جامعـــة باجـي مختـــار- عنابـــــة
UNIVERSITÉ BADJI MOKHTAR ANNABA
BADJI MOKHTAR ANNABA UNIVERSITY

FACULTÉ DE SCIENCE DE L'INGENIORAT

Département d'Electromécanique

THÈSE

Présentée

En vue de l'obtention du diplôme de

DOCTORAT

Contribution à l'allocation et à la vérification des niveaux d'intégrité de sécurité (SIL) à l'aide des réseaux bayésiens

Option: Sécurité Industrielle

Par

HAMAIDIA Mohyiddine

Soutenue le 14/07/2019 devant le Jury:

HAMAIDI Brahim	Professeur	Univ. Annaba	Président
KARA Mohammed	Professeur	Univ. Tébessa	Rapporteur
INNAL Fares	Professeur	Univ. Skikda	Co-Rapporteur
HADJADJ Aoul Elias	Professeur	Univ. Annaba	Examinateur
KABOUCHE Abdallah	Maitre de Conférences (MCA)	Univ. Annaba	Examinateur

Remerciements

Alhamdoulillah,

Le travail présenté ici a été mené au sein de Laboratoire de Génie électromécanique du département d'électromécanique de l'université Badji Mokhtar Annaba, dans le cadre d'une thèse de doctorat en hygiène et sécurité industrielle. Option Sécurité Industrielle.

J'adresse toute ma gratitude à mon encadreur Mr. KARA Mohammed, professeur à l'université de Tébessa de m'avoir encadré et de son aide et ses encouragements tout au long de ce travail. Je voudrais le remercier aussi pour sa disponibilité et ça souplesse de travail.

J'exprime mes profonds remerciements à Mr. INNAL Fares, professeur à l'université de Skikda pour sa collaboration inestimable. Sa compétence a été un atout à la réussite de mes travaux et m'a permis d'apprendre énormément durant ces années de collaboration.

J'exprime toute ma gratitude aux professeurs membres de mon jury d'examen pour avoir bien voulu me faire l'honneur de juger ce travail.

Mes remerciements très particuliers s'adressent à mes collègues des deux promotions de doctorat 2013 et 2014 Option Sécurité Industrielle. Je remercie également tout le personnel du département d'électromécaniques.

Mes vifs remerciements vont également à mes amies qui m'ont accompagnées de leur amitié et de leurs encouragements tout particulièrement à Abderazak et Abdelhak.

Je remercie enfin tous ceux qui ont contribué de près ou de loin à l'aboutissement de ce travail de thèse.

Résumé

Un enjeux important auquel fait face les analystes de sécurité industrielle est comment évaluer les paramètres liés aux scénarios d'accident et aux systèmes relatifs à la sécurité particulièrement les systèmes instrumenté de sécurité (SIS), tels que la fréquence des séquences indésirables et la détermination de niveaux d'intégrité de sécurité (SIL) en prenant toute contrainte existante dans les systèmes réels d'exploitation. L'arbre de défaillance dynamique (DFT) est convenable à capturer les dépendances fonctionnelles et dynamiques entre les événements menant à la défaillance du système. Deux modèles de résolution des DFT sont proposés. Le premier modèle représente une méthodologie complète basée sur la détermination de la fonction de structure et les coupes / séquences de défaillance. Ce modèle est capable de quantifier d'une part la probabilité moyenne de défaillance sur demande (PFDmoy) et la probabilité de défaillance par heure (PFH) des SIS et d'autre part la fréquence des scénarios d'accident. Le second modèle est le réseau bayésien temporel discontinu (DTBN) convertissant l'arbre de défaillance dynamique et donne à l'analyste en plus de l'évaluation des performances des SIS l'opportunité d'implémenter les calculs de probabilité a postériori, tels que les facteurs d'importance, le diagnostique et la prédiction.

Mots clés: Scénarios d'accident, arbre de défaillance dynamique, réseau bayésien temporel discontinu, séquences de défaillance, dépendances fonctionnelles et séquentielles.

ملخص

تتمثل إحدى التحديات المهمة التي تواجه محللي السلامة الصناعية في كيفية تقييم المؤشرات المتعلقة بسيناريوهات الحوادث وأنظمة السلامة ، وخاصة أنظمة السلامة الآلية (SIS) ، مثل تواتر المسلسلات غير المرغوب فيها ، وتحديد مستويات تكامل الأمان (SILs) مع الأخذ في الإعتبار أي عراقيل موجودة في أنظمة الإستغلال على أرض الواقع. هيكل الفشل الديناميكي (DFT) مناسب لإلتقاط العلاقات الوظيفية والديناميكية الموجودة بين الأحداث التي تؤدي إلى فشل النظام. الهدف هو إقتراح نموذجين لقراءة الـ DFT وتحليله. يمثل النموذج الأول منهجية كاملة تستند إلى تحديد وظيفة الهيكل وتقطيع / تسلسل سيناريو الفشل. هذا النموذج قادرأولا على تحديد متوسط احتمال الفشل عند الطلب (PFDmoy) واحتمال الفشل في الساعة (PFH) لـ SIS وثانيًا حساب تواتر مسلسلات الحوادث. النموذج الثاني عبارة عن شبكة بايز المتقطعة زمنيا (DTBN) التي تقوم بتحويل هيكل الفشل الديناميكي وتمنح المحلل ، بالإضافة إلى تقييم أداء الـ SIS ، الفرصة لحساب الاحتمالات الخلفية مثل عوامل الأهمية والتشخيص والتنبؤ.

الكلمات الأساسية: سيناريوهات الحوادث ، هيكل الفشل الديناميكي ، شبكة بايز المتقطعة زمنيا ، مسلسلات الفشل ، العلاقات الوظيفية والديناميكية.

Abstract

An important issue facing industrial safety analysts is how to evaluate parameters related to accident scenarios and safety-related systems, particularly instrumented safety systems (SIS), such as the frequency of unwanted sequences and the determination of Security Integrity Levels (SILs) taking any existing constraints in real-life operating systems. Dynamic failure tree (DFT) is suitable to capture functional and dynamic dependencies between events leading to system failure. Two models of DFT resolution are proposed. The first model represents a complete methodology based on the determination of the structure function and the cuts / sequences of failure. This model is able to quantify firstly the average probability of failure on demand (PFDavg) and the probability of failure per hour (PFH) of the SIS and secondly the frequency of accident scenarios. The second model is the Discrete-Time Bayesian Network (DTBN) converting the dynamic failure tree and gives the analyst in addition to the SIS performance evaluation, the opportunity to implement a posteriori probability calculations, such as importance factors, diagnosis and prediction.

Key words: Accident scenarios, dynamic failure tree, discrete-time Bayesian network, failure sequences, functional and sequential dependencies.

Table des matières

Liste des abréviations et symboles

AdD	Arbre des Défaillances
ALARP	As Low As Raisonably Practicable (Aussi faible que raisonnablement possible)
AND	AND gate (Porte ET)
BDD	Binary decision diagram (Diagramme de décision binaire)
BNT	Byesian net toolbox (Boite à outils du réseau bayésien)
BPCS	Basic Process Control System (Système basique de contrôle de procédé)
CEI	Commission Internationale d'Electrotechnique
CSP	Cold spare gate (Porte de secours froide)
DD	Défaillance dangereuse détectée
DFT	Dynamic fault tree (Arbre de défaillance dynamique)
DND	Défaillance dangereuse non détectée
DTBN	Discrete Time Bayesian Network (Réseau bayésien temporel discontinu)
EB	Evénement de Base
EI	Evénement Initiateur
ER	Evénement Redouté
ES	Evénement Sommet
EUC	Equipment Under Control (Equipement à protéger)
E/E/EP	Electrique / Electronique / Electronique Programmable
FDEP	Functional-dependency gate (Porte de dépendance fonctionnelle)
GCTBN	Generalized Continuous Time Bayesian Network (Réseau bayésien temporel continu généralisé)
HAZOP	HAZard and Operability study (Analyse de risque et d'exploitabilité)
HSP	Hot spare gate (Porte de secours chaude)
HSS	Hypothetical sprinkler system (Système gicleur hypothétique)
IPL	Independent Protection Layer (Couche de protection indépendante)
ISO	International Organisation for Standardization (Organisation internationale de normalisation)
KooN	K out of N (K parmi N)
LOPA	Layer Of Protection Analysis (Analyse des couches de protection)
MIF	Marginal Importance Factor (Facteur d'importance marginale)
OR	OR gate (Porte OU)

PAND	Priority-AND gate (Porte ET prioritaire)
PFD	Probability of Failure on Demand (Probabilité de défaillance à la demande)
PFH	Probability of Failure per Hour (Probabilité de défaillance par heure)
PL	Protection layer (Couche de protection)
RB	Réseau Bayésien
RBD	Réseau Bayésien Dynamique
SBDD	Sequential binary decision diagram (Diagramme séquentiel de décision binaire)
SBS	Steam boiler system (Système de chaudière à vapeur)
SDD	Sequence decision diagram (Diagramme de décision séquentiel)
SEQ	Sequence-enforcing gate (Porte d'exécution de séquence)
SIF	Safety Instrumented Function (Fonction instrumentée de sécurité)
SIL	Safety Integrity Level (Niveau d'intégrité de sécurité)
SIS	Système Instrumenté de Sécurité
SMs	Séquences Minimales
SPARE	Spare gate (Porte de secours)
TCP	test de course partielle
TP	test de preuve
WSP	Warm spare gate (Porte de secours douillet)
$\lhd$	Opérateur non-inclusif avant
$\triangle$	Opérateur simultané
$\underline{\lhd}$	Opérateur non-inclusif
$[A, B]$	Séquence de défaillance pour deux événements A et B
X	Évènement de défaillance
x	Probabilité d'occurrence de X
$\overline{x}$	Probabilité de non-occurrence de X
X_a	Evènement de secours en mode active
X_d	Evènement de secours en mode dormant
Pr	Probabilité de défaillance
fr	Fréquence de défaillance
λ_X	Taux de défaillance pour X
α	Facteur de dormance
λ_{X_d}	Taux de défaillance pour X en mode dormant ($\lambda_{X_d} = \alpha\lambda_X$)

Liste des tableaux

Liste des figures

Introduction

Problématique

Les conséquences des accidents survenant aux niveaux des installations industrielles actuelles sont de plus en plus catastrophiques. Cet état de fait a incité les gouvernements à se doter d'une politique rigoureuse en matière de prévention des risques industriels majeurs. Pour partiellement répondre à ce besoin, le Comité International d'Electrotechnique (CEI) a publié une série de normes dites de sécurité fonctionnelle, telles que la CEI 61508 et la CEI 61511 [1,2], visant la mise en place de moyens de protection conformes aux scénarios d'accidents. Il importe de noter que ces normes se focalisent sur un type de barrière bien particulier : les Systèmes Instrumentés de Sécurité (SIS). Plus précisément, l'objectif de ces normes est d'abord d'estimer la réduction nécessaire du risque qui doit être réalisée par les SIS et de s'assurer ensuite que ces derniers peuvent accomplir d'une manière satisfaisante les fonctions de sécurité qui leur ont été assignées.

Pour faciliter cette tâche, la CEI 61508 adopte le concept de niveau d'intégrité de sécurité (SIL : Safety Integrity Level) qui spécifie les exigences (qualitatives et quantitatives) sur la fonction de sécurité implémentée au niveau du SIS. Les exigences quantitatives d'intégrité de sécurité (intégrité de sécurité du matériel) doivent être traduites en mesures cibles de défaillances. Ces dernières s'identifient à la probabilité moyenne de défaillance à la demande du SIS (PFDmoy: Probability of Failure on Demand) pour un SIS fonctionnant en « faible demande », et à sa probabilité de défaillance dangereuse par heure (PFH: Probability of Failure per Hour) s'il est appelé à fonctionner en mode « demande élevée ou continue ».

Les méthodes de détermination du niveau d'intégrité de sécurité (SIL) correspondant à un phénomène dangereux spécifié (scénario d'accident) et les formules usuelles généralement utilisées dans ce sens sont plus ou moins adaptées en fonction du niveau de détail des

analyses de risques réalisées. La CEI 61508 décrit les méthodes suivantes : graphe de risque, matrice des évènements dangereux et la méthode LOPA (Layer Of Protection Analysis) [3]. La méthode LOPA est qualifiée de semi-quantitative et considérée comme un outil très efficace pour l'aide à la décision. En revanche cette méthode présente certains inconvénients limitant son champ applicatif. Cela dit, la méthode LOPA ne peut en aucun cas traiter d'une manière formellement correcte des situations réelles impliquant des scenarios d'accidents complexes. Cette complexité est due aux dépendances existantes entre les évènements initiateurs et les barrières de sécurité intervenant dans un scenario d'accident (ou plusieurs scenarios).

Par ailleurs, la vérification des SIL requis nécessite le calcul de la performance probabiliste (PFDmoy ou PFH) des Systèmes Instrumenté de Sécurité (SIS) concernés. Dans plusieurs cas de figures, l'usage des formules analytiques simplifiées ou certaines méthodes, telles que les arbres de défaillances (AdD) [4,5], présentent des limites liées aux éventuelles dépendances entre les éléments constitutifs des SIS.

Objectifs

Les Arbres de défaillance dynamique (DFT :Dynamic Fault Trees) [6] ont une bonne représentation sur les mécanismes de défaillances en modélisant les dépendances entre les événements à l'aide des portes statiques et dynamiques. Il existe dans la littérature plusieurs outils de résolution des DFT.

La démarche bayésienne représente une voie alternative qui permet de prendre en compte les dépendances représentées dans les DFT. Malheureusement la plupart des approches bayésiennes n'offrent pas un résultat exact de probabilité de l'événement sommet du DFT et n'intéressent pas aux calculs de fréquence, alors qu'il est un paramètre important de sûreté de fonctionnement et d'analyse des scénarios d'accident. A ce titre, l'objectif premier assigné à ce travail doctoral est d'investiguer et d'expliciter les possibles solutions offertes par les réseaux bayésiens [7].

Parmi les outils existant, les démarches algébriques qui offrent une évaluation qualitative et quantitative (calcul de probabilité) pour les DFT. Ce travail doctoral dispose une contribution dans ce sens et propose une démarche compréhensive de traitement des arbres de défaillance dynamique visant une analyse sur les deux dimensions qualitative et quantitative. Basé sur le travail de Merle et al. [8], nous détaillons la forme canonique de tout DFT grâce à des modèles algébriques pour les portes statiques et dynamiques en utilisant des opérateurs appropriés, puis les ensembles coupes / séquences seront développés afin d'exprimer la probabilité et la fréquence des sorties de portes et donc l'évaluation de la probabilité et de la fréquence de l'événement sommet du DFT. Ce modèle doit pouvoir évaluer les performances des systèmes relatifs à la sécurité d'une part et calculer la fréquence pour les scénarios LOPA d'autre part sans assumer aucune indépendance entre les événements de base.

Notre travail de thèse est structuré de la manière suivante :

Le premier chapitre est consacré à la présentation des différents concepts ayant trait aux barrières de sécurité. Plus précisément, la démarche de la norme CEI 61508 sera explicitée en terme de notions et de méthodes d'allocations et de vérification des SILs. Les formules classiques utilisées pour évaluer les performances des SIS et les fréquences des scénarios d'accident notamment les scénarios LOPA sont récapitulées. Ce chapitre permet de bien situer la problématique du travail doctoral.

Le deuxième chapitre est dédié à l'étude des différentes relations de dépendances (fonctionnelles et séquentielles sous l'arbre de défaillance dynamique) qui peuvent exister au niveau des scenarios d'accidents et dans les composants des systèmes relatifs à la sécurité (particulièrement les SIS). Cette tâche permet de bien préciser l'avantage de l'arbre de défaillance dynamique (DFT). Dans un second temps les outils de résolution du DFT notamment les chaines de Markov et les réseaux bayésiens sont bien éclairés.

Le but du troisième chapitre est de proposer une démarche algébrique traitant les arbres de défaillance dynamiques. Ce chapitre constitue une contribution doctorale majeure.

Cette démarche doit être capable de traiter les deux modes de fonctionnement des SIS (faible demande, demande élevée ou continue), et donc être capable de calculer la probabilité et la fréquence de défaillance de n'importe quel système relatif à la sécurité et d'évaluer la fréquence des scénarios LOPA sans assumer aucune indépendance entre les éléments du scénario (les couches de protection et l'événement initiateur). Les résultats de la démarche proposée sont comparés à ceux trouvés par les chaines de Markov.

Le quatrième chapitre est préservé pour souligne les avantages de l'usage des réseaux bayésiens par rapport d'autres méthodes classique telles que les arbres de défaillance. Dans un cas particulier les Réseaux Bayésien Temporel Discontinu (DTBN : Discrete Time Bayesian Network) [9] peut représenter les dépendances entre les composants avec la possibilité d'une évaluation temporelle continue du modèle. Ce formalisme bayésien spécifique est bien détaillé dans ce chapitre.

Du point de vue d'analyse, la démarche bayésienne adoptée est assignée à évaluer la probabilité a posteriori, telle que le calcul du dé-fiabilité et d'indisponibilité du système, les facteurs d'importance (sensibilité), la prédiction de l'état du système et le diagnostique.

Chapitre 1

Sécurité Fonctionnelle des Procédés Industriels

1.1 Introduction

Ce premier chapitre est entièrement consacré à introduire plusieurs termes et concepts tels que danger, risque, accident, sécurité, sécurité fonctionnelle et à décrire un résumé théorique d'une démarche de réduction des risques inhérents aux industries de procédé et leur maîtrise.

Dans ce type d'industries, la source de danger principale est l'ensemble des conditions d'exploitation du procédé lui-même figurées par ses dérives probables et non maîtrisées telles que les variations de pression, de température, de débit...

L'amplitude de ces dérives est généralement régulée par une action régulatrice assurée par un système de contrôle-commande qui mène le paramètre en question à sa valeur de référence, et qui peut cependant tomber en panne. Dans ce cas, le système est sauvé par l'intervention d'un opérateur et/ou de systèmes relatifs à la sécurité.

Le système instrumenté de sécurité (SIS) est un système relatif à la sécurité, qui représente souvent une partie intégrante du système de gestion de la sécurité [10] visant à maintenir le procédé en un état sûr (de sécurité) lorsqu'il se trouve dans une situation comportant un risque réel pour le personnel et l'environnement. Il est constitué d'une ou plusieurs fonctions sécurité assurant que les risques sont maintenus à un niveau acceptable. Ceci est habituellement assuré en effectuant un arrêt partiel ou total du processus afin de prévenir l'événement redouté ou d'en atténuer les conséquences.

Les recommandations en matière de fonctions de sécurité sont abordées dans les normes internationales CEI 61508 [1] et CEI 61511 [2] qui sont largement reconnues comme étant des prescriptions relatives à la spécification, la conception et le fonctionnement des SIS. La fonction de sécurité est spécifiée en termes de calcul de probabilité de défaillance requise qui traduit la détermination du niveau d'intégrité de sécurité (SIL) assigné au SIS. Les normes CEI offrent un cadre pour la détermination du SIL et proposent différentes méthodes pour déterminer les performances du SIS [11]. A la fin du processus de réduction de risque, nous décrivons les formules classiques utilisées pour évaluer les performances des SIS et les fréquences des scénarios d'accident notamment les scénarios LOPA.

1.2 Concepts Généraux

1.2.1 Notion de danger

Selon Desroches [12] et la norme CEI 61508, le danger désigne une nuisance potentielle pouvant porter atteinte aux personnes, aux biens ou à l'environnement. Les dangers peuvent avoir une incidence directe sur les personnes, par des blessures physiques ou des troubles de la santé, ou indirecte, au travers de dégâts subis par les biens ou l'environnement.

Le référentiel OHSAS 18001 [13] définit le danger comme étant une source ou une situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments.

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

1.2.2 Notion de risque

La perception des dommages potentiels liés à une situation dangereuse se rapporte à la notion de risque. Les risques peuvent être de nature très variée. Beaucoup de classifications ont été proposées mais les définitions du risque à deux dimensions sont courantes et assez proches.

Selon Villemeur [14], le risque est une mesure d'un danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences.

Selon OHSAS 18001 [13], un risque est la combinaison de la probabilité et de la (des) conséquence (s) de la survenue. Selon Gouriveau [15], le risque peut être défini par l'association d'événements causes et conséquences d'une situation donnée. Les événements causes peuvent être caractérisés par leur occurrence (P) et les événements-effets par leur impact (I) (voir Figure 1.1). La corrélation de ces grandeurs permet de construire un indicateur de risque R = *f* (Occurrence, Impact).

