de l'EMI, Laboratoire du Génie Industriel de l'Ecole Mohammadia d'Ingénieurs (IMOSYS), Maroc 2009.

[CAI 13] B. Cai, Y. Liu, Y. Zhang, Q. Fan, and S. Yu, Dynamic Bayesian networks based performance evaluation of subsea blowout preventers in presence of imperfect repair, *Expert Syst. Appl.*, vol. 40, no. 18 (2013), 7544–7554.

[CHA 13] Pierre-Yves CHAUX. Formalisation de la cohérence et calcul des séquences de coup e minimales pour les systèmes binaires dynamiques. ECOLE NORMALE SUPERIEURE DE CACHAN- ENSC, 2013.

[CHE 15] CHEBILA Mourad. Modélisation et Evaluation des Performances des Systèmes Instrumentés de Sécurité avec Prise en Compte des Incertitudes. Université El-Hadj Lakhdar Batna, Institut d'Hygiène et Sécurité Industrielle, Laboratoire de Recherche en Prévention Industrielle (LRPI), 2015.

[CHE 17] A.S. Cheliyan and S.K. Bhattacharyya, Fuzzy fault tree analysis of oil and gas leakage in subsea production systems, *J Ocean Eng Sci.* 3 (December 2017), 38–48.

[COR 03] Antoine CORNUEJOLS, Laurent MICLET and Yves KODRATOFF. Apprentissage artificiel : Concepts et algorithmes. France Telecom Recherche et Développement, Eyrolles, 2003.

[DAR 10] R.M. Darbra, A. Palacios, and J. Casal, Domino effect in chemical accidents: Main features and accident sequences, *J Hazard Mater.* 183(1–3) (2010), 565–573.

[DAV 04] G. Davies and P. Nolan, Development of a model to predict the effectiveness of existing water deluge systems and to optimise new systems, *J Loss Prev Process Ind.* 17(2) (2004), 159–168.

- [DEM 09] Amel DEMRI. Contribution à l'évolution de la fiabilité d'un système mécatronique par modélisation fonctionnelle et dysfonctionnelle. Laboratoire de sûreté de fonctionnement, Qualité et organisation. ANGERS 2009.
- [DEN 15] Y. Deng, H. Wang, and B. Guo, BDD algorithms based on modularization for fault tree analysis, *Prog Nucl Energy*. 85 (2015), 192–199.
- [DON 16] D.N. Dongiovanni and T. Iesmantas, Failure rate modeling using fault tree analysis and Bayesian network: DEMO pulsed operation turbine study case, *Fusion Eng Des*. 109-111 (2016), 613–617.
- [DUR 09] K. Durga Rao, V. Gopika, V.V.S. Sanyasi Rao, H. S. Kushwaha, A.K. Verma, and A. Srividya, Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment, *Reliab Eng Syst Saf*. 94(4) (2009), 872–883.
- [FEN 13] Norman FENTON, Martin NEIL. Risk Assessment and Decision Analysis with Bayesian Networks. 2013
- [FIN 08] Maxim Finkelstein, Failure Rate Modelling for Reliability and Risk, Springer, 2008
- [FIT 11] Roy E. Sanders, Handbook of Markov Chain Monte Carlo, Taylor & Francis, 2011
- [GRI 18] Module Tree | GRIF-Workshop | GRaphiques Interactifs pour la Fiabilité <http://grif-workshop.fr/modules/package-booleen/module-tree/> consulté 2018-12-03 00:39:17
- [GUE 18] Islam H.M. Guetarni ,Nassima Aissani, Eric Châtelet, and Zoubida Lounis, Reliability Analysis by Mapping Probabilistic Importance Factors into Bayesian Belief Networks for Making Decision in Water Deluge System, *Process Safety Progress*, 2018
- [GUI 92] Rémi GUILLEMET. Protection des réservoirs de stockage sous pression dans les flammes : l'arrosage par ruissellement d'eau et l'ignifugation. Engineering Sciences. Ecole Nationale Supérieure des Mines de Paris ; Ecole Nationale Supérieure des Mines de Saint-Etienne, 1992.
- [HAM 08] Michael S. HAMADA, Alyson G. WILSON, C. Shane REESE and Harry F. MARTZ. Bayesian Reliability. Springer Series in Statistics, New York, USA 2008.
- [IEC 02] IEC 61508. Sécurité fonctionnelle des systèmes électriques/électroniques /électroniques programmables relatifs à la sécurité, partie 6, mars 2002.

[INC 10] I.I. INC, API 2510 A Fire-Protection Considerations for the Design and Operation of Liquefied Petroleum Gas (LPG) Storage Facilities, American Petroleum Institute, USA (2010).