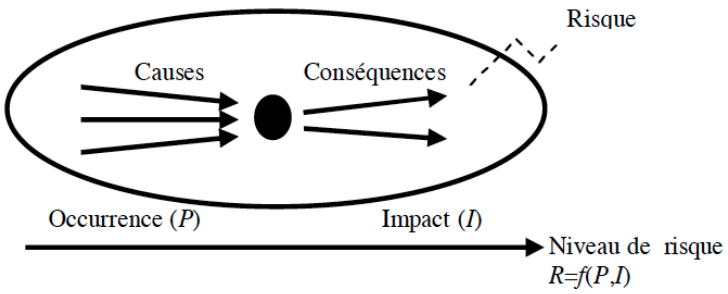

Figure 1.1 Caractérisation du risque [15]

1.2.3 Notion de sécurité

La sécurité est souvent définie par rapport à son contraire. Elle est l'absence de danger, d'accident ou de sinistre.

On peut définir la sécurité d'un système comme étant son aptitude à fonctionner ou à dysfonctionner sans engendrer d'événements dangereux pouvant porter atteinte à l'intégrité du système lui-même et à son environnement notamment humain.

Suivant le guide du management du risque [16] élaboré par l'ISO sur la terminologie du management du risque, la sécurité est l'absence de risque inacceptable, de blessure ou d'atteinte à la santé des personnes, directement ou indirectement, résultant d'un dommage au matériel ou à l'environnement.

1.2.4 Fonction de sécurité

La fonction de sécurité est la fonction qui doit être réalisée par un système relatif à la sécurité, en vue de maintenir le système à protéger en état sécurisé.

La sécurité fonctionnelle, selon la norme CEI 61508 est un sous ensemble de la sécurité globale qui se rapporte au système commandé et qui dépend du bon fonctionnement des systèmes relatifs à la sécurité basée sur une autre technologie et des dispositifs externes de réduction de risque.

Selon la norme CEI 61511, la sécurité fonctionnelle est un sous ensemble de la sécurité globale qui se rapporte à un système de commande de processus de base (BPCS, Basic Process Control System) et qui dépend du fonctionnement correct du système instrumenté de sécurité (SIS) et d'autres couches de protection.

1.3 Cycle de vie proposé par la norme CEI 61508

La norme CEI 61508 est la norme la plus usuelle concernant la sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables (E/E/PE) liés à la sécurité. Elle est considérée comme une norme générique couvrant plusieurs secteurs d'activité. La Figure 1.2 montre la norme CEI 61508 générique et ses normes filles selon le champ d'application.

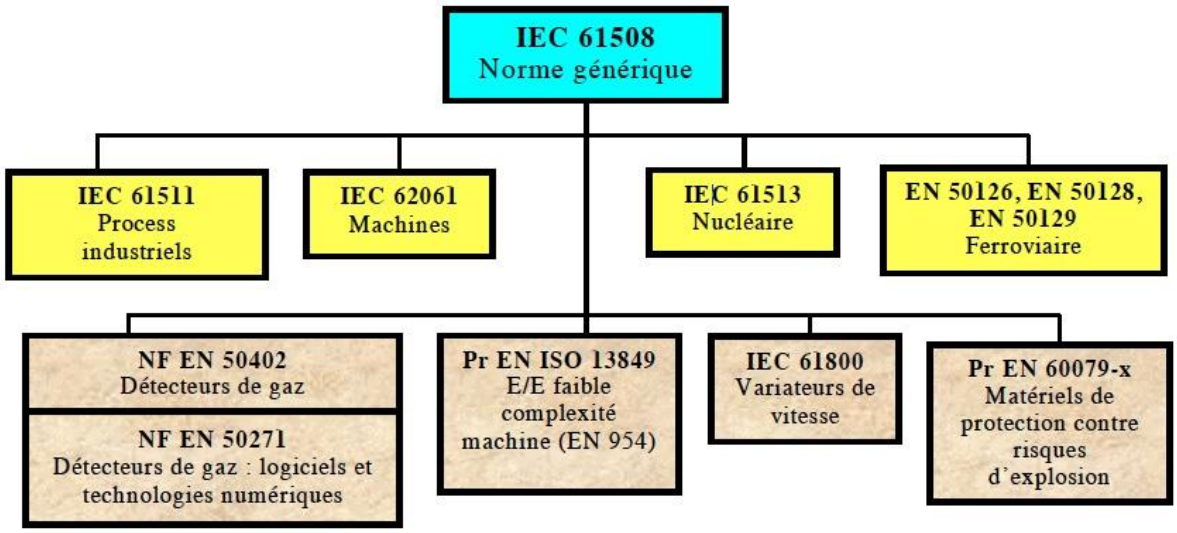

Figure 1.2 La norme CEI 61508 et ses déclinaisons sectorielles [17]

La norme CEI 61511 est apparue comme une des déclinaisons de la CEI 61508. Elle utilise la notion de systèmes instrumentés de sécurité (SIS) au lieu de systèmes relatifs à la sécurité.

La norme CEI 61508 propose une démarche opérationnelle permettant de mettre en place et gérer un système E/E/PE depuis la phase initiale de spécification jusqu'à leur mise hors service, en passant par leur conception, leur installation, leur exploitation et leur maintenance à partir d'une étude de prescriptions de sécurité issues d'une analyse et évaluation des risques. Cette démarche est basée sur un modèle de sécurité globale bien défini dans CEI 61508 sous le nom de cycle de vie de sécurité. La Figure 1.3 représente un modèle de cycle de vie de sécurité global proposé par la norme CEI 61508 afin de couvrir toutes les activités à réaliser pour assurer la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité depuis la phase initiale de spécification jusqu'à leur mise hors service, en passant par leur conception, leur installation, leur exploitation et leur maintenance.

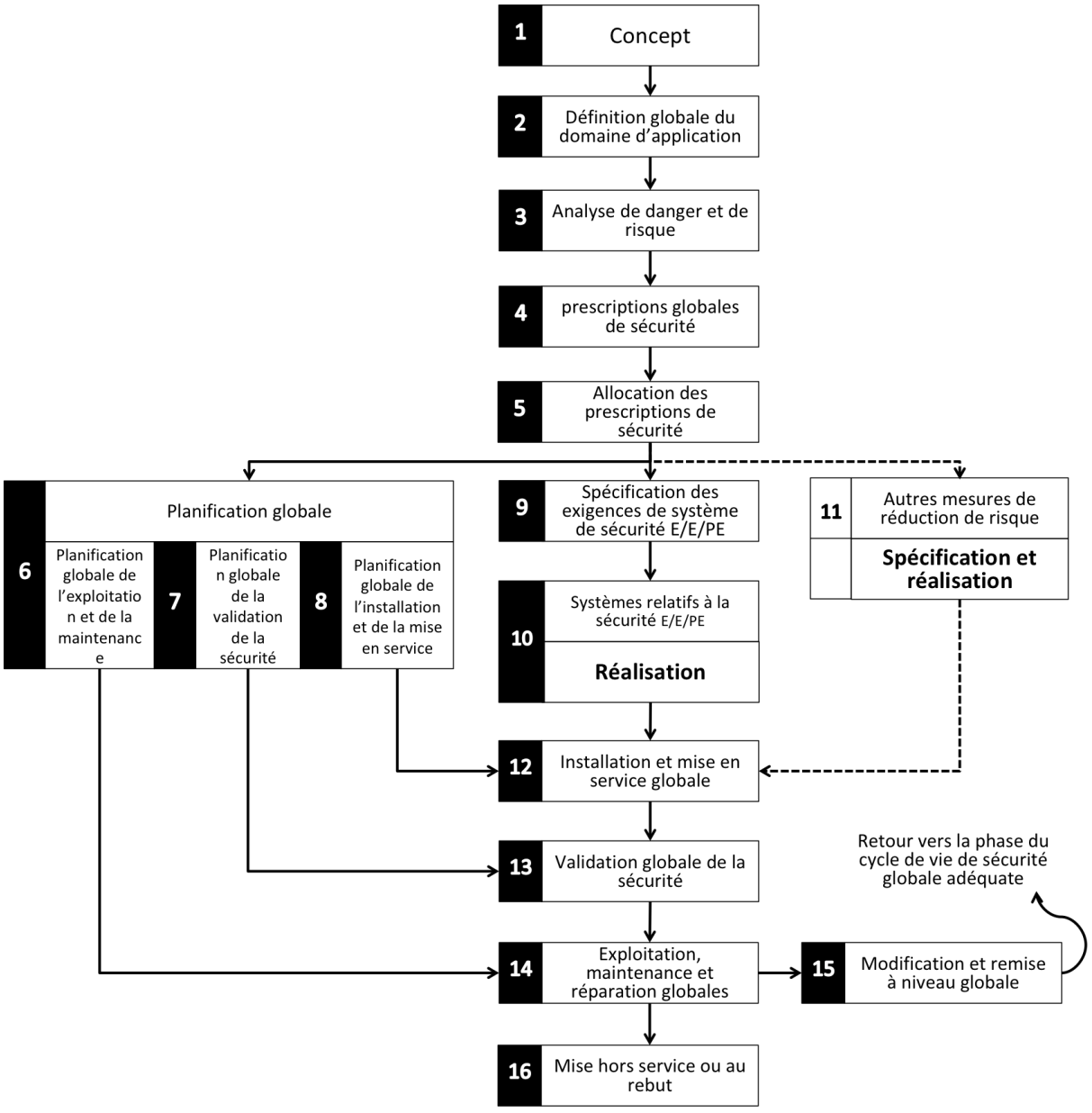

Figure 1.3 Cycle de vie de sécurité global proposé par la norme CEI 61508 [1]

Pour couvrir tous les aspect des systèmes E/E/PE relatifs à la sécurité, la norme CEI 61508 se compose de sept parties comme suit :

- La norme 61508-1 présente les définitions des prescriptions générales.
- La norme 61508-2 traite les prescriptions spécifiques et l'aspect matériel des

systèmes E/E/EP.

- La norme 61508-3 dédiée à la présentation des prescriptions spécifiques et l'aspect logiciel des Systèmes E/E/EP.

- La norme 61508-4 présente les définitions et les abréviations utilisées.

- La norme 61508-5 donne des exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité.

- La norme 61508-6 fournit les guides d'application des parties 2 et 3 de la norme.

- La norme 61508-7 présente les techniques et les mesures recommandées lors de la validation des systèmes E/E/EP.

1.4 Allocation des prescriptions de sécurité

L'objectif d'une démarche de management du risque est d'atteindre un niveau de risque acceptable représentant le seuil en dessous duquel on accepte l'existence du danger et bien que sa gravité et sa probabilité d'occurrence ne soient pas nulles.

La réduction du risque (ou maîtrise du risque) désigne l'ensemble des actions ou dispositions entreprises en vue de diminuer la probabilité ou la gravité des dommages associés à un risque particulier [18]. Cela passe par l'identification des sources de danger et les barrières de sécurité existantes et l'estimation des risques associés afin de comparer les grandeurs retenus (probabilité d'occurrence et gravité) à un niveau acceptable ou tolérable. Si le risque considéré est jugé inacceptable, la différence trouvée par rapport aux critères d'acceptation définit l'ampleur de la réduction nécessaire du risque. Cette réduction nécessaire mène à définir les prescriptions globales de sécurité chargées par des systèmes relatifs à la sécurité et/ou des barrières de sécurité supplémentaires qui exécutent des fonctions de sécurité.

1.4.1 Risque tolérable et principe ALARP

Décider qu'un risque est tolérable ou non est une tâche compliquée. Le "Health and Safety Executive" a lancé un modèle de risque tolérable sous le nom d'ALARP (As Low As Reasonably Practicable) [1,19]. L'utilisation du principe ALARP signifie que le risque devrait être réduit à un niveau aussi bas que raisonnablement possible (voir Figure 1.4).

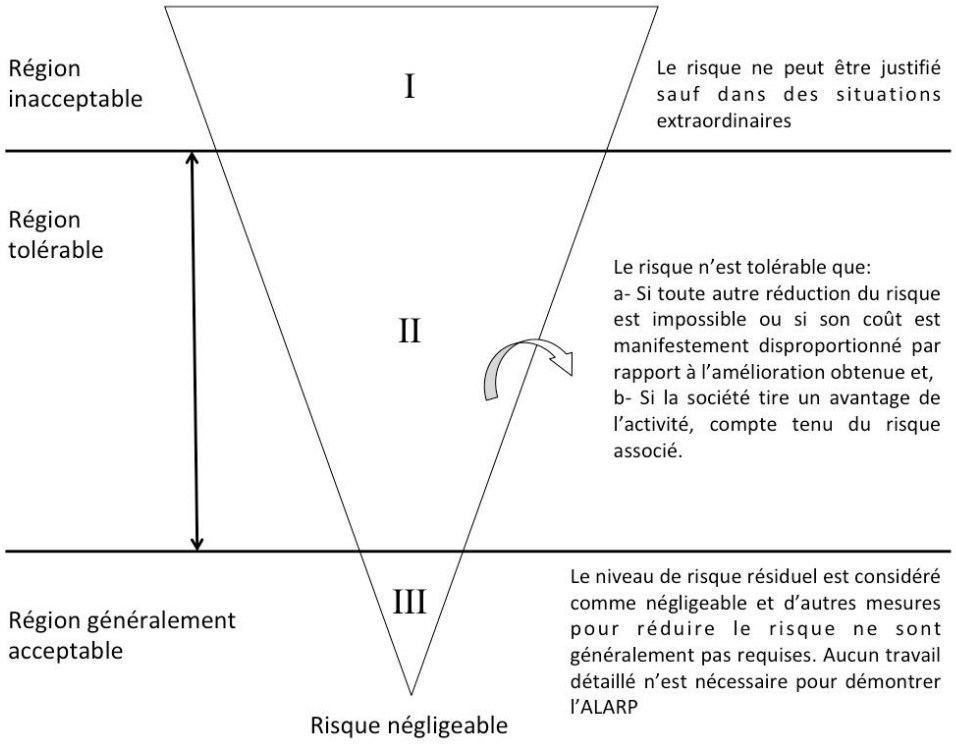

Figure 1.4 ALARP et risque tolérable [1]

La Figure 1.4 montre qu'il existe trois zones de classification des niveaux de risques. Un niveau de risque intolérable, au-delà duquel tout risque n'est justifiable d'aucune manière et est donc inacceptable. Cela correspond à la zone supérieure du schéma (zone I). En deçà de cette zone se situe la zone ALARP (zone II), pour laquelle tout risque peut être accepté si toute réduction supplémentaire du risque est incompatible ou si son coût est manifestement disproportionné vis-à-vis de l'amélioration qu'il permet d'obtenir, et si la société tire un avantage de l'activité, compte tenu du risque associé. La zone inférieure (zone III) est celle du risque résiduel dont le niveau est négligeable et donc ne nécessite aucune réduction

supplémentaire.

L'application du principe ALARP nécessite la définition d'une échelle de cotation du risque dont chacune des classes correspond à une zone du modèle ALARP. Les Tableaux 1.1 et 1.2 ci-dessous sont complémentaires, ils représentent respectivement, un exemple de classes de risque et leur correspondance aux zones [2]. Ces matrices de criticité sont sujettes des discussions par les parties intéressées en basant sur des critères et références communes pour être adaptées à chaque secteur d'activité, et cela par proposer et illustrer des classes (gravité et probabilité/fréquence) correspondent aux couples conséquence/cause des risques identifies.

Tableau 1.1 Exemple de classification des risques d'accidents [2]

Probabilité	Classes de risque			
	Conséquence catastrophique	Conséquence critique	Conséquence marginale	Conséquence négligeable
Fortement probable	I	I	I	II
Probable	I	I	II	II
Possible	I	II	II	II
Peu possible	II	II	II	III
Improbable	II	III	III	III
Invraisemblable	II	III	III	III

Tableau 1.2 Correspondance entre classes et zones de risque [2]

Classe de risque	Interprétation
Classe I	Risque intolérable
Classe II	Risque indésirable et uniquement tolérable si la réduction du risque est impossible ou si les coûts sont manifestement disproportionnés par rapport aux améliorations obtenues
Classe III	Risque négligeable

1.4.2 Détermination des niveaux d'intégrité de sécurité SIL requis

Après avoir déterminer la limite de sécurité exigée. Les étapes de réduction de risques seront effectues ci-après jusqu'à la détermination du niveau d'intégrité se sécurité requis en proposant le cas d'un procédé industriel qui peut être représenté se forme d'un équipement à protéger (EUC : Equipment Under Control) et ses systèmes de sécurité (voir l'exemple de l'annexe B de la norme ISO 61511[2]).

Une fonction de sécurité exécutée par un SIS est une fonction de sécurité instrumentée (SIF : Safety Instrumented Function) caractérisée par son niveau d'intégrité de sécurité (SIL: Safety Integrity Level) représentant la quantité de réduction de risque à achever [20]. En général l'intégrité de sécurité peut être définie comme suit : probabilité pour qu'un système E/E/EP relatif à la sécurité exécute de manière satisfaisante les fonctions de sécurité requises dans des conditions spécifiées et pour une période de temps spécifiée.

La fonction SIF est déclenchée automatiquement par un SIS suite à la détection d'une dérive dangereuse dans un procédé industriel. La méthode HAZOP (HAZard and OPerability study) [21] est souvent utilisée comme étant un outil préalable pour l'analyse des risques liés aux industries chimiques et pétrochimiques dans le but d'identifier les dérives potentielles qui peuvent générer des accidents à effets majeurs. La dérive principale ou la plus dangereuse représente généralement l'évènement initiateur (EI) qui est sujet d'une évaluation de sa fréquence d'occurrence. Cette valeur peut être fournie par la littérature [22,23], les bases de données [24] et/ou les jugements d'experts [25], ou bien calculée à l'aide d'une analyse par arbre de défaillance (AdD) basée sur des mesures de fréquences et d'indisponibilités des événements de base constituant l'événement sommet (ES) qui peut représenter par exemple la défaillance d'un système de contrôle et régulation du procédé à savoir le BPCS.

La deuxième étape sert à définir les dispositifs de sécurité existants qui empêchent l'événement initiateur de se propager et donner des conséquences indésirables. Ces dispositifs de sécurité jouent le rôle de couches de protection (PL: Protection Layer) assurant des fonctions de sécurité faisant réduire la fréquence initiale de l'événement initiateur.

Il s'agit donc de calculer la nouvelle fréquence de l'événement redouté (ER) ou du scenario d'accident ayant la conséquence la plus grave sur l'homme, l'environnement et l'installation. Ce résultat est obtenu par la multiplication des probabilités de défaillance des couches de protection par la fréquence de l'événement initiateur comme suit :

$$fr(ER) = fr(EI) \cdot \prod_i Pr(PL_i) \tag{1.1}$$

La formule précédente est utilisée lorsque les barrières de sécurité sont indépendantes entre eux et entre l'événement initiateur [26]. Si la valeur de fréquence de l'événement redouté excède la valeur seuil tolérable représentée par la fréquence de l'événement tolérable (ET) préétablie ($fr(ER) > fr(ET)$), il est nécessaire de rajouter une fonction de sécurité supplémentaire intégrée dans un SIS afin de mettre la quantité de réduction du risque non obtenue par les couches de protection. La formule suivante décrit la fréquence d'occurrence de l'événement redouté en intégrant le SIS :

$$fr(ER) = fr(EI) \cdot \prod_i Pr(PL_i) \cdot Pr(SIS) \tag{1.2}$$

Il convient donc de vérifier l'aptitude du SIS implémenté à satisfaire la SIF requise qui est caractérisée par un niveau d'intégrité SIL requis comme mentionné dans les Tableaux 1.3 et 1.4. Pour mieux comprendre la démarche d'allocation du SIL, nous considérant le procédé dans la Figure 1.5. Le système est un condensateur d'ammoniac (NH_3), sa fonction est de convertir le gaz contenant du NH_3 en ammoniaque liquide. Un système de régulation de pression (RP) est adopté pour maintenir la pression interne dans ce récipient à une valeur nominale pour maitriser une dispersion probable du gaz toxique dans l'atmosphère. En cas d'une défaillance du système de régulation, l'opérateur réagit suite à une augmentation de pression détectée par l'alarme. Si le système Alarme/Opérateur (A/O) ne réagit pas, un système d'arrêt d'urgence (AU) est prévu pour couper l'alimentation du gaz. La Figure 1.6 représente l'arbre d'événements relatif au scénario d'accident « Dispersion du gaz toxique (NH_3) dans l'atmosphère ».

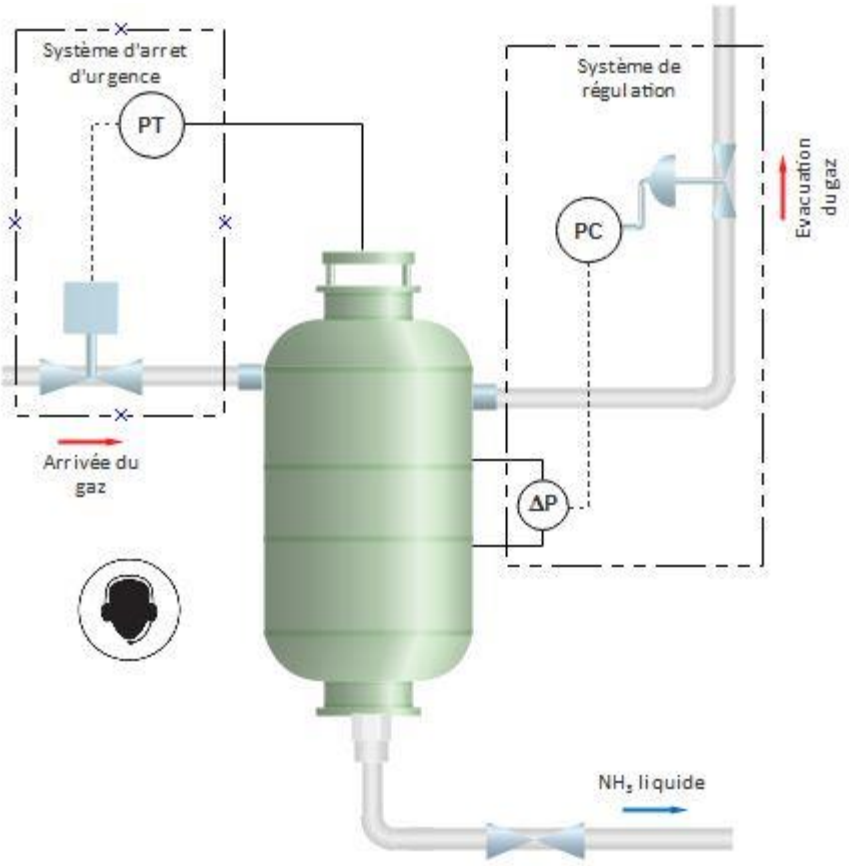

Figure 1.5 Condensateur d'ammoniac et ses systèmes de sécurité

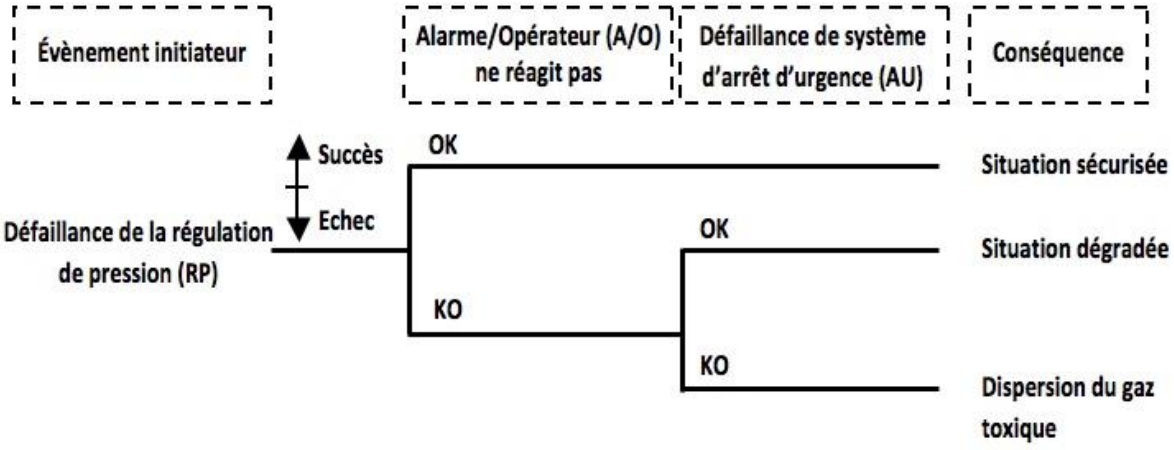

Figure 1.6 Arbre d'événements du scénario d'accident : Dispersion du gaz toxique

La surpression caractérisée par la défaillance du système de régulation est donc l'événement initiateur direct de l'événement redouté dispersion du gaz dans l'environnement, dont il va falloir comparer la fréquence d'occurrence à celle du risque tolérable prédéfinie. Il est donc nécessaire d'évaluer la fréquence d'occurrence de la surpression. On suppose que l'analyse par AdD donne, pour l'événement initiateur, une fréquence annuelle d'occurrence de l'ordre de 0,1. Pour le système Alarme/Opérateur, on présume une valeur de probabilité de défaillance de $5 \cdot 10^{-2}$. Si l'on ne considère pas le système d'arrêt d'urgence, la fréquence d'occurrence de l'événement redouté est obtenue par multiplier la fréquence de l'événement initiateur par la probabilité de défaillance de la seule couche de protection (Système Alarme/Opérateur). Cette valeur est comparée au seuil tolérable qualifie par exemple de $10^{-4} \ / \ an$ ($5 \cdot 10^{-3} > 10^{-4}$). Il convient donc de réduire la valeur calculée en implémentant une fonction de sécurité intégrée dans le système d'arrêt d'urgence dont la contribution devrait permettre d'assurer la maîtrise du risque requise. Il est donc nécessaire de vérifier la capacité de ce système à exécuter correctement la fonction de sécurité supplémentaire requise. Autrement dit, quelle est la valeur de probabilité de défaillance à la demande du système d'arrêt d'urgence nécessaire pour que la fréquence d'occurrence de l'événement redouté soit inférieur au seuil tolérable ($fr(ER) < 10^{-4}$). La valeur de probabilité limite est donnée par la formule suivante :

$$Pr(AU) \leq \frac{fr(ET)}{fr(EI) \cdot Pr(A/O)} \leq \frac{10^{-4}}{5 \cdot 10^{-3}} \leq 2 \cdot 10^{-2} \qquad (1.3)$$

La valeur de probabilité de défaillance du système d'arrêt d'urgence nécessaire pour que le risque soit tolérable doit être donc inférieur à $2 \cdot 10^{-2}$. Cela renvoie à la détermination d'un niveau SIL assurant une fréquence de l'événement redouté inférieur à $10^{-4}/an$.

1.5 Modes de fonctionnement d'un SIS

Les prescriptions concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux SIS sont spécifiées en termes de SIL. Cependant, le SIL est divisé habituellement en quatre niveaux discrets possibles allant du SIL1 au SIL4. Les normes CEI 61508 et CEI

61511 considèrent les valeurs moyennes de probabilité de défaillance dangereuse pour la détermination du SIL tout dépend de la manière de sollicitation du SIS.

1.5.1 Mode de fonctionnement à faible sollicitation

Ce mode de fonctionnement correspond à une fréquence d'activation du SIS inférieure ou égale à 1 an^{-1} ou inférieure ou égale au double de la fréquence des tests périodiques auxquels il est soumis. Dans ce cas, la mesure de performance appropriée de la SIF est sa probabilité moyenne de défaillance sur demande PFD_{moy} (Average Probability of Failure on Demand). L'équation (1.2) devient :

$$fr(ER) = fr(EI) \cdot \prod_i Pr(PL_i) \cdot PFD_{moy}(SIS) \tag{1.4}$$

Le risque n'est toléré que si la valeur de l'événement redouté est inférieure ou égale à la valeur limite tolérable. La valeur $PFD_{moy}(SIS)$ requise peut être obtenue comme suit :

$$fr(ER) = fr(EI) \cdot \prod_i Pr(PL_i) \cdot PFD_{moy}(SIS) \leq fr(ET) \tag{1.5}$$

Nous avons donc :

$$PFD_{moy}(SIS) \leq \frac{fr(ET)}{fr(EI) \cdot \prod_i Pr(PL_i)} \tag{1.6}$$

1.5.2 Mode de fonctionnement forte sollicitation ou sollicitation continue

Ce mode correspond à une fréquence d'activation du SIS supérieure à 1 an^{-1} ou supérieure au double de la fréquence des tests périodiques auxquels il est soumis. Dans ce cas, la mesure de performance appropriée de la SIF est une valeur moyenne de probabilité de défaillance dangereuse par heure appelée PFH (Probability of Failure per Hour). Dans ce cas l'événement initiateur est représenté par la défaillance du SIS, et la fréquence de l'événement redouté peut être obtenue en remplaçant $fr(EI)$ par $PFH(SIS)$ dans l'équation (1.7) comme suit :

$$fr(ER) = fr(EI) \cdot \prod_i Pr(PL_i) \quad (1.7)$$

Comme nous avons vu pour le mode précédent, la valeur $PFH(SIS)$ requise est obtenu en insérant la fréquence de l'événement tolérable, nous obtenons :

$$fr(ER) = PFH(SIS) \cdot \prod_i Pr(PL_i) \leq fr(ET) \quad (1.8)$$

Nous avons donc :

$$PFH(SIS) \leq \frac{fr(ET)}{\prod_i Pr(PL_i)} \quad (1.9)$$

Les Tableaux 1.3 et 1.4 montrent les niveaux SIL et les exigences probabilistes correspondantes exprimées en termes de PFD_{moy} et PFH suivant le mode de fonctionnement du SIS.

Tableau 1.3 SIL en mode faible demande [1]

Niveau d'Intégrité de Sécurité (SIL)	**Probabilité moyenne de défaillance sur demande (PFD_{moy})**
4	$\geq 10^{-5}$ à $< 10^{-4}$
3	$\geq 10^{-4}$ à $< 10^{-3}$
2	$\geq 10^{-3}$ à $< 10^{-2}$
1	$\geq 10^{-2}$ à $< 10^{-1}$

Tableau 1.4 SIL en mode forte demande ou demande continue [1]

Niveau d'Intégrité de Sécurité (SIL)	**Probabilité de défaillance dangereuse par heure (PFH)**
4	$\geq 10^{-9}$ à $< 10^{-8}$
3	$\geq 10^{-8}$ à $< 10^{-7}$
2	$\geq 10^{-7}$ à $< 10^{-6}$
1	$\geq 10^{-6}$ à $< 10^{-5}$

D'après les deux Tableaux ci-dessus la détermination du niveau SIL d'une SIF requiert

le calcul des performances probabilistes du SIS (PFD_{moy} ou PFH) suivant son mode de sollicitation. On constate aussi que plus le SIL a une valeur élevée, plus la réduction du risque est importante.

Il est essentiel de noter ici que le calcul de la fréquence de l'événement redouté et les probabilités requises du SIS (PFD_{moy} et PFH) n'est possible via les formules précédentes que si les éléments du scenario d'accident (l'événement initiateur, le SIS et les couches de protection) sont indépendants [26,27]. Contrairement, s'il existe des dépendances entre les événements, ce qui est par exemple le cas pour les systèmes complexes, le calcul mène finalement à une détermination imprécise du SIL.

1.6 Composition du SIS

Un SIS est un ensemble d'éléments (matériel et logiciel) assurant la mise en état de sécurité des procédés lorsque des conditions prédéterminées sont atteintes. Il se compose de n'importe quelle combinaison de trois sous-systèmes (capteurs, unité logique et éléments terminaux). La norme CEI 61508 définit les SIS comme suit : un système E/E/PE (électrique/électronique/électronique programmable) relatifs aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité.

L'architecture type d'un SIS est donnée à la Figure 1.7. Voici un descriptif succinct de chacune de ses parties :

- **Eléments d'entrée :** constitués d'un ensemble d'éléments d'entrée (capteurs, détecteurs) qui surveillent l'évolution des paramètres représentatifs du comportement de l'EUC (température, pression, débit, niveau…).

- **Unité logique :** comprend un ensemble d'éléments logiques qui récoltent l'information provenant du sous-système E et réalisent un processus de décision, par l'activation du sous-système F dans le cas où l'un des paramètres dévie au-delà d'une valeur-seuil.

- **Eléments finaux :** agissent directement (vanne d'arrêt d'urgence) ou indirectement (vanne solénoïdes) sur le procédé pour neutraliser la dérive remarquée en mettant la situation dans un état sûr.

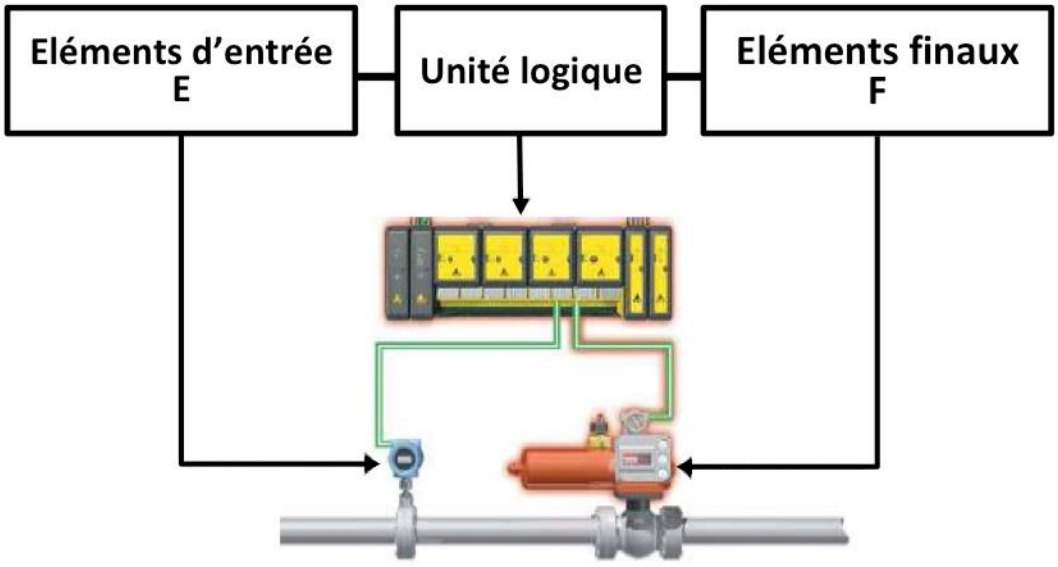

Figure 1.7 Exemple d'un SIS [17]

1.7 Conclusion

Dans ce premier chapitre nous avons d'abord rappelé les définitions des termes fondamentaux du domaine de la sécurité et la sécurité fonctionnelle, particulièrement la sécurité des procédés industriels afin de positionner notre problématique. Nous avons ensuite précisé le modèle de la sécurité globale proposé par la norme CEI 61508 et sa composition et ses déclinations sectorielles qui est le document de référence de la sécurité fonctionnelle.

La deuxième partie de ce chapitre décrit, à partir de la notion du risque tolérable et de l'identification et évaluation des risques inhérents aux procédés, les prescriptions de sécurité en termes de niveau d'intégrité de sécurité requis et par conséquent l'ampleur de la réduction du risque chargée par le système instrumenté de sécurité (SIS) implémenté.

Pour s'assurer qu'un SIS donné est capable de remplir sa fonction de sécurité prévue, il est devenu habituel d'estimer ses performances en termes de son PFDmoy s'il fonctionne dans un mode à faible demande et son PFH pour les modes à demande forte et continue. Cette tâche pourrait être atteint grâce à l'utilisation des formules relatives aux scénarios d'accident en prenant en compte les composantes de chaque scenario (ses couches de protection et son événement initiateur). Le calcul via ses formules propose l'indépendance entre les éléments du scénario, alors que ce n'est pas toujours le cas pour les systèmes complexes où des dépendances fonctionnelles et séquentielles sont persistes, et ce qui rend aussi l'utilisation des divers outils de fiabilité tels que les diagrammes fonctionnels, les arbres de défaillance donnent des résultats erronés [28]. Dans la suite de ce travail, nous discutons comment calculer précisément ces indicateurs de performance en prenant en compte les différents types de dépendances.

Chapitre 2

Arbre de défaillance dynamique et outils de résolution

2.1 Introduction

L’arbre de défaillances (AdD) a été introduit en 1962 chez Bell Telephone Laboratories, dans le cadre d’une évaluation de la sécurité du système de lancement du missile intercontinental « Minuteman ». Aujourd'hui, l’arbre de défaillance est l'une des techniques les plus couramment utilisées pour les études de risque et de fiabilité. Une analyse par l’AdD peut être qualitative ou/et quantitative, en fonction des objectifs attendus. Les résultats possibles de l'analyse peuvent, par exemple, être:

- Une liste des combinaisons possibles de facteurs environnementaux, d'erreurs humaines et de défaillances de composants pouvant entraîner un événement critique dans le système.

- La probabilité que l'événement critique se produira pendant un intervalle de temps spécifié.

L’AdD est une technique déductive dans laquelle nous commençons par une défaillance du système ou un accident. La défaillance du système, ou l’accident, représente l'événement sommet. Les événements intermédiaires dont seuls ou en combinaison, peuvent conduire à l'événement sommet sont identifiés et connectés entre eux et à cet événement des portes logiques. Ensuite, nous identifions tous les événements causaux potentiels qui peuvent

conduire à ces événements intermédiaires. Les événements causaux d'un événement intermédiaire sont connectés via une porte logique. Cette procédure est poursuivie par déduction (c.-à-d. en arrière dans la chaîne causale) jusqu'à ce que nous atteignions un niveau de détail approprié. Les événements du niveau le plus bas sont appelés des événements de base de l'AdD.

L'arbre de défaillance dynamique (DFT : Dynamic Fault Tree) a été introduit en tant qu'extension de l'AdD pour modéliser les défaillances séquentiellement dépendantes dans les systèmes dynamiques [6]. Dans un système dynamique, la séquence d'événements de défaillance est aussi importante que leurs combinaisons pour que le système soit indisponible ou en panne. En d'autres termes, par rapport à l'AdD dans laquelle seuls les composants participent à une coupe minimale, dans le DFT, la séquence de défaillance des composants est également importante [29]. Le DFT prend en compte les dépendances séquentielles en utilisant plusieurs portes dynamiques telles que la porte de dépendance fonctionnelle (FDEP), la porte de secours (SPARE), la porte d'application séquentielle (SEQ) et la porte ET prioritaire PAND [6].

En raison des dépendances séquentielles et du comportement dynamique des composants du système, le DFT ne peut pas être analysé à l'aide des algorithmes conventionnels disponibles pour l'AdD traditionnel. À cet égard, le DFT a toujours été convertie en modèle de chaîne de Markov correspondant pour lequel des techniques de résolution bien établies et efficaces ont été développées [30].

Les réseaux bayésiens (RB) offrent une représentation graphique parfaite sur le mécanisme de défaillance et les combinaisons existantes entre les composants du système. Les auteurs dans [31] ont fait une comparaison entre RB et les arbres de défaillance. La conversion de l'arbre de défaillance dynamique (DFT) en un réseau bayésien dynamique (RBD) [32] est une technique bien connue pour représenter le caractère séquentiel du processus de défaillance [33,34].

2.2 Rappels de quelques mesures de sûreté de fonctionnement

2.2.1 Fiabilité

La fiabilité d'un système S à l'instant t est mesurée par la probabilité, notée $R_S(t)$, que le système ne connaisse aucune défaillance sur la durée [0, t]. On a donc :

$$R_S(t) = Pr(t < T) \tag{2.1}$$

Où T est la durée de vie du système S.

La probabilité de l'événement complémentaire est la dé-fiabilité, notée $F_S(t)$.

$$F_S(t) = 1 - R_S(t) = Pr(t \geq T) \tag{2.2}$$

Où $F_S(t)$ est la fonction de répartition.

2.2.2 Densité de défaillance

Notée $f_S(t)$, elle s'exprime la densité de probabilité de la variable aléatoire t. Elle représente la dérivée de la fonction de répartition $F_S(t)$.

$$f_S(t) = \frac{dF_S(t)}{dt} \tag{2.3}$$

La quantité $f_S(t)dt$ exprime la probabilité que le système S défaille entre t et $t + dt$, sachant qu'il était en état de marche à $t = 0$.

2.2.3 Taux de défaillance

Noté $\lambda_S(t)$, il est défini de la façon suivante :

$$\lambda_S(t) = \lim_{dt \to 0} \frac{Pr\{S \text{ défaille entre } t \text{ et } t+dt/D\}}{dt} \tag{2.4}$$

L'événement D signifie que le système S n'a connu aucune défaillance sur la durée $[0, t]$.