[JEN 07] J.D. Jensen, NFPA 20: Standard for the Installation of Stationary Pumps for Fire Protection, National Fire Protection Association, USA 2007.

[JUN 17] H.-B. Jun and D. Kim, A Bayesian network-based approach for fault analysis, *Expert Syst Appl.* 81 (2017), 332–348.

[KAB 17] S. Kabir, An overview of fault tree analysis and its application in model based dependability analysis, *Expert Syst Appl.* 77 (2017), 114–135.

[KAD 13] F. Kadri, E. Châtelet, and G. Chen, Method for quantitative assessment of the domino effect in industrial sites, *Process Saf Environ Prot.* 91(6) (2013), 452–462.

[KAL 09] M. Kalantarnia, F. Khan, and K. Hawboldt, Dynamic risk assessment using failure assessment and Bayesian theory, *J Loss Prev Process Ind.* 22(5) (2009), 600–606.

[KHA 11] N. Khakzad, F. Khan, and P. Amyotte, Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches, *Reliab Eng Syst Saf.* 96(8) (2011), 925–932.

[KHA 15] F. Khan, S. Rathnayaka, and S. Ahmed, Methods and models in process safety and risk management: Past, present and future, *Process Saf Environ Prot.* 98 (2015), 116–147.

[KHA1 13] N. Khakzad, F. Khan, and P. Amyotte, Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network, *Process Saf Environ Prot.* 91(1–2) (2013), 46–53.

[KHA2 13] N. Khakzad, F. Khan, and P. Amyotte, Quantitative risk analysis of offshore drilling operations: A Bayesian approach, *Saf Sci.* 57 (2013), 108–117.

[KUO 12] W. Kuo and X. Zhu, *Importance Measures in Reliability, Risk, and Optimization*, John Wiley & Sons, Ltd, Chichester, UK (2012).

[KUO 12] Way Kuo, Xiaoyan Zhu, *IMPORTANCE MEASURES IN RELIABILITY, RISK, AND OPTIMIZATION*, John Wiley, 2012

[LAB 12] Delphine LABOUREUR. Experimental characterization and modeling of hazards: BLEVE and Boilover. Ecole polytechnique de Bruxelles

- [LAK 10] James D. Lake. Automatic Sprinkler Systems Handbook. National Fire Protection Association 2010.
- [LAM 10] Mariapia LAMPIS. Application of Bayesian Belief Networks to System Fault Diagnostics. Loughborough University Institutional Repository 2010.
- [LAM 2009] M. Lampis and J.D. Andrews, Bayesian belief networks for system fault diagnostics, *Qual Reliab Eng Int.* 25(4) (2009), 409–426.
- [LEG 09] Aurélie LEGER. Contribution à la formalisation unifiée des connaissances fonctionnelles et organisationnelles d'un système industriel en vue d'une évaluation quantitative des risques et de l'impact des barrières envisagées. Université Henri Poincaré - Nancy I, 2009.
- [LER 06] Ph. LERAY. Apprentissage et diagnostic de systèmes complexes, Modeling and simulation. Université de Rouen 2006.
- [LEV 04] Levitin, G., A universal generating function approach for the analysis of multi-state systems with dependent elements. *Reliab. Eng. Syst. Saf.* 84, (2004)285–292.
- [LEV 05] Gregory Levitin, *The Universal Generating Function in Reliability Analysis and Optimization*, Springer, 2005
- [LIN 02] K.W. Linder, *NFPA 25: Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems*, National Fire Protection Association, USA 2002.
- [MAN 05] Sam Mannan, *Lees' Loss Prevention in the Process Industries*, Elsevier, 205
- [MAT 15] V. Matuzas and S. Contini, Dynamic labelling of BDD and ZBDD for efficient non-coherent fault tree analysis, *Reliab Eng Syst Saf.* 144 (2015), 183–192.
- [MAZ 08] Mohamed-Habib MAZOUNI. Pour une Meilleure Approche du Management des Risques : De la Modélisation Ontologique du Processus Accidentel au Système Interactif d'Aide à la Décision. Institut National Polytechnique de Lorraine-INPL 2008.
- [MEC 11] Walid MECHRI. Evaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis. L'Ecole Nationale d'Ingénieurs de Tunis 2011.

[MEG 04] Malik MEGDICHE. Sûreté de fonctionnement des réseaux de distribution en présence de production décentralisée. Sciences de l'ingénieur. Institut National Polytechnique de Grenoble - INPG, 2004.

[MER 10] Guillaume MERLE. Algebraic modelling of Dynamic Fault Trees, contribution to qualitative and quantitative analysis. Ecole normale supérieure de Cachan - ENS Cachan, 2010.