D'après la relation de Bayes nous avons :

$$Pr\{S \text{ défaille entre } t \text{ et } t+dt/D\} = \frac{Pr\{(S \text{ défaille entre } t \text{ et } t+dt) \cap D\}}{Pr(D)} \qquad (2.5)$$

On peut donc écrire :

$$\lambda_S(t) = \lim_{dt\to 0} \frac{1}{dt} \cdot \frac{Pr\{(t < T \geq t+dt) \cap (t < T)\}}{Pr(t < T)}$$

$$\lambda_S(t) = \frac{1}{R_S(t)} \lim_{dt\to 0} \frac{F_S(t+dt)-F_S(t)}{dt} = \frac{1}{R_S(t)} \lim_{dt\to 0} \frac{-\left(R_S(t+dt)-R_S(t)\right)}{dt}$$

$$\lambda_S(t) = \frac{-\frac{dR_S}{dt}(t)}{R_S(t)} \qquad (2.6)$$

En intégrant des deux membres, on obtient :

$$R_S(t) = exp\left(-\int_0^t \lambda_S(u)\, du\right) \qquad (2.7)$$

2.2.4 Intensité de défaillance inconditionnelle

$w_S(t)$ ou encore fréquence de défaillance, elle est définie par la formule :

$$w_S(t) = \lim_{dt\to 0} \frac{Pr\{S \text{ défaille entre } t \text{ and } t+dt/E\}}{dt} \qquad (2.8)$$

L'événement E signifie que le système S était en état de marche à l'instant $t = 0$.

L'intensité de défaillance inconditionnelle peut être obtenue à l'aide de la propriété suivante [35]:

$$w_S(t) = \lambda_S^v(t) \cdot A_S(t) \qquad (2.9)$$

Où $\lambda_S^v(t)$ et $A_S(t)$ représentent respectivement l'intensité de défaillance conditionnelle et l'indisponibilité du système S. $\lambda_S^v(t)$ est appelé aussi taux de défaillance de Vesely [36].

Si le système S est non-réparable et il était en état de marche à l'instant $t = 0$, $\lambda_S(t) = \frac{\left(\frac{dF_S(t)}{dt}\right)}{1-F_S(t)}$ et $A_S(t) = 1 - F_S(t)$. Par conséquent, nous obtenons l'égalité suivante :

$$w_S(t) = \frac{dF_S(t)}{dt} = f_S(t) \tag{2.10}$$

2.3 Caractère dynamique de l'arbre de défaillance dynamique

Les portes dynamiques du DFT telles que définies par Dugan et al. [6] sont : la porte prioritaire PAND, la porte de dépendance fonctionnelle (FDEP), la porte de secours (SPARE) et la porte séquentielle SEQ. Elles sont utilisées pour capturer le comportement dynamique entre les événements, comme expliqué ci-après :

- La porte PAND : C'est une porte AND en plus de la condition que les événements doivent se produire dans un ordre spécifique. Dans une porte PAND de deux événements A et B (voir la Figure 2.1a), la sortie est vrai seulement et seulement si : A et B se produisent simultanément et A se produit avant B (on choisit un seul ordre parmi deux).

- La porte de dépendance fonctionnelle (FDEP) : Cette porte est composée d'un événement déclencheur et une série de composants en dépendance. Lorsque l'événement déclencheur se produit, il cause l'inaccessibilité ou l'indisponibilité des autres composants. Pour le cas de la Figure 2.1b, l'un des deux événements A et B se produit s'il est forcé de devenir inaccessible par l'occurrence de l'événement déclencheur (T) ou s'il se produit lui-même. Cette porte est composée d'un événement déclencheur et une série de composants en dépendance. Lorsque l'événement déclencheur se produit, il cause l'inaccessibilité ou l'indisponibilité des autres composants.

- La porte de secours (Figure 2.1c) : Dans le cas d'une porte avec un événement primaire A et un événement de réserve B, on distingue deux modes de défaillance (actif et dormant) en prenant les deux variables Ba et Bd. La sortie de la porte de rechange se produit si son composant principal tombe en panne et que le composant de secours tombe en panne.

L’événement de réserve peut survenir à la fois dans l'état de veille et dans l'état de fonctionnement: si son taux de défaillance dans l'état de fonctionnement est λ, son taux de défaillance est αλ, α étant le facteur de dormance ($0 \leq \alpha \geq 1$). La porte de rechange (SPARE) est plus précisément appelée «porte de secours douillet (WSP : warm spare gate)» si $\alpha < 1$, «porte de secours chaude (HSP : hot spare gate)» si $\alpha = 1$ et «porte de rechange froide (CSP : cold spare gate)» si $\alpha = 0$.

- La porte séquentielle (SEQ) : Pour une porte séquentielle avec n événements de base (voir la Figure 2.1d), les événements sont forcés de se produire dans un ordre particulier (un seul choix) de gauche à droite.

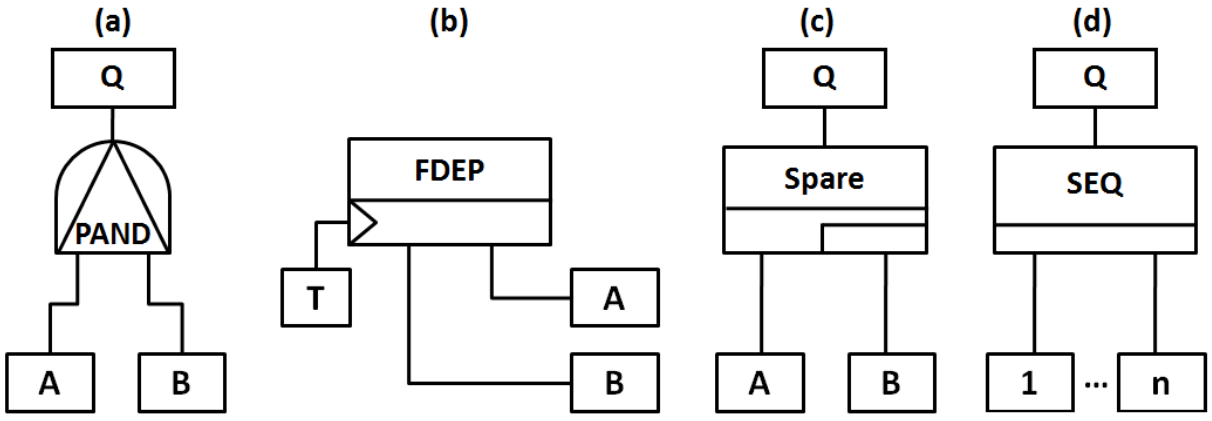

Figure 2.1 (a) Porte PAND. (b) Porte FDEP. (c) Porte Spare. (d) Porte SEQ

2.4 Les chaines de Markov

L’arbre de défaillance dynamique (DFT) est défini comme étant un modèle suffisamment flexible utilisé pour prendre en compte les aspects dynamiques du système, et qui est aussi simple à utiliser qu'un arbre de défaillances habituel. La première idée était de convertir le DFT en modèle de Markov correspondant [37-40], qui est soumis au problème d’explosion de l'espace d'état bien connu [41], même si l'algorithme de modularisation est utilisé [42].

Le modèle de Markov représente la solution traditionnelle du DFT proposée par [6] où le DFT préserve la représentation graphique de l'AdD classique, et le calcul de la probabilité de l'évènement sommet s'effectue via les chaines de Markov [43,44]. Quand les systèmes sont réparables et/ou l'ordre d'occurrence des défaillances est important, les modèles markoviens sont souvent convenables.

Pour l'analyse par les chaines de Markov, on considère un système constitué de n composants réparables ayant deux états probables (fonctionnement et panne). Le système a donc un nombre maximum 2^n d'états composés d'états de fonctionnement ou de panne.

La construction du modèle markovien est initiée par l'état où tous les composants sont parfais, au cours de la vie du système, les états de défaillance peuvent apparaître suite à des défaillances constatées ou disparaître suite à des réparations effectuées. La deuxième étape est l'identification de toutes les transitions possibles entre les états suite à la défaillance ou la réparation d'un ou plusieurs composants. Ces deux étapes construisent un graphe d'états de la manière suivante :

- Chaque cercle représente un état du système.

- Chaque arc représente une transition entre deux cercles, à un arc est associé un taux de transition entre deux états.

- Pour le cas d'un grand système, il est utile de réduire la taille du graphe lorsque ceci est possible par l'agrégation des états ayant des caractéristiques identiques.

La probabilité de passer de l'état i à l'état j dans l'intervalle élémentaire $[t, t+dt]$ est $a_{ij}dt$ où a_{ij} est le taux de transition entre les deux états i et j. Lorsque les taux de transitions sont constants, le processus est markovien homogène. La Figure 2.2 montre un exemple de graphe d'états avec états de fonctionnement et de panne.

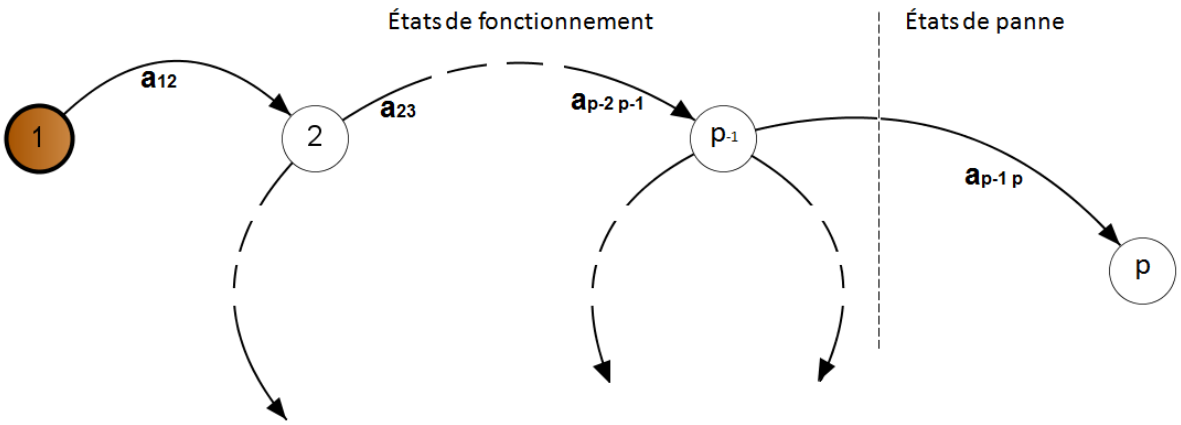

Figure 2.2 Exemple de graphe d'états

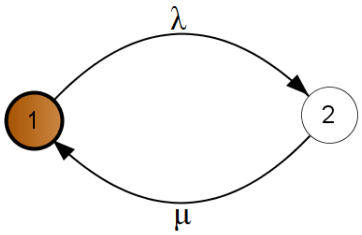

Figure 2.3 Modèle de Markov pour un seul composant réparable

La probabilité que le système étant à l'état i à l'instant $(t + dt)$ en fonction des probabilités des autres états est obtenue par la formule suivante :

$$P_i(t + dt) = \sum_{k \neq i} P_k(t)\, a_{ki} dt + P_i(t) \cdot (1 - \sum_{k \neq i} a_{ik}\, dt) \qquad (2.11)$$

La formule précédente conduit à résoudre un ensemble d'équations différentielles de premier ordre pour obtenir les probabilités relatives aux états du système $P(t) = [P_1(t), P_2(t) \cdots]$ avec la condition initiale $P(0) = [1, 0, \cdots, 0]$ par la relation suivante :

$$\frac{dP(t)}{dt} = M \cdot P(t) \qquad (2.12)$$

Où M est la matrice des taux transition, et $P_i(t)$ est la probabilité que le système étant dans l'état i à l'instant t.

A titre l'illustration, on considère le graphe d'états dans la Figure 2.3 pour un système avec un seul composant réparable. λ et μ représentent respectivement le taux de défaillance et le taux de réparation.

Appliquant l'équation (2.11) sur les deux états, nous obtenons :

$$\begin{cases} P_1(t+dt) = P_1(t) \cdot (1 - \lambda\, dt) + P_2(t) \cdot \mu\, dt \\ P_2(t+dt) = P_1(t) \cdot \lambda\, dt + P_2(t) \cdot (1 - \mu\, dt) \end{cases} \tag{2.13}$$

$$\Longrightarrow \begin{cases} \frac{P_1(t+dt) - P_1(t)}{dt} = \dot{P}_1(t) = -P_1(t) \cdot \lambda + P_2(t) \cdot \mu \\ \frac{P_2(t+dt) - P_2(t)}{dt} = \dot{P}_2(t) = P_1(t) \cdot \lambda - P_2(t) \cdot \mu \end{cases} \tag{2.14}$$

Ce système d'équations différentielles linéaires vaut à résoudre l'équation matricielle suivante :

$$\begin{bmatrix} \dot{P}_1(t) \\ \dot{P}_2(t) \end{bmatrix} = \begin{bmatrix} -\lambda & \mu \\ \lambda & -\mu \end{bmatrix} \times \begin{bmatrix} P_1(t) \\ P_2(t) \end{bmatrix} \tag{2.15}$$

L'équation (2.15) est résolue en considérant que le composant est initialement disponible ($P_1(0) = 1$ et $P_2(0) = 0$) avec l'information que la somme des probabilités égale à 1 ; nous obtenons la probabilité que le système reste dans l'état E_1 comme suit :

$$P_1(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} \tag{2.16}$$

$P_1(t)$ est la disponibilité du système au cours du temps.

Le calcul de probabilité d'un système quelconque soit en état de défaillance vaut à calculer la somme des probabilités des états finaux de défaillance.

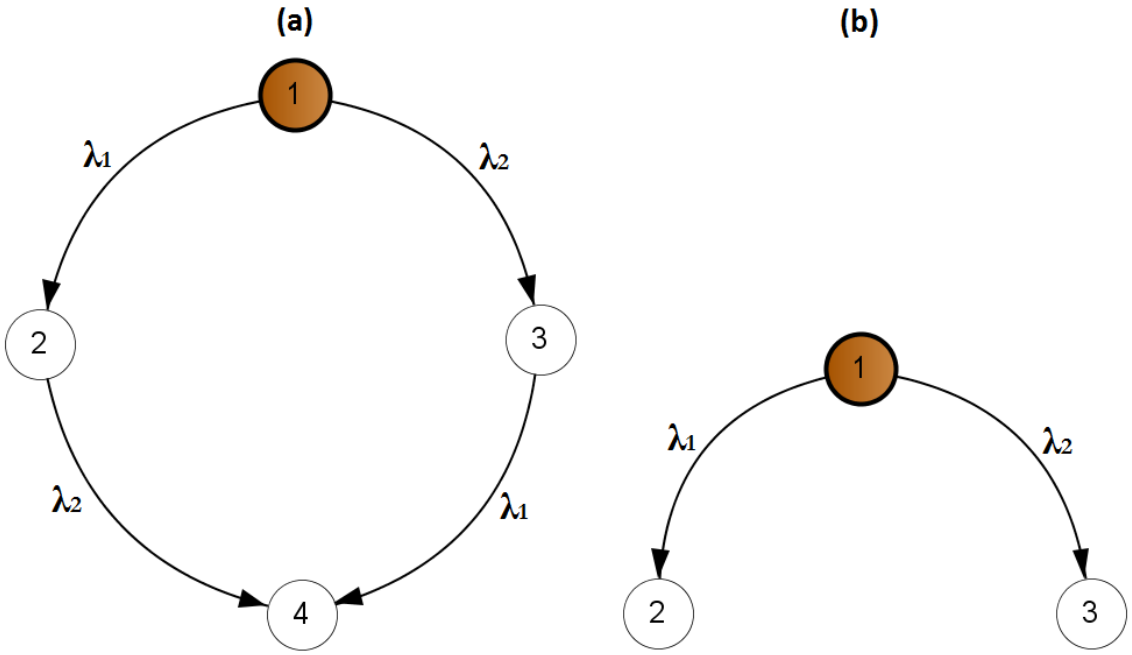

Figure 2.4 (a) Graphe markovien lié à la porte AND. (b) Graphe markovien lié à la porte OR

2.4.1 Modèles markoviens des portes statiques et dynamiques

2.4.1.1 Modèles de Markov correspondants aux portes statiques

L'arbre de défaillance classique (AdD) est principalement composé de portes ET (AND), OU (OR) et K parmi N (KooN). La Figure 2.4 montre les graphes markoviens correspondants aux portes AND et OR, tandis que la Figure 2.5 représente le graphe de Markov lié à la porte 2oo3, λ_i est le taux de transition entre deux états quelconques.

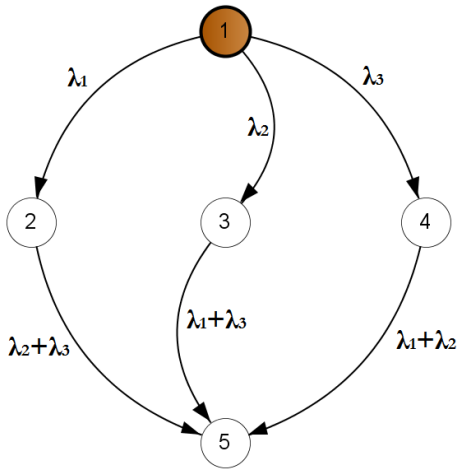

Figure 2.5 Graphe de Markov lié à la porte 2oo3

L'état 4 dans la Figure 2.4a représente l'état de défaillance pour la porte AND et les deux états 2 et 3 dans la Figure 2.4b sont les états de défaillances pour la porte OR. Pour la porte 2oo3 (Figure 2.5) la probabilité que le système soit en état 5 représente la probabilité de défaillance du système.

2.4.1.2 Modèles de Markov correspondants aux portes dynamiques

Les portes dynamiques du DFT (PAND, SPARE, SEQ) exposées dans la Figure 2.1 sont converties respectivement en modèles markoviens correspondants dans la Figure 2.6. Dans la Figure 2.6a l'état 4 représente l'état de défaillance relatif à la porte PAND, pour la Figure 2.6b les deux états 4 et 5 sont les états de défaillance de la porte SPARE et pour la Figure 2.6c l'état 3 est l'état de défaillance.

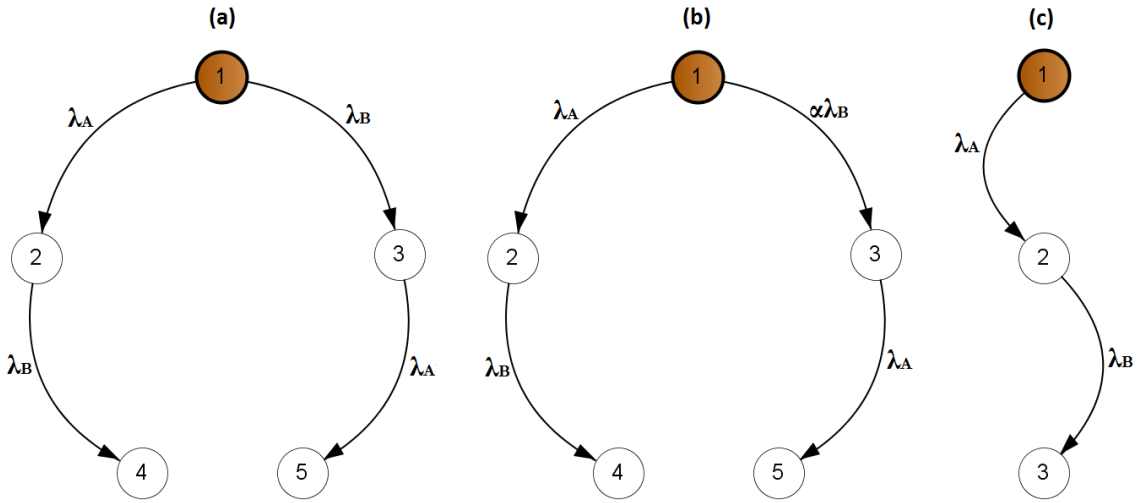

Figure 2.6 (a) Graphe markovien lié à la porte PAND. (b) Graphe markovien lié à la porte SPARE. (c) Graphe markovien lié à la porte SEQ

2.4.2 Calcul de fréquence de défaillance à l'aide des chaines de Markov

2.4.2.1 Règle générale

Considérant maintenant un système à n états de défaillance, le calcul de la fréquence de défaillance ou bien l'intensité de défaillance inconditionnelle via le modèle de Markov est généralement dérivé du calcul de probabilité selon les étapes suivantes:

- Calculer la probabilité de l'ensemble des états avant défaillance.

- Multiplier chaque probabilité obtenue par le taux de défaillance conduisant vers l'état de défaillance.

- Faire la somme des parties trouvées.

Un état avant défaillance ou état de marche critique est un état possédant au moins une transition sortante conduisant à un état de panne.

2.4.2.2 Cas des portes statiques

Pour la porte AND, les états 2 et 3 (Figure 2.4a) sont les états avant défaillance détectés. La fréquence de défaillance déduite est écrite comme suit :

$$fr_{AND} = \lambda_2 P_2(t) + \lambda_1 P_3(t) \tag{2.17}$$

Pour la porte OR, l'état 1 (Figure 2.4b) est l'état avant défaillance détecté. La fréquence de défaillance déduite est écrite comme suit :

$$fr_{OR} = \lambda_1 P_1(t) + \lambda_2 P_1(t) \tag{2.18}$$

2.4.2.3 Cas des portes dynamiques

De même pour les portes statiques, on obtient les expressions de fréquence à partir des modèles markoviens équivalents aux portes dynamiques (Figure 2.6).

Dans le cas de la porte PAND (Figure 2.6a), la fréquence de défaillance est écrite comme suit :

$$fr_{PAND} = \lambda_B P_2(t) \tag{2.19}$$

La fréquence de défaillance obtenue par le modèle markovien (Figure 2.6b) relatif à la porte SPARE est écrite comme suit :

$$fr_{Spare} = \lambda_B P_2(t) + \lambda_A P_3(t) \tag{2.20}$$

Pour le cas de la porte séquentielle, la fréquence de défaillance obtenue par le modèle markovien équivalent est donnée par :

$$fr_{SEQ} = \lambda_B P_2(t) \tag{2.21}$$

La porte de dépendance fonctionnelle suit un comportement équivalent à la porte statique OR. Son propre modèle markovien pour un événement de base donné est celui de la Figure 2.4b et sa fréquence est obtenue à l'aide de l'équation (2.18).

2.4.3 Avantages et limites des chaine de Markov

Très souvent, la conversion d'un AdD relativement simple peut donner lieu à un espace d'états très grand et compliqué dans un modèle markovien correspondant. Le modélisateur peut bénéficier de la représentation arborescente de défaillances du système pour générer automatiquement l'espace d'état de la chaîne de Markov, puis ajuster le modèle obtenu selon les besoins (en cas de défaillances dynamiques).

Néanmoins, la conversion de DFT en modèle markovien est un exercice fastidieux et source d'erreurs [8]. De plus, l'espace d'état (c'est-à-dire l'ensemble de ses nœuds) croît de manière exponentielle avec le nombre de composants du DFT correspondant, ce qui rend le graphe markovien très grand et inexécutable. En effet, pour un modèle de Markov équivalent à un DFT avec m composants d'états binaires (fonctionnement / défaillance) pour lesquels k composants sur m sont séquentiellement dépendants, le nombre d'états est proportionnel au produit de 2^m (Nombre de combinaisons d'états) et $k!$ (Nombre possible de combinaisons de séquences) [44]. Ce problème est fréquemment rencontré dans les modèles markoviens, il est appelé explosion de l'espace d'état. Il convient de noter que même un DFT relativement simple peut donner lieu à un graphe markovien complexe et prenant du temps, en particulier en présence de portes dynamiques en cascade [45]. De plus, il a été mentionné que les chaines de Markov avaient des limites dans la modélisation des dépendances entre les composants avec des distributions de temps de défaillance non exponentielles [28].

2.5 Les réseaux bayésiens

Au cours des dernières années, les réseaux bayésiens [46] sont devenus populaires pour l'analyse de fiabilité et des risques de systèmes complexes, comme alternative fiable par rapport à la plupart des méthodes traditionnelles telles que le diagramme de blocs de fiabilité, l'arbre de défaillance et les arbres d'événements [47-49].

2.5.1 Définition générale

Un réseau bayésien est une représentation graphique intuitive d'un événement ou d'une variable sur une autre en reliant une cause à un effet par une flèche orientée [7]. Les variables sont représentés par des nœuds et les relations de causalité par des flèches. Des tables de probabilité sont assignées à chaque variable et déterminent comment ces nœuds sont reliés (voir Figure 2.7).

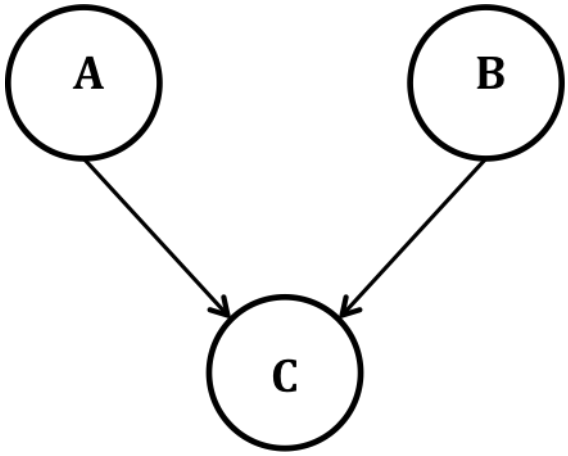

Figure 2.7 Réseau bayésien avec trois nœuds

Le réseau bayésien est un graphe acyclique dirigé [50] défini comme un couple: $\mathcal{G} = ((N, A), \mathcal{P})$ où " N " est un ensemble de nœuds, " A " est un ensemble d'arcs et $\mathcal{P}$ représente l'ensemble de distributions de probabilités conditionnelles qui quantifient les dépendances probabilistes. Une variable aléatoire discrète X est représentée par un nœud $n \in N$ avec un nombre fini d'états mutuellement exclusifs $\mathcal{E}_n$: $\{e_1^n, \dots, e_m^n\}$. Le vecteur $x^n = [p_1 \dots p_m]$ dénote une distribution de probabilité sur $\mathcal{E}_n$, où p_m est la probabilité marginale de n étant dans l'état e_m^n. Dans la Figure 2.8, les nœuds n_i et n_j sont liés par un arc $(n_i, n_j) \in A$ alors n_i est appelé le parent de n_j. L'ensemble des parents d'un nœud n_j contient tous les parents de n_j (par exemple : $pa(n_j) = \{n_i\}$).

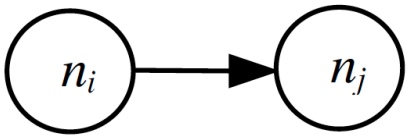

Figure 2.8 Réseau bayésien simple

La **d-séparation** est une propriété très importante pour quantifier le réseau [51]. Elle stipule que tous les nœuds racines sont mutuellement indépendants, et les autres variables du graphe sont conditionnellement dépendantes uniquement en leurs parents, c'est-à-dire dans un graphe contient plusieurs nœuds pour déterminer la valeur de probabilité d'une variable il suffit de connaitre la valeur de ces parent. Dans la Figure 2.7 les deux variables A et B représentent les parents de la variable C et C représente la fille de A et B. Quantitativement, les réseaux bayésiens décrivent la probabilité jointe $Pr(U)$ d'un ensemble de variables $U = \{X_1, \dots, X_n\}$ reliées en un graphe de causalité.

$$Pr(U) = \prod_{i=1}^{n} Pr(X_i | Pa(X_i)) \tag{2.22}$$

Où $Pa(X_i)$ sont les parents de X_i.

Chaque nœud a une table de probabilité conditionnelle TPC associée, où ces TPC représentent l'ensemble $\mathcal{P}$. Par exemple, les nœuds n_i et n_j dans la Figure 4.2 sont définis sur les états $\mathcal{E}_{n_i}: \{e_1^{n_i}, \dots, e_m^{n_i}\}$ et $\mathcal{E}_{n_j}: \{e_1^{n_j}, \dots, e_l^{n_j}\}$. Ensuite, la table de probabilité conditionnelle (TPC) de n_j est définie par les probabilités conditionnelles $Pr(n_j/n_i)$ sur chaque état n_j sachant ses états parents n_i [52]. Cette TPC est définie par le Tableau suivant :

Tableau 2.1 TPC pour le cas statique

$\boldsymbol{e_1^{n_i}}$	$\cdots$	$\boldsymbol{e_m^{n_i}}$
$\boldsymbol{Pr(n_j = e_1^{n_j} / n_i = e_1^{n_i})}$	$\cdots$	$Pr(n_j = e_1^{n_j} / n_i = e_m^{n_i})$
$\vdots$		$\vdots$
$\boldsymbol{Pr(n_j = e_l^{n_j} / n_i = e_m^{n_i})}$	$\cdots$	$Pr(n_j = e_l^{n_j} / n_i = e_m^{n_i})$

On peut donc comprendre qu'un réseau bayésien (RB) est la fusion entre la théorie des graphes acycliques et la théorie de probabilité.

2.5.2 Les réseaux bayésiens dynamiques

Pour prendre en compte l'aspect temporel et les dépendances séquentielles, nous avons besoin d'une représentation explicite dans temps [53].

Dans ces types de modélisations bayésiennes on peut décomposer les relations entre les variables en deux catégories. La première consiste à un instant t donné, ces relations sont constantes (statiques), alors que l'autre catégorie décrit la relation dans le réseau entre deux instants de temps t et $(t + \Delta)$. Cette relation est assurée par des arcs temporels. Un réseau bayésien dynamique est obtenu par la répétition de la même structure pour tout instant de temps.

Supposant que X_i^t est la copie de la variable X_i à l'instant t. Le modèle de transition de X_i décrit $Pr\left[X_i^t | X_i^{t-\Delta}, Y^{t-\Delta}, Y^t\right]$. Où $Y^{t-\Delta}$ est un ensemble de variables à $(t - \Delta)$ diffèrent de X_i, et de même Y^t est un ensemble de variables à t diffèrent de X_i. Les arcs temporels sont ceux qui relient les variables $X_i^{t-\Delta}$ et $Y^{t-\Delta}$ à la variable X_i^t [54].

De même pour le cas statique, Par exemple, les nœuds n_i définis sur les états $\mathcal{E}_{n_i}: \{e_1^{n_i}, \dots, e_m^{n_i}\}$ représentent les parents de n_j à un instant t. Où n_j est un ensemble de variables à l'instant t définis sur les états $\mathcal{E}_{n_j}: \{e_1^{n_j}, \dots, e_l^{n_j}\}$. Un autre ensemble de variables n_k définies sur les états $\mathcal{E}_{n_k}: \{e_1^{n_k}, \dots, e_m^{n_k}\}$ représentant les copies de n_j à l'instant $(t - \Delta)$. La Figure 4.3 décrit la relation entre les trois ensembles.

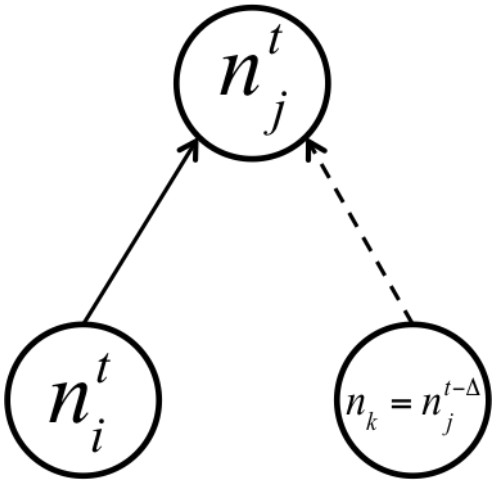

Figure 2.9 Réseau bayésien dynamique simple

La TPC de n_j à l'instant t est définie par les probabilités conditionnelles $Pr(n_j/n_i, n_k)$ sur chaque état n_j sachant ses états parents n_i et n_k.

Tableau 2.2 TPC pour le cas dynamique

$\boldsymbol{e_1^{n_k}}$	$\cdots$	$\boldsymbol{e_m^{n_k}}$
$\boldsymbol{e_1^{n_i}, \ldots, e_m^{n_i}}$	$\cdots$	$e_1^{n_i}, \ldots, e_m^{n_i}$
$\boldsymbol{Pr(n_j = e_1^{n_j}/n_i = e_1^{n_i}, n_j = e_1^{n_k}) \cdots Pr(n_j = e_1^{n_j}/n_i = e_m^{n_i}, n_j = e_1^{n_k})}$	$\cdots$	$Pr(n_j = e_1^{n_j}/n_i = e_1^{n_i}, n_j = e_m^{n_k}) \cdots Pr(n_j = e_1^{n_j}/n_i = e_m^{n_i}, n_j = e_m^{n_k})$
$\vdots$		$\vdots$
$\boldsymbol{Pr(n_j = e_l^{n_j}/n_i = e_1^{n_i}, n_j = e_1^{n_k}) \cdots Pr(n_j = e_l^{n_j}/n_i = e_m^{n_i}, n_j = e_1^{n_k})}$	$\cdots$	$Pr(n_j = e_l^{n_j}/n_i = e_1^{n_i}, n_j = e_m^{n_k}) \cdots Pr(n_j = e_l^{n_j}/n_i = e_m^{n_i}, n_j = e_m^{n_k})$

Les réseaux bayésiens dynamiques (RBD) peuvent être aussi utilisés pour résoudre les arbres de défaillance (DFT), les auteurs dans [55] présentaient RADYBAN, un outil qui convertit automatiquement un DFT en un RBD. La Figure 4.4 représente un graphe RBD simple obtenu par le logiciel HUGIN Expert [56].

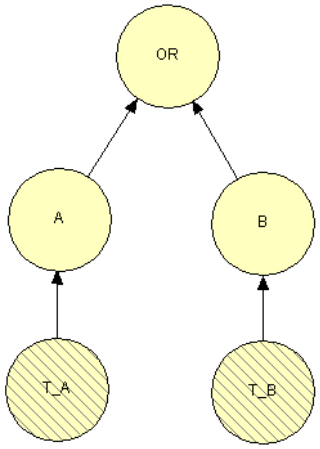

Figure 2.10 RBD équivalent à la porte OR

2.6 Autres outils de résolution des DFT

La formulation inclusion-exclusion donnée dans [57,58] donne un résultat exact avec une détermination des coupes/séquences minimales, mais la seule porte dynamique considérée est la porte priorité-AND (PAND). Néanmoins, la plupart des approches évoquées dans ce cadre ont pour limite de ne considérer que la distribution des défaillances des composants comme exponentielle.

Xing et al. [59] développent une méthode basée sur les diagrammes de décision binaire séquentielle (SBDD) proposée pour la modélisation du DFT avec des portes dynamiques PAND. Cette approche présente l'avantage de prendre en compte toute distribution de défaillance.

Ge et al. [29,60] ont fourni une SBDD améliorée pour quantifier les DFT complexes. Rauzy [61] a proposé un diagramme de décision de séquence (SDD) pour coder des ensembles de séquences modélisées algébriquement et équivalentes au DFT.

Monte Carlo est une méthode de simulation utilisée pour résoudre des tâches DFT pour des systèmes complexes avec la considération de n'importe quelle distribution de temps de défaillance des composants [62-64]. Le principal problème des techniques basées sur la

simulation est la nécessité d'un long temps de calcul pour obtenir des résultats précis, en particulier dans le cas d'événements rares [65].

Cheshmikhani et Zarandi [66] ont utilisé des portes logiques stochastiques pour convertir chaque porte de sortie statique et dynamique de DFT afin d'accélérer le calcul des méthodes basées sur la méthode de Monte Carlo à l'aide d'un "arbre de temps de défaillance" présenté dans [67]. Il convient de noter que les approches basées sur la méthode de Monte Carlo sont moins précises que les approches analytiques et qu'elles ne peuvent pas effectuer d'analyses qualitatives (détermination des coupes/séquences minimales). En ce qui concerne le calcul de fréquence, nous n'avons pas trouvé dans la littérature de tentatives pour calculer la fréquence de l'événement sommet du DFT, alors qu'il s'agit d'un paramètre important dans les analyses de fiabilité et de sécurité.

2.7 Conclusion

Dans ce chapitre, nous avons exposé l'arbre de défaillance dynamique et sa résolution à l'aide d'un outil traditionnel (les chaines de Markov). Nous avons vu comment les portes statiques et dynamiques du DFT sont converties en modèles markoviens représentant les séquences de défaillance existantes et comment les calculs de probabilité et fréquence d'occurrence sont découlés via le modèle de Markov. Les avantages et les limites des modèles markoviens sont aussi bien clarifiés. Un bref examen sur les principes fondamentaux des réseaux bayésiens a été fait où les tables de probabilité conditionnelle ont été envisagées pour le cas général et le cas dynamique. A la fin, nous avons récapitulé quelques outils usuels existants dans la littérature visant la résolution des DFT.

Dans la suite de ce travail doctoral, les chaines de Markov sont utilisées comme un outil de référence dans la résolution des DFT surtout en terme de comparaison des résultats de la démarche algébrique développée dans le chapitre suivant. Le dernier chapitre est consacré au développement d'un modèle particulier des réseaux bayésiens et voir leur pouvoir de modélisation.

Chapitre 3

Traitement qualitative et quantitative des arbres de défaillance

3.1 Introduction

Dans ce chapitre, nous présentons une approche complète permettant de réaliser des analyses qualitatives et quantitatives pour les arbres de défaillance dynamiques [68]. Les auteurs dans [69,70] ont proposé différents cadres algébriques pour exprimer l'événement sommet du DFT à l'aide d'opérateurs booléens et dynamiques.

Basé sur le travail de Merle [71], nous détaillons la forme canonique de toute DFT grâce à des modèles algébriques de portes statiques et dynamiques à l'aide des opérateurs appropriés, puis les ensembles de coupes / séquences seront développés afin d'exprimer la probabilité et la fréquence des soties de portes et évaluer la probabilité et la fréquence de l'événement sommet du DFT. Ce modèle doit être capable de calculer la probabilité et la fréquence de défaillance des systèmes liés à la sécurité, et d'évaluer la fréquence des scénarios LOPA en basant sur l'approche proposée sans assumer aucune indépendance entre les éléments du scénario (les couches de protection et l'événement initiateur) [27,28].

3.2 Modèle algébrique de l'arbre de défaillance dynamique

3.2.1 Modèle algébrique des portes statiques et dynamiques

L'arbre de défaillance statique (AdD) est composé de portes OR, AND et KooN, cette dernière peut être représentée par la combinaison des deux premières portes. Ainsi, seuls les opérateurs + (pour la porte OR) et · (pour la porte AND) sont utilisés pour modéliser les AdD. La porte 2oo3 (2 parmi 3) est illustrée par la combinaison des portes OR et AND avec les événements répétés A, B et C, comme illustré dans la Figure 3.1.

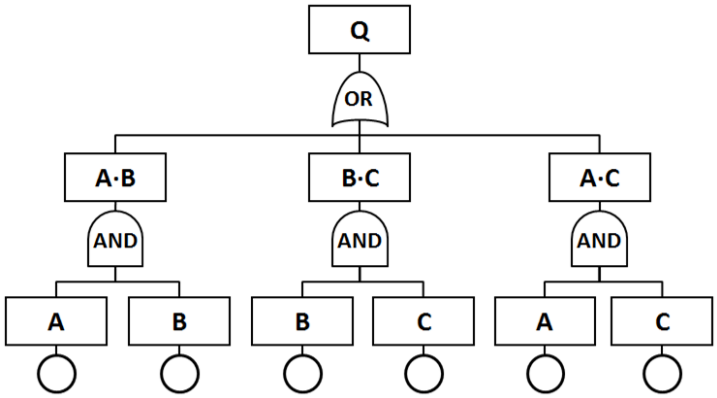

Figure 3.1 La porte 2oo3 modélisée par les portes AND et OR [68]

La forme algébrique de l'événement Q peut être exprimée comme suit:

$$Q = A \cdot B + B \cdot C + A \cdot C \tag{3.1}$$

De plus, Merle et al. [8] ont défini l'opérateur non inclusif avant, l'opérateur simultané et l'opérateur inclusif antérieur avec les symboles algébriques $\lhd$, $\triangle$ et $\underline{\lhd}$, respectivement. Les modèles algébriques de toutes les portes dynamiques susmentionnées sur les Figures 2.1a-2.1d sont décrits en utilisant les opérateurs ci-dessus.

3.2.2 Fonction de structure de l'arbre de défaillance dynamique

Il existe de nombreuses façons pour déterminer la fonction de structure de l'AdD. Les méthodes existantes utilisées pour obtenir les coupes minimales sont basées sur les théorèmes

de l'algèbre de Boole ou sur le diagramme de décision binaire (BDD) [72]. Une coupe minimale représente la combinaison minimale de défaillances des composants qui entraînent la défaillance totale du système et dont le nombre ne peut pas être réduit. En outre, une séquence minimale est définie pour représenter la séquence de défaillances des composants qui en se produisant, provoquent l'occurrence de la sortie de portes dynamiques ou la défaillance du système [73].