[MER 14] G. Merle, J.-M. Roussel, and J.-J. Lesage, Quantitative analysis of dynamic fault trees based on the structure function, Qual Reliab Eng Int. 30(1) (2014), 143–156.

[MER 16] G. Merle, J.-M. Roussel, J.-J. Lesage, V. Perchet, and N. Vayatis, Quantitative analysis of dynamic fault trees based on the coupling of structure functions and Monte Carlo simulation, Qual Reliab Eng Int. 32(1) (2016), 7–18.

[MKH 08] Abdelhak MKHIA. Contribution à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant de l'intelligence. Institut National Polytechnique de Lorraine – INPL 2008.

[MUR 02] Kevin Patrick MURPHY. Dynamic Bayesian Networks: Representation, Inference and Learning. University of California, Berkeley Fall 2002.

[NAC 05] Joel A. Nachlas, Reliability Engineering Probabilistic Models and Maintenance Methods, Taylor & Francis, 2005

[NAI 07] Patrick Naïm, Réseaux bayésiens, eyrolles, 2007

[NEC 15] A. Necci, V. Cozzani, G. Spadoni, and F. Khan, Assessment of domino effect: State of the art and research Needs, Reliab Eng Syst Saf. 143 (2015),

[NEI, 07] J.G. O'Neill, NFPA 13: Standard for the Installation of Sprinkler Systems, National Fire Protection Association, USA (2007).

[NOL 14] DENNIS P. NOLAN, Handbook of FIRE AND EXPLOSION PROTECTION ENGINEERING PRINCIPLES for Oil, Gas, Chemical and Related Facilities, Third Edition Elsevier / William Andrew, 2014

[OLF 04] OLF. Report forum OLF's Gas leak Reduction Project, 2004.

[OUA 14] OUAZRAOUI Nouara. Application des Techniques de l'Intelligence Artificielle aux Problèmes de Gestion des Risques Industriels. Université El-Hadj Lakhdar Batna, Institut

d'Hygiène et Sécurité Industrielle, Laboratoire de Recherche en Prévention Industrielle (LRPI), 2014.

[PEA 86] J. Pearl. Fusion, propagation, and structuring in belief networks. *Journal of Artificial Intelligence*, 29 :241–288, 1986.

[PER 09] Gabriel Antonio Perez Castaneda, Evaluation par simulation de la sûreté de fonctionnement de systèmes en contexte dynamique hybride, Institut National Polytechnique de Lorraine INPL, 09

[PET 09] Morten Nilstad PETERSEN. Reliability Analysis of Fire Water Systems on Offshore Installations. Norwegian University of Science and Technology 2009.

[PRO 03] Henri PROCACCIA, Marie-Christine SUHNER. Démarche Bayésienne et Application à la Sûreté de Fonctionnement. Lavoisier Paris 2003.

[PRO 11] Henri PROCACCIA, Eric FERTON and Marc PROCACCIA. Fiabilité Et Maintenance Des Matériels Industriels Réparables Et Non Réparables. Lavoisier Paris 2011.

[RAU 04] Marvin RAUSAND, Arnljot HSYLAND. System Reliability Theory: Models, Statistical Methods, and Applications. Published simultaneously in Canada 2004.

[REG 08] François-Régis Chevreau. Maîtrise des risques industriels et culture de sécurité : le cas de la chimie pharmaceutique. Engineering Sciences. Ecole Nationale Supérieure des Mines de Paris, 2008.

[ROB 04] T. Roberts, Directed deluge system designs and determination of the effectiveness of the currently recommended minimum deluge rate for the protection of LPG tanks, *J Loss Prev Process Ind.* 17(2) (2004), 103–109.

[ROS 14] Elsa Rosner, Florent Brissaud, Bruno Declerck, Yann Flauw, Valérie De Dianous. Différences entre approches semi-quantitative et quantitative pour l'évaluation probabiliste des risques technologiques. Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda-Mu 19, Oct 2014, Dijon, France. Institut pour la Maîtrise des Risques, 2014.

[RUI 15] E. Ruijters and M. Stoelinga, Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools, *Comput Sci Rev.* 15-16 (2015), 29–62.

[SAL 04] Andrea SALTELLI, Stefano TARANTOLA, Francesca CAMPOLONGO and Marco RATTO. Sensitivity Analysis In Practice A Guide To Assessing Scientific Models. Joint Research Centre of the European Commission, Ispra, Italy 2004.

[SAL 07] MOHAMED SALLAK. Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : Application aux Systèmes Instrumentés de Sécurité. Institut National Polytechnique de Lorraine – INPL 2007

[SAN 05] Roy E. Sanders, Chemical Process Safety Learning from Case Histories, Elsevier, 2005

[SIN 00] SINTEF, Offshore Reliability Data (OREDA), 4th edition, DNV, Norway (2002).

[SIN 06] Nozer D. Singpurwalla, Reliability and Risk A Bayesian Perspective, John Wiley, 2006

[SMI 01] David J Smith, RELIABILITY, MAINTAINABILITY AND RISK Practical methods for engineers, Elsevier, 2001

[SMI 04] David J SMITH and Kenneth G L SIMPSON, Functional Safety: A Straightforward Guide to applying IEC 61508 and Related Standards. Linacre House, Jordan Hill, Oxford OX2 8DP, 2004.

[SMI 10] David J SMITH and Kenneth G L SIMPSON. Safety Critical Systems HandBook. 2010.

[SPO 99] John SPOUGE. A Guide To Quantitative Risk Assessment for Offshore Installations. 1999.

[STA 09] Rudolph Frederick Stapelberg, Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design, Springer, 2009

[TAL 16] M. Talebberrouane, F. Khan, and Z. Lounis, Availability analysis of safety critical systems using advanced fault tree and stochastic Petri net formalisms, J Loss Prev Process Ind. 44 (2016), 193–203.

[TAY 13] Zachary TAYLOR, Subramanyam RANGANATHAN. Designing High Availability Systems: Design For Six Sigma and Classical Reliability Techniques with Practical Real-Life Examples. IEEE Press Editorial Board 2013.

- [TOD 16] Michael Todinov, RELIABILITY AND RISK MODELS SETTING RELIABILITY REQUIREMENTS, John Wiley, 2016
- [USH 12] IGOR USHAKOV, PROBABILISTIC RELIABILITY MODELS, John Wiley, 2012
- [VAN 00] K. Van Wingerden, Mitigation of gas explosions using water deluge, *Process Saf Prog.* 19(3) (2000), 173–178.
- [VAU 11] J.K. Vaurio, Importance measures in risk-informed decision-making: Ranking, optimisation and configuration control, *Reliab Eng Syst Saf.* 96(11) (2011), 1426–1436.
- [VAU 10] J.K. Vaurio, Ideas and developments in importance measures and fault-tree techniques for reliability and risk analysis, *Reliab Eng Syst Saf.* 95(2) (2010), 99–107.
- [VIN 99] Jan Erik VINNEM. Offshore Risk Assessment: Principles, Modelling and Applications of QRA Studies. Springer, 1999.
- [WAN 12] Y. Wang, Q. Li, M. Chang, H. Chen, and G. Zang, Research on fault diagnosis expert system based on the neural network and the fault tree technology, *Procedia Eng.* 31 (2012), 1206–1210.
- [WEB 12] P. Weber, G. Medina-Oliva, C. Simon, and B. Iung, Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas, *Eng Appl Artif Intell.* 25(4) (2012), 671–682.
- [YU 07] Lu YU Fault Tree Analysis and Reliability Assessment of Auxiliary Power Supply system for an HVDC Plant the Royal Institute of Technology, 2007.
- [ZAI 12] Abdelaziz Zaidi, Intégration des réseaux bayésiens et bond graphs pour la supervision des systèmes dynamiques, Université Lille1, 2012.

Annexes

Annexe A : Bases de données et lois de probabilité

A.1. Les lois de probabilité utilisées en fiabilité	131
A.1.1. La loi exponentielle	131
A.1.2. Loi de Weibull.....	131
A.1.3. Loi normale	132
A.1.4. Loi log-normale ou loi de Galton	132
A.1.5. Loi uniforme.....	133
A.2. Bases de données	133
A.2.1. Bases de données de fiabilité	133
A.2.2 Limite d'utilisation des bases de données mécaniques	135

Annexe B : Panorama des méthodes d'analyse prévisionnelle

B.1. Analyse par l'AMDEC	137
B.1.1. Effet d'un mode de défaillance :	137
B.1.2. Les modes de défaillance.....	137
B.1.3. Criticité et tableau d'AMDEC	138
B.2 Analyse par Arbre de Défaillances	139

Annexe A

Bases de données et lois de probabilité

Sommaire de l'Annexe:

A.1. Les lois de probabilité utilisées en fiabilité.....	131
A.1.1. La loi exponentielle	131
A.1.2. Loi de Weibull.....	131
A.1.3. Loi normale	132
A.1.4. Loi log-normale ou loi de Galton.....	132
A.1.5. Loi uniforme.....	133
A.2. Bases de données	133
A.2.1. Bases de données de fiabilité	133
A.2.2 Limite d'utilisation des bases de données mécaniques	135

A.1. Les lois de probabilité utilisées en fiabilité

La fiabilité est une grandeur quantitative et nécessite la connaissance des distributions de donnée selon une durée de vie afin de l'estimer. Dans ce paragraphe, nous présenterons quelques modèles qui interviennent le plus fréquemment dans l'analyse des données de fiabilité communes à plusieurs disciplines. Nous parlerons en particuliers des lois continues. Nous énoncerons les principales propriétés de ces lois (densité de probabilité, fonctions fiabilité et taux de défaillance).