La fonction de structure de l'arbre de défaillance dynamique peut être développée et simplifiée grâce aux théorèmes de l'algèbre de Boole et à ceux donnés dans [8], où certains d'entre eux seront largement utilisés dans la suite de ce chapitre.

A, B et C trois événements statistiquement indépendants qui répondent aux propriétés suivantes:

$$A + A \cdot B = A \tag{3.2}$$

$$A \triangle B = 0 \tag{3.3}$$

$$A \underline{\lhd} B = A \lhd B + A \triangle B = A \lhd B \tag{3.4}$$

$$A \underline{\lhd} A = A \tag{3.5}$$

$$A \cdot (A \lhd B) = A \lhd B \tag{3.6}$$

$$A + (A \lhd B) = A \tag{3.7}$$

$$(A + B) \lhd C = (A \lhd C) + (B \lhd C) \tag{3.8}$$

$$A \lhd (B + C) = (A \lhd B) \cdot (A \lhd C) \tag{3.9}$$

$$A \lhd (B \cdot C) = (A \lhd B) + (A \lhd C) \tag{3.10}$$

$$(A \lhd B) \cdot (B \lhd C) \cdot (A \lhd C) = (A \lhd B) \cdot (B \lhd C) \tag{3.11}$$

Selon les équations (3.3), (3.4) et (3.5), les opérateurs ($\triangle$ et $\underline{\lhd}$) peuvent être éliminés de la fonction de structure. Le résultat d'un traitement algébrique d'un DFT devient une forme canonique normalisée se forme de somme des produits, où chaque terme contient au moins un des deux opérateurs ($\cdot$ et $\lhd$). Finalement, la fonction de structure de l'événement sommet (ES) peut être exprimée comme suit:

$$ES = \sum(Coupes\ minimales) + \sum\left(\prod b_i \cdot \prod\left(b_j \lhd b_k\right)\right),\ j \neq \{i,k\} \qquad (3.12)$$

Où chaque terme $\prod b_i \cdot \prod\left(b_j \lhd b_k\right)$ est une expression algébrique des événements de base représente un ensemble de séquences minimales et donne des informations sur la façon dont ces événements peuvent être combinés pour offrir des séquences possibles conduisant à ES.

3.2.3 Probabilité de défaillance du système dynamique

L'objectif principal d'une analyse DFT est le calcul de probabilité de son ES. L'obtention de la probabilité du ES peut être réalisée en utilisant la formule inclusion-exclusion appliquée aux coupes minimales précédemment déterminées. Par souci de simplicité, x et $\overline{x} = (1 - x)$ représentent respectivement la probabilité d'occurrence et de non occurrence d'un événement X. La probabilité de sortie de la porte 2oo3 peut être évaluée comme suit:

$$Pr(Q) = Pr(A \cdot B + B \cdot C + A \cdot C)$$

$$Pr(Q) = Pr(A \cdot B) + Pr(B \cdot C) + Pr(A \cdot C) - Pr(A \cdot B \cdot B \cdot C) - Pr(A \cdot B \cdot A \cdot C) - Pr(B \cdot C \cdot A \cdot C) + Pr(A \cdot B \cdot B \cdot C \cdot A \cdot C)$$

$$= a \cdot b - a \cdot b \cdot c + b \cdot c - a \cdot b \cdot c + a \cdot c - a \cdot b \cdot c + a \cdot b \cdot c$$

$$= a \cdot b \cdot (1 - c) + b \cdot c \cdot (1 - a) + a \cdot c \cdot (1 - b) + a \cdot b \cdot c$$

$$Pr(Q) = a \cdot b + b \cdot c \cdot \overline{a} + a \cdot c \cdot \overline{b} \tag{3.13}$$

L'équation (3.13) donne l'expression de probabilité de la porte 2oo3.

Dans les parties dynamiques, la probabilité est obtenue en faisant la somme des probabilités de séquences disjonctives. La probabilité de ES peut être obtenue grâce à la relation suivante:

$$Pr(ES) = Pr_{(Coupes\ minimales\ )} + \left(1 - Pr_{(Coupes\ minimales\ )}\right) \cdot Pr_{(Séquences\ Disjonctives)} \tag{3.14}$$

L'extraction des séquences disjonctives de défaillance sera expliquée par la suite. La probabilité d'une seule séquence disjonctive composée de deux événements de base $[B_1, B_2]$ est donnée par la relation suivante [59] :

$$Pr([B_1, B_2]) = \int_0^t \left(\int_0^{\tau_2} f_1(\tau_1)\, d\tau_1 \right) f_2(\tau_2) d\tau_2 \tag{3.15}$$

$f_i(t)$ représente la fonction de densité de probabilité de l'événement de base B_i.

La relation effectue la probabilité que B_1 se produise avant B_2 à τ_2 et que B_1 et B_2 se produisent tous deux pendant un temps de mission t.

Dans le cas général, considérons la séquence de n événements $[B_1, B_2, \dots, B_n]$, la probabilité de cette séquence est trouvée par la relation suivante:

$$\begin{gathered} Pr([B_1, B_2, \dots, B_n]) = \\ \int_0^t \dots \left(\int_0^{\tau_4} \left(\int_0^{\tau_3} \left(\int_0^{\tau_2} f_1(\tau_1)\, d\tau_1 \right) f_2(\tau_2) d\tau_2 \right) f_3(\tau_3) d\tau_3 \right) \dots f_n(\tau_n) d\tau_n \end{gathered} \tag{3.16}$$

3.3 Analyse qualitative de l'arbre de défaillance dynamique

Le but de l'analyse qualitative des DFT est de déterminer à la fois les coupes minimales pour la partie statique et les séquences minimales (SMs) pour la partie dynamique. Par conséquent, deux cas peuvent être considérés: si un terme dans la fonction de structure DFT

ne contient pas d'opérateurs temporels BF ($\lhd$), il est statique et fournit un ensemble de coupes minimales. S'il contient des opérateurs temporels BF ($\lhd$), le terme est dynamique et donne un ensemble de séquences minimales.

3.3.1 Détermination des séquences de défaillance primaires

Nous détaillons ici comment les séquences de défaillance du DFT peuvent être extraites de la fonction de structure [74]. Comme expliqué précédemment, une coupe minimale représente la combinaison minimale d'un ensemble d'événements qui en se produisant l'événement ES produit. Il est à noter qu'un ensemble de SMs fournit une ou plusieurs séquences minimales (séquences de défaillance). Considérons un DFT avec trois événements de base A, B et C. Pour une fonction de structure donnée, les séquences de défaillance peuvent être facilement déduites.

1) La seule séquence obtenue à partir du terme algébrique $B \cdot (A \lhd B)$ est la séquence $[A, B]$.

2) L'expression algébrique $C \cdot B \cdot (A \lhd B)$ représente les séquences $[A, B, C]$, $[A, C, B]$ et $[C, A, B]$.

3) Le terme $(A \lhd B) \cdot (B \lhd C)$ donne les deux séquences $[A, B, C]$, $[A, B, \overline{C}]$, où $\overline{C}$ représente la non occurrence de C.

4) Le terme $(A \lhd B) \cdot (A \lhd C)$ est équivalent au terme algébrique $A \lhd (B + C)$, cette forme produit cinq séquences de défaillance $[A, B, C]$, $[A, C, B]$, $[A, B, \overline{C}]$, $[A, C, \overline{B}]$ et $[A, \overline{B}, \overline{C}]$.

Il est important de noter que dans un terme algébrique du DFT, l'absence d'un événement qui apparaît dans un terme conditionnel signifie que cet événement doit prendre deux modes dans une séquence, l'occurrence et la non-occurrence. Par exemple: l'expression $(A \lhd B)$ signifie la condition selon laquelle A doit se produire avant B et fournit deux séquences $[A, B]$ et $[A, \overline{B}]$ en prenant l'occurrence et la non-occurrence de B.

3.3.2 Inclusion et absorption des Séquences de défaillance

Il s'agit d'un nouveau traitement qui est utilisé pour éliminer les séquences incluses dans d'autres séquences qui sont des séquences absorbantes. Considérons une séquence de défaillance $S = [B_1, B_2, \dots, B_n]$. La séquence de défaillance S absorbe des séquences incluses de défaillance, si ces séquences contiennent tous les événements de S, tout en respectant le même ordre d'apparition. Les séquences $S_1 = [B_4, B_1, B_2, B_3]$, $S_2 = [B_1, B_2, B_4, B_5, B_3]$ et $S_3 = [B_1, B_2, B_3, B_5, \overline{B_4}]$, par exemple, sont incluses dans $S_4 = [B_1, B_2, B_3]$, et S_4 est absorbante.

De la même manière, un terme algébrique qui fournit des séquences de défaillance peut être retiré de la fonction de structure si ses séquences sont couvertes par au moins un des autres termes algébriques dans la fonction de structure. Le terme $(A \triangleleft B)$ par exemple, donne $[A, B]$ et $[A, \overline{B}]$; alors que le terme $B \cdot (A \triangleleft B)$ fournit seulement $[A, B]$. Donc, pour la fonction de structure $Q = (A \triangleleft B) + B \cdot (A \triangleleft B)$, le second terme peut être supprimé, et Q devient équivalent à $(A \triangleleft B)$.

3.3.3 Détermination des séquences disjonctives de défaillance

À la fin du processus précédent (suppression des séquences incluses de l'ensemble des séquences de défaillance ou élimination des termes redondants de la fonction de structure), les séquences dérivées de la fonction de structure ne sont pas disjonctives. En supprimant les conjonctions entre les séquences primaires, on peut obtenir tous les chemins possibles vers l'événement sommet du DFT (ES) et sa probabilité peut être calculée simplement de la manière suivante :

$$Pr_{(Séquences\ primaires)} = \sum Pr_{(Séquences\ Disjunctive)} \tag{3.17}$$

Afin de retirer les conjonctions existantes, les procédures suivantes sont effectuées:

- Trier les séquences primaires obtenues du plus courte au plus longue.

- Séparer les séquences en ensembles de séquences de défaillance où chaque ensemble contenant des séquences avec les mêmes événements de base.

- En commençant par le deuxième ensemble, ajouter des événements de séquences précédentes qui ne façonnent pas l'ensemble d'intérêt des séquences de défaillance, tout en préservant la propriété d'absorption. Cette opération s'inspire de la méthode dite de disjonction des coupes minimales appliquée au lieu de la méthode inclusion-exclusion pour obtenir l'expression de probabilité de l'événement sommet dans l'arbre de défaillance statique. Par conséquent, l'équation (3.13) peut être obtenue en utilisant la disjonction des coupes minimales AB, BC et AC comme suit :

$A \cdot B \rightarrow A \cdot B$;

$B \cdot C \rightarrow B \cdot C \cdot \overline{A \cdot B} \rightarrow B \cdot C \cdot (\overline{A} + \overline{B}) \rightarrow B \cdot C \cdot \overline{A}$;

$A \cdot C \rightarrow A \cdot C \cdot \overline{B \cdot C} \cdot \overline{A \cdot B} \rightarrow A \cdot C \cdot (\overline{B} + \overline{C}) \cdot (\overline{A} + \overline{B}) \rightarrow A \cdot C \cdot \overline{B}$.

$$Pr(A \cdot B + B \cdot C + A \cdot C) = Pr(A \cdot B) + Pr\left(B \cdot C \cdot \overline{A}\right) + Pr(A \cdot C \cdot \overline{B})$$

$$Pr(A \cdot B + B \cdot C + A \cdot C) = a \cdot b + b \cdot c \cdot \overline{a} + a \cdot c \cdot \overline{b} \tag{3.18}$$

Cette méthode de disjonction (liée aux coupes minimales) peut être résumée comme suit: à partir du deuxième ensemble de coupes minimales, ajoutez les événements des ensembles précédents aux ensembles de coupes minimales qui ne façonnent pas la coupe minimale sélectionnée.

Les procédures ci-dessus génèrent des séquences supplémentaires et donnent des séquences de défaillance mutuellement exclusives (disjonctives) permettant ensuite de quantifier ES.

Considérons les séquences primaires ordonnées: $[A, B], [A, E]$ et $[A, C, D]$. Pour supprimer les conjonctions existantes, l'événement B est ajouté dans $[A, E]$ alors que B ne peut pas être après l'événement A. B et E seront ajoutés dans $[A, C, D]$ tandis que B et E ne

peuvent pas être après l'occurrence de A selon la propriété d'absorption. En conséquence, nous avons les séquences de défaillance disjonctives suivantes :

$[A, B] \rightarrow [A, B]$;

$[A, E] \rightarrow [B, A, E]$ et $[A, E, \overline{B}]$;

$[A, C, D] \rightarrow [B, E, A, C, D]$, $[E, B, A, C, D]$,$[B, A, C, D, \overline{E}]$, $[E, A, C, D, \overline{B}]$ et $[A, C, D, \overline{B}, \overline{E}]$.

La probabilité de défaillance est trouvée comme suit:

$$\begin{aligned} Pr([A,B]+[A,E]+[A,C,D]) = {} & Pr([A,B]) + Pr([B,A,E]) + Pr\left([A,E,\overline{B}]\right) \\ & + Pr([B,E,A,C,D]) + Pr([E,B,A,C,D]) + Pr\left([B,A,C,D,\overline{E}]\right) \\ & + Pr\left([E,A,C,D,\overline{B}]\right) + Pr\left([A,C,D,\overline{B},\overline{E}]\right) \end{aligned} \quad (3.19)$$

Pour conclure; le traitement qualitatif pour tout DFT est réalisé en effectuant les étapes suivantes:

- Déterminer à la fois les coupes minimales et les séquences minimales.

- Détermination des séquences de défaillance primaires de chaque ensemble de séquences minimales.

- Éliminer les séquences de défaillance incluses.

- Suppression des conjonctions entre les séquences de défaillance primaires pour obtenir toutes les séquences disjonctives de défaillance.

3.3.4 Relation entre les événements dans les séquences de défaillance

Il est important de noter que les relations entre les événements dans une séquence ou dans un terme algébrique n'ont pas la même nature. Par exemple, si on prend la séquence $[A, B]$ les deux événements A et B peuvent être reliés avec une porte PAND ou bien par une

porte SEQ ou encore par une porte SPARE. Ces relations séquentielles peuvent être remarquées dans la représentation du DFT, et de ce fait il est primordial de prendre en compte la nature de la séquence dans les calculs.

3.4 Fréquence de défaillance basée sur la détermination des séquences disjonctives de défaillance

3.4.1 Fréquence de défaillance d'une séquence disjonctive de défaillance

Le but de cette sous-section est de montrer comment la fréquence de défaillance du DFT peut être évalue à partir de la détermination des séquences disjonctives de défaillance. Nous admettons qu'une séquence disjonctive de défaillance S comprend k événements survenus et $(n-k)$ événements non survenus peut être formulée comme suit $[B_1, B_2, \dots, B_k, \overline{B_{k+1}}, \dots, \overline{B_n}]$. La séquence avant-défaillance liée à S est la séquence $[B_1, B_2, \dots, \overline{B_k}, \overline{B_{k+1}}, \dots, \overline{B_n}]$ caractérisée par la non-occurrence du dernier événement dans l'ensemble des événements survenus. La fréquence d'occurrence de S est trouvée comme suit:

$$fr(S) = Pr\left([B_1, B_2, \dots, \overline{B_k}, \overline{B_{k+1}}, \dots, \overline{B_n}]\right) \cdot \lambda_{B_k} \tag{3.20}$$

Pour le cas particulier d'une séquence avec deux événements A et B, on obtient:

$$fr([A, B]) = Pr\left([A, \overline{B}]\right) \cdot \lambda_B \tag{3.21}$$

En se basant sur l'équation ci-dessus, la fréquence de défaillance pour chaque porte dynamique avec deux événements d'entrée est développée dans l'Annexe A.

Une séquence avant-défaillance $[B_1, B_2, \dots, \overline{B_k}, \overline{B_{k+1}}, \dots, \overline{B_n}]$ qui contient n événements ordonnés absorbe les séquences dans lesquelles elles couvrent d'autres événements survenus de B_k à B_{n-1} et respectent l'ordre d'apparition de ces événements. La séquence avant-défaillance $[B_1, \overline{B_2}, \overline{B_3}, \overline{B_4}]$, par exemple, absorbe les deux séquences $[B_1, B_2, \overline{B_3}, \overline{B_4}]$ et

$[B_1, B_2, B_3, \overline{B_4}]$. De plus, si les deux dernières séquences sont extraites à partir d'un traitement de disjonction de séquences de défaillance, la fréquence de défaillance est calculée en multipliant la probabilité de $[B_1, \overline{B_2}, \overline{B_3}, \overline{B_4}]$ par le taux de défaillance de B_2, et les deux autres séquences absorbées ne sont pas considérées.

$$fr\big([B_1, B_2, \overline{B_3}, \overline{B_4}], [B_1, B_2, B_3, \overline{B_4}]\big) = Pr\big([B_1, \overline{B_2}, \overline{B_3}, \overline{B_4}]\big) \cdot \lambda_{B_2} \tag{3.22}$$

3.4.2 Fréquence de défaillance relative à la porte PAND

Tout d'abord, considérons la sortie Q d'une porte PAND avec deux événements d'entrée A et B. Ainsi, nous avons la forme algébrique $Q = B \cdot (A \lhd B)$ qui représente la seule séquence $[A, B]$. Si A et B sont considérés comme des événements représentant la défaillance de composant et suivent une distribution exponentielle avec les taux de défaillance λ_A et λ_B respectivement. La fréquence de défaillance de la sortie PAND peut être trouvée comme suit:

$$fr(PAND) = \lambda_B \cdot \big(1 - F_B(t)\big) \cdot \int_0^t \lambda_A e^{-\lambda_A \tau_A} \, d\tau_A \tag{3.23}$$

Par souci de simplicité, nous utilisons la notation suivante: pour un composant C, $Pr(C\ est\ bon) = \overline{c}$ et $Pr(C\ est\ défaillant) = c$. Dans le cas de la distribution exponentielle, $\overline{c} = e^{-\lambda_C t}$ et $c = 1 - e^{-\lambda_C t}$ représentent la fiabilité et la probabilité de défaillance de C respectivement. Par conséquent, l'équation ci-dessus peut être exprimée comme suit (voir Annexe A.1):

$$fr(PAND) = \lambda_B \cdot \overline{b} \cdot a \tag{3.24}$$

3.4.3 Fréquence de défaillance relative à la porte SPARE

La forme algébrique de la porte SPARE est $(A \cdot (B_d \lhd A) + B_a \cdot (A \lhd B_a)$ [7]. Ainsi, deux séquences $[B_d, A]$ et $[A, B_a]$ sont obtenues. Il convient de noter que l'événement de secours (B) comporte deux modes de défaillance: le mode dormant et le mode actif. Ainsi, deux distributions de défaillance différentes doivent être déterminées.

Dans le cas d'une distribution exponentielle, le taux de défaillance en mode veille (dormant) est représenté par ($\lambda_{B_d} = \alpha \cdot \lambda_B$), où α est le facteur de dormance et λ_B est le taux de défaillance en mode actif [55]. La fonction de densité de probabilité correspondante et la fonction de distribution cumulative de l'événement de secours en mode dormant sont :

$$\begin{cases} f_{B_d}(t) = \alpha\, \lambda_B e^{-\alpha\, \lambda_B t} \\ F_{B_d}(t) = 1 - e^{-\alpha\, \lambda_B t_A} \end{cases} \tag{3.25}$$

En mode actif, nous avons [75] :

$$\begin{cases} f_{B_a}(t, t_A) = \lambda_B e^{-\lambda_B (t-(1-\alpha)t_A)} \\ F_{B_a}(t, t_A) = 1 - e^{-\lambda_B (t-(1-\alpha)t_A)} \end{cases} \tag{3.26}$$

Où t_A est l'instant de défaillance de l'événement primaire A. À cette date, l'événement de secours passe immédiatement du mode veille (dormant) au mode actif.