A.1.1. La loi exponentielle

Cette loi a de nombreuses applications dans plusieurs domaines. Elle décrit la vie des composants qui subissent des défaillances brutales. La loi exponentielle est la plus couramment utilisée en fiabilité pour décrire la période durant laquelle le taux de défaillance des équipements est considéré comme constant (défaillance aléatoire). Elle décrit le temps écoulé jusqu'à une défaillance, ou l'intervalle de temps entre deux défaillances.

Elle est caractérisée par :

- ✓ La fiabilité: $R(t) = e^{-\lambda t}$
- ✓ La densité de probabilité: $f(t) = \lambda e^{-\lambda t}$
- ✓ Le taux de défaillance: $\lambda(t) = \frac{f(t)}{R(t)} = \lambda$

Le taux de défaillance est donc constant, ce qui signifie que la loi exponentielle modélise les durées de vie de systèmes qui ne s'usent pas et qui ne s'améliorent pas.

Une propriété principale de la loi exponentielle est d'être sans mémoire ou "Memory less property", ce qu'on exprime de la façon suivante : si le système n'est pas encore tombé en panne à l'instant t , c'est comme s'il était neuf à cet instant. Mathématiquement, cela s'écrit :

$$P(T \geq t + \Delta t / T \geq t) = \frac{e^{-\lambda(t+\Delta t)}}{e^{-\lambda t}} = e^{-\lambda \Delta t} = P(T \geq \Delta t) \quad t > 0, \Delta > 0$$

Ceci signifie qu'à l'instant t , le dispositif est considéré comme neuf (ou "as good as new" en anglais).

Cette loi est aussi utilisée pour des composant réparable par l'intégration du taux de réparation.

A.1.2. Loi de Weibull

Cette loi est très utilisée pour représenter le comportement des composants pendant toute leur période de vie avec une loi de densité de probabilité définie par :

$$f(t) = \frac{\beta(t - \gamma)^{\beta-1}}{\eta^\beta} \exp\left(-\frac{t - \gamma}{\eta}\right)^\beta$$

Avec β paramètre de forme (sans unité),
 η paramètre d'échelle (en unités de temps),
 γ paramètre de position (en unité de temps).

La valeur moyenne et la variance sont données par :

$$m = \gamma + \eta \Gamma\left(\frac{1 + \beta}{\beta}\right)$$

Et $Var(t) = \eta^2 \left[\Gamma\left(\frac{2}{\beta} + 1\right) - \Gamma^2\left(\frac{1 + \beta}{\beta}\right) \right]$

Avec $\Gamma(b) = \int_0^{+\infty} x^{b-1} \exp(-x) dx$

A.1.3. Loi normale

La variable aléatoire est dans ce cas une variable continue t entre $[-\infty$ et $+\infty]$ dont la loi de densité de probabilité est donnée par :

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(t - \mu)^2}{2\sigma^2}\right)$$

avec μ moyenne,
 σ écart-type.

La valeur moyenne et la variance sont données par :

$$m = \mu \text{ et } Var(t) = \sigma^2$$

A.1.4. Loi log-normale ou loi de Galton

La variable aléatoire est dans ce cas une variable continue t entre $[0$ et $+\infty]$ dont la loi de densité de probabilité est donnée par :

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} \frac{1}{t} \exp\left(-\frac{(\ln(t) - \mu)^2}{2\sigma^2}\right)$$

avec μ moyenne des $\ln(t)$,
 σ écart-type des $\ln(t)$.