La fréquence de défaillance pour la sortie de la porte SPARE peut être simplement exprimée au moyen de l'occurrence de ses événements d'entrée et par considérer $\overline{b_\alpha} = e^{-\alpha \lambda_B t}$ (voir Annexe A.2):

$$fr(Spare) = \lambda_A \cdot \left(\overline{a} - \overline{a} \cdot \overline{b_\alpha}\right) + \frac{\lambda_A \cdot \lambda_B}{\lambda_A - (1-\alpha)\lambda_B} \left(\overline{b} - \overline{a} \cdot \overline{b_\alpha}\right), \text{pour } \lambda_B \neq \frac{\lambda_A}{1-\alpha} \tag{3.27}$$

3.4.4 Fréquence de défaillance relative à la porte SEQ

La porte séquentielle (SEQ) pour deux événements de défaillance de composant d'entrée A et B est illustrée par la forme algébrique $B \cdot (A \lhd B)$, telle que A et B sont connectés successivement et représentés par la seule séquence $[A, B]$. La durée t_A de la défaillance du premier composant A est la date de déclenchement du composant B ce qui est parfait à cet instant. La fréquence de défaillance est calculée comme suit :

$$fr(SEQ) = \lambda_B \cdot \left(1 - \int_{t_A}^{t} \lambda_B e^{-\lambda_B(t_B - t_A)}\, dt_B\right) \cdot \int_0^t \lambda_A e^{-\lambda_A t_A}\, dt_A \quad (3.28)$$

Par conséquent, il se résulte (voir Annexe A.3) :

$$fr(SEQ) = \frac{\lambda_A \cdot \lambda_B}{\lambda_A - \lambda_B} \cdot \left(\overline{b} - \overline{a}\right), \text{pour } \lambda_A \neq \lambda_B \quad (3.29)$$

3.5 Expression de fréquence de défaillance d'un système dynamique

3.5.1 Formulation mathématique de la fréquence de défaillance

La Fréquence de défaillance également appelée "Intensité de défaillance inconditionnelle" [76] pour un système S est définie comme la probabilité de défaillance du système par unité de temps à l'instant t; étant donné qu'il était en état de fonctionnement à l'instant 0.

$$w_S(t) = \lim_{dt \to 0} \frac{Pr\{S \text{ défaille entre } t \text{ et } t + dt / D\}}{dt} \quad (3.30)$$

Où D désigne l'événement "le système fonctionnait à l'instant 0".

L'intensité de défaillance inconditionnelle peut également être déterminée selon la propriété bien connue suivante:

$$w_S(t) = \lambda_S(t) \cdot A_S(t) \quad (3.31)$$

Où $\lambda_S(t)$ et $A_S(t)$ représentent respectivement l'intensité de défaillance conditionnelle et la disponibilité du système.

Si le système S est parfait à $t = 0$ et est considéré comme non-réparable, $\lambda_S(t) = \frac{\left(\frac{dF_S(t)}{dt}\right)}{1 - F(t)}$ et $A_S(t) = 1 - F_S(t)$. Où $F_S(t)$ désigne la fiabilité du système S.

Par conséquent, l'égalité suivante tient :

$$w_S(t) = \frac{dF_S(t)}{dt} = f_S(t) \tag{3.32}$$

3.5.2 Expression de fréquence de défaillance d'un système non dynamique

Dans cette sous-section, nous montrons une procédure qui sert à convertir l'expression de probabilité des portes dynamiques DFT en expression de fréquence de défaillance. Singh [77] a établi des règles pour obtenir les fréquences d'échec et de succès d'un système statique. Un deuxième travail [78] du même auteur a étendu et généralisé son travail précédent, dans lequel quatre règles ont été développées pour dériver l'expression de fréquence d'un système statique. L'une de ces règles consiste à obtenir l'expression de fréquence de défaillance d'un système donné à partir de son expression de probabilité de défaillance qui est fonction d'échec et succès des composants. La règle à présenter ici est utilisée pour transformer l'expression de probabilité pour chaque sortie de porte dynamique en expression de fréquence de défaillance et les résultats sont ensuite comparés à ceux obtenus dans la section précédente.

Comme nous l'avons vu précédemment, l'expression de probabilité de la porte 2oo3 peut être dérivée de sa forme algébrique qui est une somme de produits (coupes minimales). Généralement, pour les systèmes statiques, l'expression de probabilité de défaillance peut être formulée à travers les probabilités de défaillance et de succès de leurs composants, elle peut s'écrire comme suit :

$$Pr(ES) = \sum_j G_j = \sum_j \prod_{1 \le k \le n_j} b_k \cdot \prod_{1 \le m \le n_j} \overline{b_m}\,; k \neq m \tag{3.33}$$

L'expression de fréquence de l'événement sommet ES tient [25]:

$$fr(ES) = \sum_j G_j \left[\sum_{1 \le k \le n_j} \frac{\lambda_k \cdot \overline{b_k}}{b_k} - \sum_{1 \le m \le n_j} \lambda_m\right] \tag{3.34}$$

Laissez-nous appliquer cette règle sur la porte statique 2oo3. Selon l'équation (3.13), l'expression de probabilité de l'événement de sortie est :

$$Pr(2oo3) = a \cdot b + b \cdot c \cdot \overline{a} + a \cdot c \cdot \overline{b} \tag{3.35}$$

En supposant la distribution exponentielle, l'expression de fréquence pour la porte 2oo3 est donnée en utilisant l'équation (3.34) comme suit :

$$\begin{aligned} fr(2oo3) = \lambda_A \cdot \overline{a} \cdot b + \lambda_B \cdot \overline{b} \cdot a + \lambda_B \cdot \overline{b} \cdot c \cdot \overline{a} + \lambda_C \cdot \overline{c} \cdot b \cdot \overline{a} - \lambda_A \cdot \overline{a} \cdot b \cdot c \\ + \lambda_A \cdot \overline{a} \cdot c \cdot \overline{b} + \lambda_C \cdot \overline{c} \cdot a \cdot \overline{b} - \lambda_B \cdot \overline{b} \cdot a \cdot c \end{aligned} \tag{3.36}$$

Après restructuration, l'expression de fréquence de la porte 2oo3 devient :

$$fr(2oo3) = a \cdot \overline{b} \cdot \overline{c} \cdot (\lambda_B + \lambda_C) + b \cdot \overline{a} \cdot \overline{c} \cdot (\lambda_A + \lambda_C) + c \cdot \overline{a} \cdot \overline{b} \cdot (\lambda_A + \lambda_B) \tag{3.37}$$

3.5.3 Expression de fréquence pour les portes dynamiques

Nous montrons ci-après comment les expressions de fréquence de sortie des portes dynamiques peuvent être trouvées cas par cas en appliquant la même règle de conversion (l'équation (3.34)) si leurs expressions de probabilité sont écrites en fonction des événements d'entrée. Par ailleurs, la fréquence de défaillance est obtenue en utilisant l'équation (3.32). Les expressions de probabilité utilisées ici sont détaillées à l'Annexe B.

3.5.3.1 Expression de fréquence pour la porte PAND

La probabilité d'occurrence de la sortie de cette porte est obtenue en utilisant l'équation (3.15) :

$$Pr(PAND) = \int_0^t \left(\int_0^{\tau_B} \lambda_A e^{-\lambda_A \tau_A} \, d\tau_A \right) \lambda_B e^{-\lambda_B \tau_B} d\tau_B \tag{3.38}$$

L'expression de probabilité peut être écrite comme suit (voir Annexe B.1) :

$$Pr(PAND) = b - \frac{\lambda_B}{\lambda_A + \lambda_B}(a + \overline{a} \cdot b) \tag{3.39}$$

Selon l'expression ci-dessus, l'expression de fréquence est obtenue en appliquant l'équation (3.34) comme suit :

$$fr(PAND) = \lambda_B \cdot \overline{b} - \frac{\lambda_B}{\lambda_A+\lambda_B}\left(\lambda_A \cdot \overline{a} - \lambda_A \cdot \overline{a} \cdot b + \lambda_B \cdot \overline{a} \cdot \overline{b}\right) =$$

$$\lambda_B \cdot \overline{b} - \frac{\lambda_B}{\lambda_A+\lambda_B}\left(\lambda_A \cdot \overline{a} \cdot (1-b) + \lambda_B \cdot \overline{a} \cdot \overline{b}\right) =$$

$$\lambda_B \cdot \overline{b} - \frac{\lambda_B}{\lambda_A+\lambda_B} \cdot \overline{a} \cdot \overline{b} \cdot (\lambda_A + \lambda_B) = \lambda_B \cdot \overline{b} - \lambda_B \cdot \overline{a} \cdot \overline{b}$$

$$fr(PAND) = \lambda_B \cdot \overline{b} \cdot a \tag{3.40}$$

3.5.3.2 Expression de fréquence pour la porte SPARE

Comme indiqué à la quatrième section, deux séquences de défaillance distinguent les modes dormant et actif pour l'événement de secours. L'expression de probabilité de la première séquence est obtenue comme pour la porte PAND. Cependant, l'expression de probabilité de la seconde séquence ne peut pas être obtenue directement par l'équation (3.15) car l'événement de secours ne peut se produire que pendant l'intervalle de temps $[t_A, t]$. Les probabilités des deux séquences se trouvent comme suit :

$$\begin{cases} Pr([B_d, A]) = \int_0^t \left(\int_0^{t_A} f_{B_d}(t_B)\, dt_B\right) f_A(t_A) dt_A \\ Pr([A, B_a]) = \int_0^t \left(\int_{t_A}^t f_{B_a}(t_B, t_A)\, dt_B\right) f_A(t_A) dt_A \end{cases} \tag{3.41}$$

Parce que $[B_d, A]$ et $[A, B_a]$ sont disjonctives, nous avons :

$$Pr(Spare) = Pr([B_d, A]) + Pr([A, B_a]) \tag{3.42}$$

De la même manière que pour la porte précédente, la probabilité de sortie de la porte SPARE peut également être exprimée au moyen de l'occurrence et la non-occurrence de ses événements d'entrée (voir Annexe B.2) :

$$Pr(Spare) = a - \frac{\lambda_A}{\lambda_A-(1-\alpha)\lambda_B}\overline{b} + \frac{\lambda_A}{\lambda_A-(1-\alpha)\lambda_B}\overline{a}\cdot\overline{b_\alpha}\text{ , pour } \lambda_B \neq \frac{\lambda_A}{1-\alpha} \quad (3.43)$$

Pour $\lambda_B = \frac{\lambda_A}{1-\alpha}$, la dernière expression ne doit pas être utilisée pour donner la probabilité de sortie de la porte Spare, et le calcul doit être référé aux intégrales dans l'équation (3.41) pour atteindre l'expression adoptée pour ce cas. L'obtention des probabilités de $[B_d, A]$ et $[A, B_a]$ nous permet d'avoir l'expression suivante :

$$Pr(Spare) = a - \lambda_A \cdot t\,\overline{b}\text{, pour } \lambda_B = \frac{\lambda_A}{1-\alpha} \quad (3.44)$$

L'expression de fréquence pour $\lambda_B \neq \frac{\lambda_A}{1-\alpha}$ est déduite à partir de l'équation (3.42) en appliquant l'équation (3.34). Pour $\lambda_B = \frac{\lambda_A}{1-\alpha}$ la fréquence est obtenue à partir de l'équation (3.43) en utilisant l'équation (3.32) car l'expression de probabilité est une fonction des événements d'entrée et du temps t. Finalement, nous obtenons :

$$fr(Spare) = \begin{cases} \overline{a}\cdot\lambda_A + \frac{\lambda_A\cdot\lambda_B}{\lambda_A-(1-\alpha)\lambda_B}\overline{b} - \frac{\lambda_A}{\lambda_A-(1-\alpha)\lambda_B}\,\overline{a}\cdot\overline{b_\alpha}(\lambda_A+\alpha\cdot\lambda_B)\text{ , for } \lambda_B \neq \frac{\lambda_A}{1-\alpha} \\ \lambda_A\cdot\overline{a} + (\lambda_B\cdot t - 1)\cdot\lambda_A\cdot\overline{b}\text{ , for } \lambda_B = \frac{\lambda_A}{1-\alpha} \end{cases} \quad (3.45)$$

3.5.3.3 Expression de fréquence pour la porte SEQ

L'expression de probabilité pour la porte SEQ est donnée en appliquant la relation suivante :

$$Pr(SEQ) = \int_0^t \left(\int_{t_A}^t \lambda_B e^{-\lambda_B(t_B-t_A)}\,dt_B\right)\lambda_A e^{-\lambda_A t_A} dt_A \quad (3.46)$$

Pour $\lambda_A = \lambda_B = \lambda$, elle devient :

$$Pr(SEQ) = \int_0^t \left(\int_{t_A}^t \lambda\cdot e^{-\lambda(t_B-t_A)}\,dt_B\right)\lambda\cdot e^{-\lambda t_A} dt_A \quad (3.47)$$

Formellement, pour les deux cas, nous avons (voir Annexe B.3) :

$$Pr(SEQ) = \begin{cases} a - \frac{\lambda_A}{\lambda_A - \lambda_B} \cdot \overline{b} + \frac{\lambda_A}{\lambda_A - \lambda_B} \cdot \overline{a}\,, \text{for } \lambda_A \neq \lambda_B \\ 1 - (1 + \lambda \cdot t)\, e^{-\lambda t}\,, \text{for } \lambda_A = \lambda_B = \lambda \end{cases} \quad (3.48)$$

Pour le premier cas de l'équation (3.48), l'expression de fréquence de la porte SEQ est obtenue en appliquant l'équation (3.34). Cependant, il convient de noter que la seconde formule n'est pas seulement fonction des événements d'entrée, à cause de l'existence de la variable t, la fréquence de défaillance associée est obtenue en utilisant l'équation (3.32). Enfin ça arrive :

$$fr(SEQ) = \begin{cases} \overline{a} \cdot \lambda_A + \frac{\lambda_A \cdot \lambda_B}{\lambda_A - \lambda_B} \overline{b} - \frac{{\lambda_A}^2}{\lambda_A - \lambda_B} \overline{a} = \frac{\lambda_A \cdot \lambda_B}{\lambda_A - \lambda_B} \cdot \left(\overline{b} - \overline{a}\right), \text{pour } \lambda_A \neq \lambda_B \\ -\lambda \cdot e^{-\lambda t} + \lambda \cdot e^{-\lambda t} + \lambda \cdot t \cdot \lambda \cdot e^{-\lambda t} = \lambda^2 \cdot t\, e^{-\lambda t}\,, \text{pour } \lambda_A = \lambda_B = \lambda \end{cases} \quad (3.49)$$

3.5.3.4 Comparaison des résultats

Les fréquences de défaillance des sorties des portes obtenues à la section 3.4 en utilisant les séquences avant-défaillance sont vérifiées par rapport à celles obtenues en convertissant les expressions de probabilité de défaillance correspondantes. Pour la porte PAND, l'équation (3.24) donne l'expression équivalente de l'équation (3.40). Les expressions de fréquence pour les portes SPARE et SEQ données par les équations (3.27) et (3.29) sont identiques aux premiers cas des équations (3.45) et (3.48) respectivement. La faisabilité du modèle détaillé dans la section 3.4 pour donner la valeur précise de la fréquence de défaillance pour tout DFT sera montrée dans les prochaines sections.

3.6 Analyse de Système gicleur hypothétique

Dans cette section, nous illustrons la méthodologie proposée pour résoudre le DFT lié à un système dynamique. Le système présenté ici est un système gicleur hypothétique (Hypothetical sprinkler system (HSS)) [54], qui peut être considéré comme un système instrumenté de sécurité (SIS) (voir Figure 3.2).

Il est composé de trois capteurs, deux pompes et une unité de contrôle numérique. Lorsque la température relevée sur deux des capteurs (S1, S2 et S3) atteint la valeur seuil, l'unité de contrôle digitale (DigCon) active la pompe. Chaque pompe possède un flux de support composé de vannes et de filtres (VF1 et VF2) qui est par défaillance, cause l'indisponibilité de la pompe. Une des pompes est considérée comme une pompe de secours (P2) qui fonctionne si la pompe principale (P1) tombe en panne.

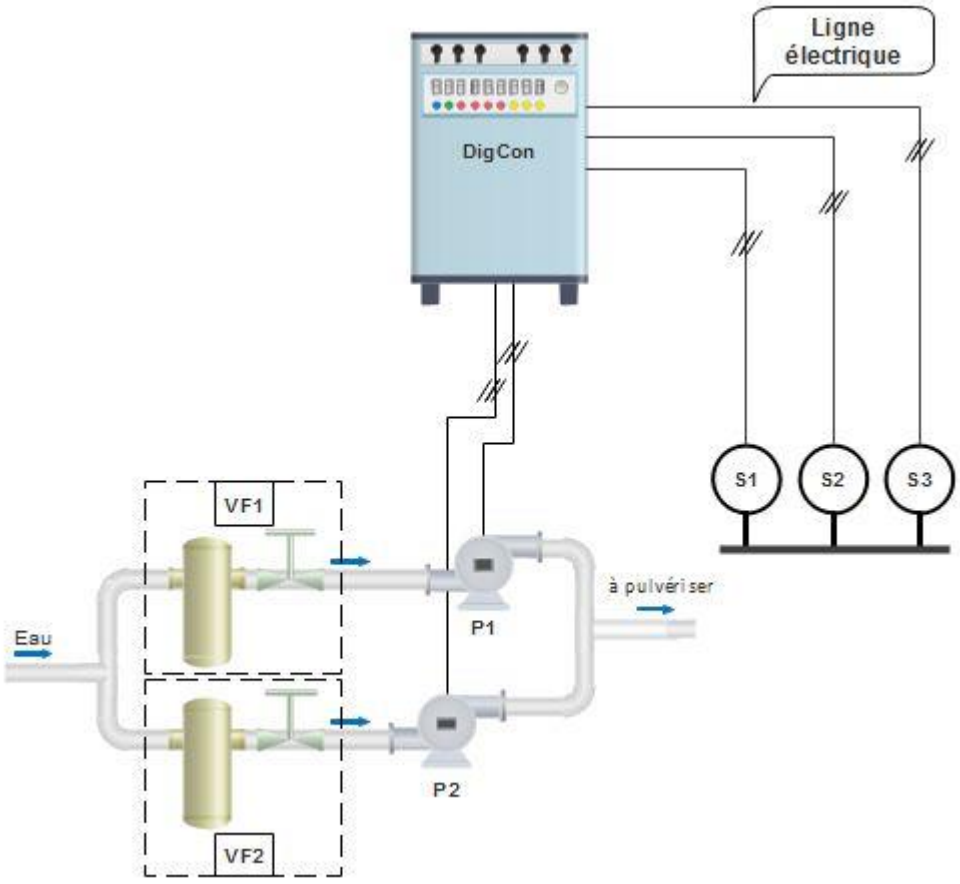

Figure 3.2 Système gicleur hypothétique (HSS) [68]

Tableau 3.1 Taux de défaillance des composants de HSS [54]

Composant	Lambda (λ)
Capteurs (S_1, S_2, S_3)	$10^{-4}\ h^{-1}$
VF_1, VF_2	$10^{-5}\ h^{-1}$
Pompes (P_1, P_2)	$10^{-6}\ h^{-1}$
DigCon	$10^{-6}\ h^{-1}$

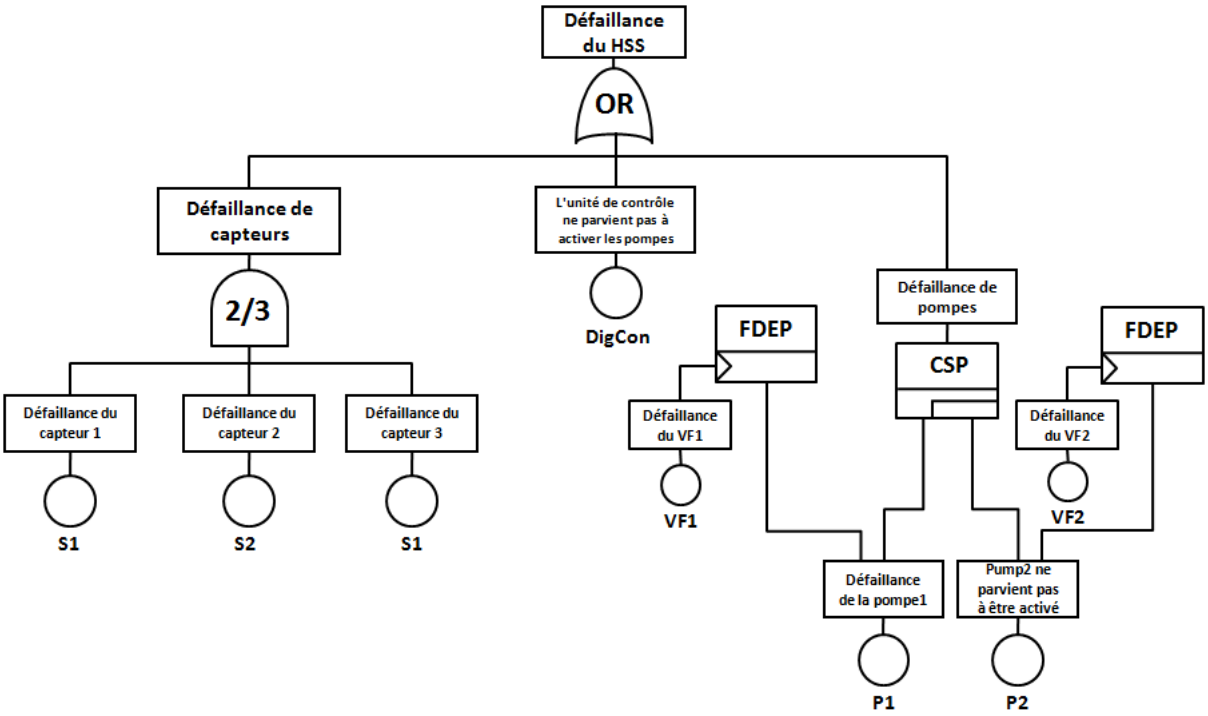

Figure 3.3 DFT modélisant la défaillance du HSS [68]

La Figure 3.3 représente le DFT du système, tandis que les taux de défaillance correspondants sont rassemblés dans le Tableau 3.1. Il convient de noter que la porte CSP (porte de secours froide) qualifie la porte de secours (SPARE) avec $\alpha = 0$. L'objet de l'étude est de calculer la probabilité et la fréquence de défaillance du HSS sur la base de la détermination des séquences de défaillance en utilisant l'approche proposée du DFT et de démontrer ainsi sa capacité de modélisation et d'analyse des systèmes avec des dépendances fonctionnelles et dynamiques. Les résultats obtenus seront comparés à ceux dérivés du modèle de Markov correspondant présenté à la Figure 3.4.