La valeur moyenne et la variance sont données par :

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

Et $Var(t) = \frac{1}{\lambda^2}$

A.1.5. Loi uniforme

La densité de probabilité et la fiabilité d'une loi uniforme sur $[0, a]$ sont données par les formules suivantes :

$$f(t) = \begin{cases} \frac{1}{a} & \text{si } 0 \leq t \leq a \\ 0 & \text{si } t > a \end{cases}$$

Plus généralement, la distribution de probabilité d'une loi uniforme sur $[a, b]$ s'écrit :

$$f(t) = \begin{cases} \frac{1}{b-a} & \text{si } a \leq t \leq b \\ 0 & \text{si non} \end{cases}$$

A.2. Bases de données

A.2.1. Bases de données de fiabilité

Les bases de données disponibles peuvent être classées en trois catégories :

- Les bases de données spécifiques à une entreprise ou à un site industriel : ce sont des données collectées des équipements similaires, utilisés dans des conditions similaires par une entreprise ;
- Les bases de données spécifiques à une industrie : les données sont issues d'un secteur d'activité donné (télécommunication, nucléaire, militaire, etc.)
- Les bases de données génériques : les données proviennent de plusieurs secteurs d'activités et de plusieurs sources. Ces bases de données présentent souvent des expressions mathématiques qui sont des modèles de régression pour l'estimation des taux de panne, par exemple.

Les informations disponibles supposent généralement que les taux de pannes sont constants dans les conditions spécifiées. Le tableau A.1 présente quelques bases de données de fiabilité et leur auteur. Les taux de pannes des composants sont les principales informations contenues dans ces bases de données.

Tableau A.1 Quelques bases de données de fiabilité

Base de données (dernière mise à jour)	Auteur	Catégorie et remarques
NRPD-5, Non-Electronic parts Reliability Data(1995)	RIAC (Reliability Information Analysis Center), USA	✓ Générique (composants électromécaniques, mécaniques, hydraulique et pneumatiques) ✓ Modes de défaillances.

Handbook of Reliability Prediction for Mechanical Equipment(2007)	NSWC (Naval Surface Warfare Center), USA	<ul style="list-style-type: none"> ✓ Générique composants mécaniques) ✓ Modes de défaillances ✓ Expressions des taux de panne.
OREDA, Offshore Reliability Data (2015)	Consortium de neuf compagnies pétrolières (BP, Elf, Agip, Shell, Total, etc.)	<ul style="list-style-type: none"> ✓ Spécifique à l'industrie pétrolière ✓ Modes de défaillances détaillés. ✓ MTTR.
TECHNIS	Technis,UK	<ul style="list-style-type: none"> ✓ Générique et industrie. ✓ Plusieurs modes de défaillances ✓ Quelques temps de réparation
UKAEA, United Kingdom Atomic Energy Authority	SRD (System Reliability Department) of UKAEA	<ul style="list-style-type: none"> ✓ Générique et industrie nucléaire ✓ Plusieurs modes de défaillance
ANSI/IEEE500 (1991)	IEEE	<ul style="list-style-type: none"> ✓ Spécifique réacteurs nucléaires ✓ Temps de réparations.
NUCLAAR, Nuclear Computerized Library for Assessing Reactor Reliability	NRC (Nuclear Regulatory Commission), USA	<ul style="list-style-type: none"> ✓ Spécifique réacteurs nucléaires ✓ Taux de pannes logiciels ✓ Infos sur les erreurs humaines
EIREDA European Industry Reliability Data(1997)	EDF, France	<ul style="list-style-type: none"> ✓ Spécifique à la production d'énergie électrique (composants mécaniques et électriques).
EPRI	EPRI (Electric Power Research Institute), USA	<ul style="list-style-type: none"> ✓ Spécifique à la production d'énergie électrique (turbines à gaz).
GADS (Generating Availability Data System)	NERC (North American Electric Reliability Council	<ul style="list-style-type: none"> ✓ Spécifique à la production d'énergie électrique ✓ Données (statistiques) annuelles
US Military Handbook of 217 (1992)	RIAC (Reliability Information Analysis	<ul style="list-style-type: none"> ✓ Générique (composants électriques)

	Center), USA Department of Defence	✓ Expressions des taux de pannes.
HRD5, Handbook of Reliability Data (1994)	British Telecom, UK	✓ Spécifique à l'industrie des télécommunications.
Recueil de Données de Fiabilité	CENT (Centre National d'Etudes des Télécommunications), France	✓ Spécifique à l'industrie des télécommunications. ✓ Expressions des taux de pannes.
BELLCORE5, Reliability Prediction Procedure for Electronic Equipment (1995)	BELL (compagnie téléphonique), USA	✓ Spécifique à l'industrie des télécommunications.
EPRD-97 Electronic Parts Reliability Data (1997)	RIAC (Reliability Information Analysis Center), USA	✓ Générique (composants électriques).

A.2.2 Limite d'utilisation des bases de données mécaniques

Ces recueils de données de fiabilité sont fondés soit sur des résultats d'exploitation ou des résultats d'essais en laboratoire. Le processus de dégradation des équipements (modes, mécanismes et causes de défaillance), les conditions d'utilisation et l'évolution des technologies sont des paramètres nécessaires pour le calcul des taux de défaillance et l'élaboration des modèles prévisionnels de la fiabilité, or il est difficile de les prendre tous en considération. Les données sont souvent inappropriées aux systèmes et environnements réels.

Par conséquent, aucune de ces sources de données ne fournit des données parfaites pour une évaluation plus précise de la fiabilité, les informations recueillies ne permettent qu'une exploitation partielle des données, cependant elles restent toujours utiles pour de nouvelles conceptions.

Annexe B

Panorama des méthodes d'analyse prévisionnelle

Sommaire de l'Annexe:

B.1. Analyse par l'AMDEC	137
B.1.1. Effet d'un mode de défaillance :	137
B.1.2. Les modes de défaillance.....	137
B.1.3. Criticité et tableau d'AMDEC	138
B.2. Analyse par Arbre de Défaillances	139

B.1. Analyse par l'AMDEC

L'AMDEC repose sur les concepts de : défaillance (failure), mode de fonctionnement (functional mode), cause de défaillance (failure cause), effet d'un mode défaillance (failure mode effect) et de sa criticité (criticality).

La notion de causes de défaillance peut être vue comme l'ensemble des événements qui conduisent aux modes de défaillances.

B.1.1. Effet d'un mode de défaillance :

Soit les conséquences associées à la perte de l'aptitude d'une entité à remplir une fonction requise.

B.1.2. Les modes de défaillance

Les modes de défaillance sont définis à partir des fonctions remplies par le système, ceci en se posant la question « qu'est ce qui se passe si »:

- ✓ La fonction ne se réalise pas à la sollicitation ? ou bien
- ✓ se réalise de façon intempestive ? ou bien
- ✓ est dégradée ? ou alors
- ✓ ne se réalise plus.

Le [Tableau B.1](#) présente une liste de modes de défaillance établi par la norme AFNOR.

Pour chaque mode de défaillance, on identifie les causes possibles et ensuite les effets sur les fonctions supérieures du système et de ses interfaces.

Tableau B.1 liste de modes de défaillance

1. Défaillance structurelle (rupture)	12. Est en dessous de la limite inférieure tolérée	23. Fonctionnement après délai prévu (retard)
2. Blocage physique ou coincement	13. Fonctionnement intempestif	24. Entrée erronée (augmentation)
3. Vibrations	14. Fonctionnement intermittent	25. Entrée erronée (diminution)
4. Ne reste pas en position	15. Fonctionnement irrégulier	26. Sortie erronée (augmentation)
5. Ne s'ouvre pas	16. Indication erronée	27. Sortie erronée (diminution)
6. Ne se ferme pas	17. Ecoulement réduit	28. Perte de l'entrée
7. Défaillance en position ouverte	18. Mise en marche erronée	29. Perte de sortie

8. Défaillance en position fermée	19. Ne s'arrête pas	30. Court-circuit (électrique)
9. Fuite interne	20. Ne démarre pas	31. Circuit ouvert (électrique)
10. Fuite externe	21. Ne commute pas	32. Fuite (électrique)
11. Dépasse la limite supérieure tolérée	22. Fonctionnement prématuré	33. Autres conditions de défaillance exceptionnelles

B.1.3. Criticité et tableau d'AMDEC

Les criticités des modes de défaillance sont évaluées en fonction de la gravité des conséquences et la fréquence d'occurrence des événements redoutés en [Tableau B.2](#) présentés dans la matrice des risques [Figure B.1](#).

Tableau B.2 Criticités et probabilités des défaillances

Gravité 1	Morts ou perte totale du système
Gravité 2	Blessés graves ou dommage matériel majeur
Gravité 3	Blessés légers ou dommage matériel significatif
Gravité 4	Aucun mort ou blessé ni dommage matériel
Probabilité A	$> 10^{-3}/h$ (fréquent)
Probabilité B	entre $10^{-3}/h$ et $10^{-5}/h$ (probable)
Probabilité C	entre $10^{-5}/h$ et $10^{-7}/h$ (occasionnel)
Probabilité D	entre $10^{-7}/h$ et $10^{-9}/h$ (rare)
Probabilité E	$< 10^{-9}/h$ (improbable)

	Gravité 1	Gravité 2	Gravité 3	Gravité 4
Probabilité A				
Probabilité B				
Probabilité C				
Probabilité D				
Probabilité E				

Figure B.1 Exemple de matrice de criticité

Le [Figure B.2](#) représente le contenu d'un tableau d'AMDEC

© AMDEC CETIM	ANALYSE DES MODES DE DÉFAILLANCE DE LEURS EFFETS ET DE LEUR CRITICITÉ								AMDEC MACHINE			
SYSTÈME.....				PHASE DE FONCTIONNEMENT :		DATE DE L'ANALYSE :		Page			
SOUS-SYSTÈME												
Élément	Fonction	Mode de défaillance	Cause	Effet	Détection	TI	Criticité				Action corrective	
							F	G	N	C		

Figure B.2 Tableau générique d'AMDEC

B.2. Analyse par Arbre de Défaillances

La méthode consiste en une représentation graphique des multiples causes d'un événement dangereux. Elle permet de visualiser les relations entre les défaillances d'équipement, les erreurs humaines et les facteurs environnementaux qui peuvent conduire à des accidents. On peut donc éventuellement y inclure des facteurs liés aux aspects organisationnels.

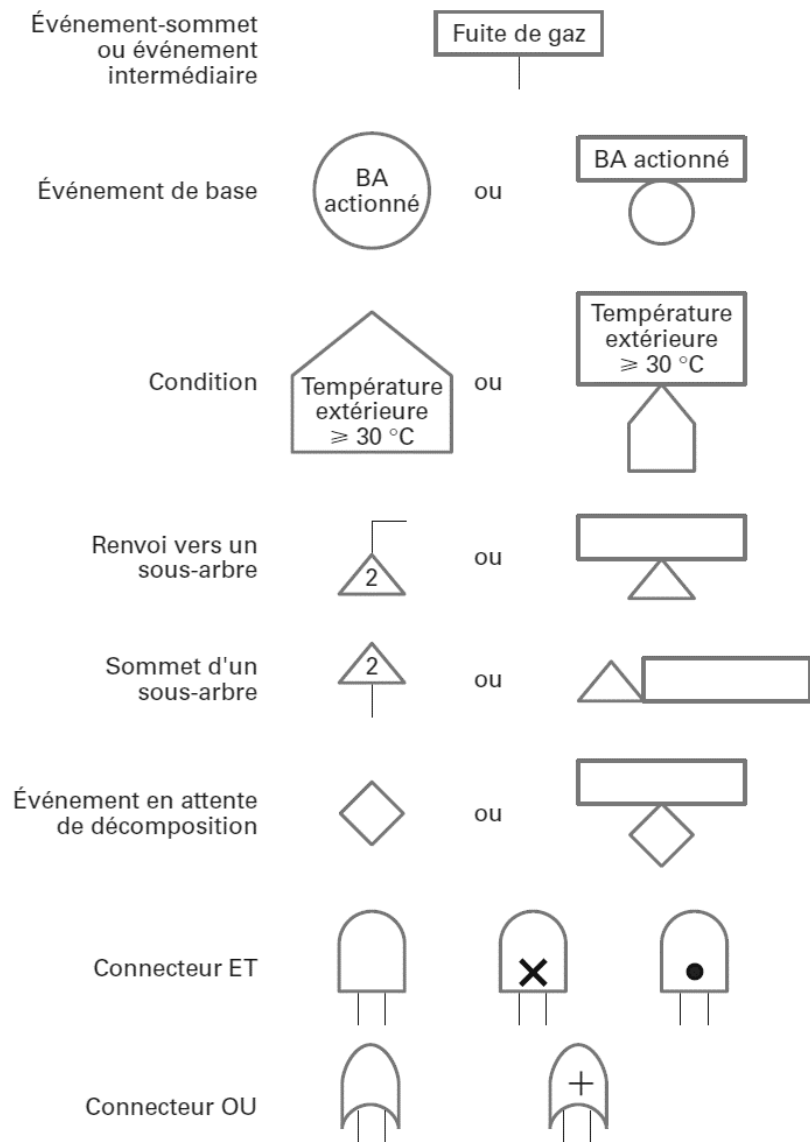


Figure B.3 Les éléments de base pour la construction de la structure de l'arbre de défaillance

Le **Tableau B.3** présente quelques règles d'optimisation permettant de réduire les Arbres en faisant appliquer l'algèbre booléenne :

Tableau B.3 Règles d'optimisation des arbres de défaillances

Propriétés	Produit (Porte logique Et)	Somme (Porte logique Ou)
Commutativité	$A \cdot B = B \cdot A$	$A + B = B + A$
Idempotence	$A \cdot A = A$	$A + A = A$
Absorption	$A \cdot (A + B) = A$	$A + A \cdot B = A$
Associativité	$A \cdot (B \cdot C) = (A \cdot B) \cdot C$	$A + (B + C) = (A + B) + C$
Distributivité	$A \cdot (B + C) = A \cdot B + A \cdot C$	$A + B \cdot C = (A + B) \cdot (A + C)$