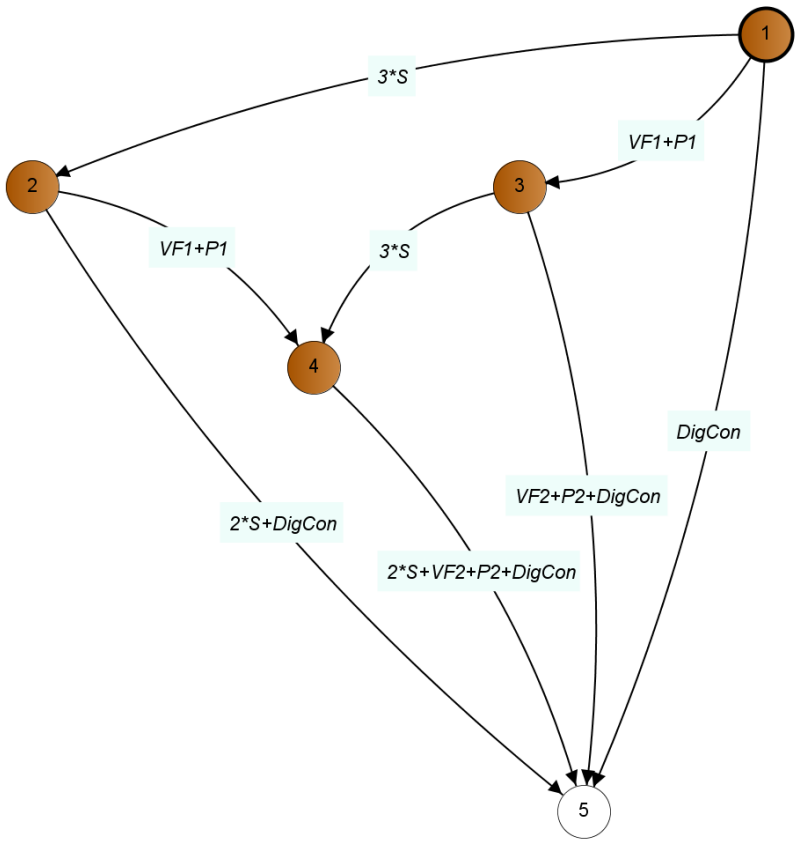

Figure 3.4 Modèle markovien relatif à la défaillance du HSS [68]

3.6.1 Fonction de structure pour la défaillance du HSS

La fonction de structure du DFT présentée dans la Figure 3.3 peut être exprimée comme suit :

$$Défaillance\ du\ HSS = Défaillance\ de\ capteurs + DigCon + Défaillance\ de\ pompes$$

$$Défaillance\ du\ HSS = (S_1S_2 + S_2S_3 + S_1S_3) + DigCon + (P_2{+}VF_2) \cdot (P_1 + VF_1) \triangleleft (P_2{+}VF_2) \tag{3.50}$$

Le terme $\left((P_2{+}VF_2) \cdot (P_1 + VF_1) \triangleleft (P_2{+}VF_2)\right)$ peut être simplifié en utilisant les théorèmes de simplification (les équations (3.8) et (3.9)), il devient:

$$Défaillance\ de\ pompes\ = (P_2{+}VF_2)\cdot[P_1{\lhd}(P_2{+}VF_2)+VF_1{\lhd}(P_2{+}VF_2)]=$$
$$(P_1{\lhd}P_2)(P_1{\lhd}VF_2)(P_2{+}VF_2)+(VF_1{\lhd}P_2)(VF_1{\lhd}VF_2)(P_2{+}VF_2)=(P_1{\lhd}P_2)(P_1{\lhd}VF_2)\cdot$$
$$P_2+(P_1{\lhd}P_2)(P_1{\lhd}VF_2)\cdot VF_2+(VF_1{\lhd}P_2)(VF_1{\lhd}VF_2)\cdot P_2+(VF_1{\lhd}P_2)(VF_1{\lhd}VF_2)\cdot VF_2$$

Par conséquent, la fonction de structure devient :

$$Défaillance\ du\ HSS=(S_1S_2+S_2S_3+S_1S_3)+DigCon+$$
$$(P_1{\lhd}P_2)(P_1{\lhd}VF_2)\cdot P_2+(P_1{\lhd}P_2)(P_1{\lhd}VF_2)\cdot VF_2+(VF_1{\lhd}P_2)(VF_1{\lhd}VF_2)\cdot \quad (3.51)$$
$$P_2+(VF_1{\lhd}P_2)(VF_1{\lhd}VF_2)\cdot VF_2$$

Nous notons que le terme $\big((P_2{+}VF_2)\cdot(P_1+VF_1){\lhd}(P_2{+}VF_2)\big)$ ne peut être représenté que par la séquence $[(P_1+VF_1),(P_2{+}VF_2)]$. Dans le cas de la distribution exponentielle, (P_1+VF_1) et $(P_2{+}VF_2)$ sont considérés comme deux événements de base et leurs probabilités peuvent être exprimées comme suit :

$$\begin{cases} Pr(P_1+VF_1)=1-e^{-(\lambda_{P_1}+\lambda_{VF_1})t} \\ Pr(P_2+VF_2)=1-e^{-(\lambda_{P_2}+\lambda_{VF_2})t} \end{cases} \quad (3.52)$$

3.6.2 Coupes minimales et séquences de défaillance

Selon la fonction de structure (l'équation (3.51)), les termes S_1S_2, S_2S_3, S_1S_3 et $DigCon$ sont considérés comme des coupes minimales. Dans le cas de la partie dynamique, les séquences de défaillance peuvent être déterminées à partir des quatre termes dynamiques :

$\big((P_1{\lhd}P_2)(P_1{\lhd}VF_2)\cdot P_2\big)$, $\big((P_1{\lhd}P_2)(P_1{\lhd}VF_2)\cdot VF_2\big)$, $\big((VF_1{\lhd}P_2)(VF_1{\lhd}VF_2)\cdot P_2\big)$ et

$\big((VF_1{\lhd}P_2)(VF_1{\lhd}VF_2)\cdot VF_2\big)$.

Les séquences de défaillance respectives sont :

$\big([P_1,VF_2,P_2],[P_1,P_2,VF_2],[P_1,P_2,\overline{VF_2}]\big)$, $\big([P_1,P_2,VF_2],[P_1,VF_2,P_2],[P_1,VF_2,\overline{P_2}]\big)$,

$\left([VF_1, VF_2, P_2], [VF_1, P_2, VF_2], [VF_1, P_2, \overline{VF_2}]\right)$ et
$\left([VF_1, P_2, VF_2], [VF_1, VF_2, P_2], [VF_1, VF_2, \overline{P_2}]\right)$

En supprimant les séquences répétées, nous obtenons les séquences de défaillance primaires suivantes triées en deux ensembles :

$\left\{[P_1, VF_2, P_2], [P_1, P_2, \overline{VF_2}], [P_1, P_2, VF_2], [P_1, VF_2, \overline{P_2}]\right\}$ et
$\left\{[VF_1, VF_2, P_2], [VF_1, P_2, \overline{VF_2}], [VF_1, P_2, VF_2], [VF_1, VF_2, \overline{P_2}]\right\}$.

Pour éliminer les conjonctions entre les séquences, nous devons ajouter l'événement P_1 du premier ensemble aux séquences du deuxième ensemble. Notons qu'à partir du premier ensemble P_1 ne peut pas être ajouté avant $[VF_2, P_2]$, $[P_2, \overline{VF_2}]$, $[P_2, VF_2]$ et $[VF_2, \overline{P_2}]$ dans le deuxième ensemble. Par ailleurs P_1 est un événement primaire et ne peut être pris en compte après l'occurrence d'événements de secours (P_2 et VF_2). Ainsi, les séquences primaires restent inchangées et les séquences de défaillance disjonctives finales sont :

$[P_1, VF_2, P_2], [P_1, P_2, \overline{VF_2}], [P_1, P_2, VF_2], [P_1, VF_2, \overline{P_2}], [VF_1, VF_2, P_2], [VF_1, P_2, \overline{VF_2}]$, $[VF_1, P_2, VF_2]$ et $[VF_1, VF_2, \overline{P_2}]$.

3.6.3 Calcul de probabilité de défaillance

La probabilité d'occurrence de l'événement sommet du DFT peut être trouvée par l'application de l'équation (3.12) :

$$Pr_{(Défaillance\ du\ HSS)} = Pr_{(Défaillance\ de\ capteurs+DigCon)} + Pr_{(Défaillance\ de\ pompes\ )} - Pr_{(Défaillance\ de\ capteurs+DigCon)} \cdot Pr_{(Défaillance\ de\ pompes)} \quad (3.53)$$

Où:

$$\begin{cases} Pr_{(Défaillance\ de\ capteurs+DigCon)} = Pr_{(DigCon)} + \left(1 - Pr_{(DigCon)}\right) \cdot Pr_{(Défaillance\ de\ capteurs)} \\ Pr_{(Défaillance\ de\ capteurs)} = s_1 \cdot s_2 + s_2 \cdot s_3 \cdot \overline{s_1} + s_1 \cdot s_3 \cdot \overline{s_2} \\ Pr_{(Défaillance\ de\ pompes)} = \sum Pr(Séquences\ de\ défaillance\ disjunctive) \end{cases} \quad (3.54)$$

Comme nous l'avons vu, l'événement ($Défaillance\ de\ pompes$) est représenté par la séquence de défaillance $[(P_1 + VF_1), (P_2 + VF_2)]$. Donc, il n'est pas nécessaire de détailler les probabilités de toutes les séquences de défaillance disjonctives et l'expression de probabilité doit être obtenue en utilisant l'équation (3.43) comme suit :

$$\begin{aligned} &Pr([(P_1 + VF_1), (P_2 + VF_2)]) \\ &= (p + vf - p \cdot vf) - (\lambda_P + \lambda_{VF}) \cdot \overline{(p + vf - p \cdot vf)} \cdot t \end{aligned} \quad (3.55)$$

Sachant que: $p = p_1 = p_2$ et $vf = vf_1 = vf_2$.

Par conséquent, la probabilité de l'événement sommet peut être écrite comme suit :

$$\begin{aligned} &Pr_{(Défaillance\ du\ HSS)} = Pr_{(DigCon)} + \left(1 - Pr_{(DigCon)}\right) \cdot \\ &Pr_{(Défaillance\ de\ capteurs)} + Pr([(P_1 + VF_1), (P_2 + VF_2)]) - Pr_{(DigCon)} + \\ &\left(1 - Pr_{(DigCon)}\right) \cdot Pr_{(Défaillance\ de\ capteurs)} \cdot Pr([(P_1 + VF_1), (P_2 + VF_2)]) \end{aligned} \quad (3.56)$$

3.6.4 Calcul de fréquence de défaillance

La fréquence de défaillance du système est obtenue en utilisant la règle de conversion (les équations (3.34) et (3.21)) pour les parties statiques et dynamiques.

Considérant un système S contenant trois sous-systèmes A, B et C en série, la fréquence de défaillance de S peut être exprimée comme suit :

$$fr_{(S)} = fr_{(A)} \cdot \overline{b} \cdot \overline{c} + fr_{(B)} \cdot \overline{a} \cdot \overline{c} + fr_{(C)} \cdot \overline{a} \cdot \overline{b} \quad (3.57)$$

Par conséquent, la fréquence de défaillance du HSS peut être écrite comme suit :

$$fr_{(Défaillance\ du\ HSS)} = fr_{(Défaillance\ de\ capteurs)} \cdot \overline{digcon} \cdot \overline{PumpFault} + \quad (3.58)$$

$$fr_{(DigCon)} \cdot \overline{Défaillance\ de\ capteurs} \cdot \overline{Défaillance\ de\ pompes} + fr_{(Défaillance\ de\ pompes)} \cdot \overline{digcon} \cdot \overline{Défaillance\ de\ capteurs}$$

$$fr_{(Défaillance\ de\ capteurs)} = s_1 \cdot \overline{s_2} \cdot \overline{s_3} \cdot (\lambda_{S_2} + \lambda_{S_3}) + s_2 \cdot \overline{s_1} \cdot \overline{s_3} \cdot (\lambda_{S_1} + \lambda_{S_3}) + s_3 \cdot \overline{s_1} \cdot \overline{s_2} \cdot (\lambda_{S_1} + \lambda_{S_2}) \quad (3.59)$$

Puisque: $s_1 = s_2 = s_3 = s$, ça devient :

$$fr_{(Défaillance\ de\ capteurs)} = 3 \cdot (2 \cdot \lambda_S) \cdot s \cdot \overline{s}^{\,2} \quad (3.60)$$

$$fr_{(DigCon)} = \lambda_{DigCon} \cdot \overline{digcon} \quad (3.61)$$

L'événement $Défaillance\ de\ pompes$ est une porte de secours froide (CSP), donc nous avons :

$$fr_{(Défaillance\ de\ pompes)} = \left(Pr\left([(P+VF)_d, \overline{(P+VF)}]\right) + Pr\left([(P+VF), \overline{(P+VF)_a}]\right)\right) \cdot \left(\lambda_p + \lambda_{vf}\right) \quad (3.62)$$

$$\begin{cases} Pr\left([(P+VF)_d, \overline{(P+VF)}]\right) = e^{-(\lambda_p+\lambda_{vf})t} \cdot \left(\int_0^t \alpha\left(\lambda_p + \lambda_{vf}\right) \cdot e^{-\alpha\left(\lambda_p+\lambda_{vf}\right)\cdot t_B}\, dt_B\right) \\ Pr\left([(P+VF), \overline{(P+VF)_a}]\right) = e^{-\left(\lambda_p+\lambda_{vf}\right)\cdot(t-(1-\alpha)t_A)} \cdot \left(\int_0^t \left(\lambda_p + \lambda_{vf}\right) \cdot e^{-\left(\lambda_p+\lambda_{vf}\right)\cdot t_A} dt_A\right) \end{cases} \quad (3.63)$$

$$\Leftrightarrow$$

$$\begin{cases} Pr\left([(P+VF)_d, \overline{(P+VF)}]\right) = \alpha\left(\lambda_p + \lambda_{vf}\right) \cdot e^{-\left(\lambda_p+\lambda_{vf}\right)\cdot t} \int_0^t e^{-\alpha\left(\lambda_p+\lambda_{vf}\right)\cdot t_B}\, dt_B \\ Pr\left([(P+VF), \overline{(P+VF)_a}]\right) = \left(\lambda_p + \lambda_{vf}\right) \cdot e^{-\lambda_B \cdot t} \cdot \int_0^t e^{-\left(\left(\lambda_p+\lambda_{vf}\right)-\left(\lambda_p+\lambda_{vf}\right)\right)\cdot t_A}\, dt_A \end{cases} \quad (3.64)$$

$$\Leftrightarrow \begin{cases} Pr\left([(P+VF)_d, \overline{(P+VF)}]\right) = 0 \\ Pr\left([(P+VF), \overline{(P+VF)_a}]\right) = \left(\lambda_p + \lambda_{vf}\right) \cdot e^{-\left(\lambda_p+\lambda_{vf}\right)\cdot t} \cdot t \end{cases} \quad (3.65)$$

Par conséquent, nous obtenons :

$$fr_{(Défaillance\ de\ pompes)} = \left(\lambda_p + \lambda_{vf}\right)^2 \cdot \overline{(p + vf - p \cdot vf)} \cdot t \tag{3.66}$$

3.6.5 Résultats numériques

Le Tableau 3.2 rassemble les résultats obtenus, à t = 1000 h, à partir de l'approche proposée (les équations (3.56) et (3.58)) et ceux dérivés d'une approche basée sur les chaines de Markov. La probabilité et la fréquence de défaillance du HSS peuvent être déduites du modèle de Markov de la Figure 3.4 comme suit :

$$Pr_{(Défaillance\ du\ HSS)} = E_5 \tag{3.67}$$

$$\begin{aligned} fr_{(Défaillance\ du\ HSS)} = E_1 \cdot \lambda_{DigCon} + E_2 \cdot \left(2 \cdot \lambda_S + \lambda_{DigCon}\right) + E_3 \cdot \\ \left(\lambda_p + \lambda_{vf} + \lambda_{DigCon}\right) + E_4 \cdot \left(2 \cdot \lambda_S + \lambda_{DigCon} + \lambda_p + \lambda_{vf}\right) \end{aligned} \tag{3.68}$$

Où E_i représente la probabilité d'être dans l'état i. Le modèle de Markov a été développé et évalué à l'aide du logiciel GRIF [79].

Tableau 3.2 Probabilité et fréquence de défaillance du HSS

Résultats	Approche proposée	Model de Markov
$Pr_{(Défaillance\ du\ HSS)}$	2.6476E-02	2.6476E-02
$Pr_{(Défaillance\ de\ pompes\ )}$	6.0058E-05	6.0058E-05
$fr_{(Défaillance\ du\ HSS)}$($h^{-1}$)	4.7788E-05	4.7788E-05

Le Tableau 3.2 montre que l'approche proposée et le modèle de Markov donnent des résultats similaires. Ceci peut être vu comme une validation de la méthodologie proposée. De plus, la Figure 3.5 illustre la variation de la probabilité et de la fréquence de défaillance du HSS.

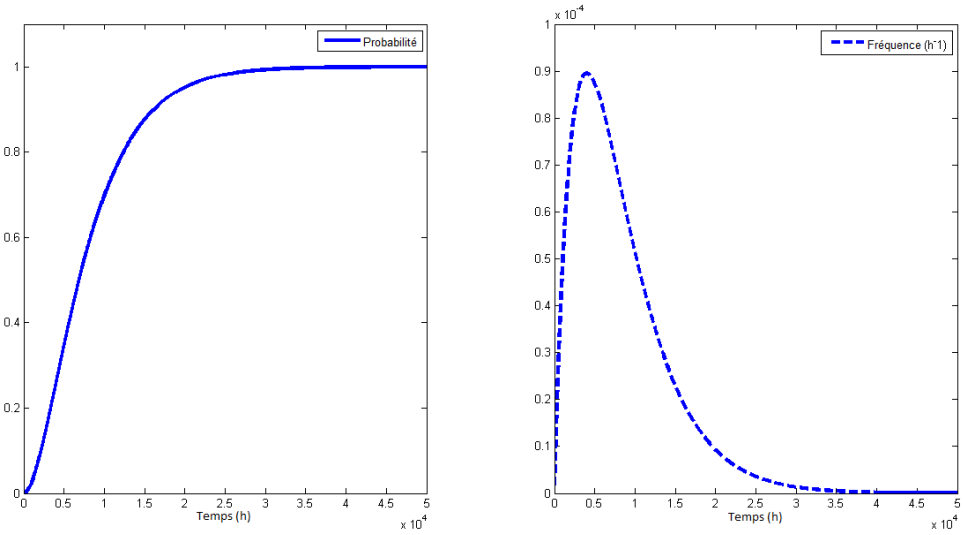

Figure 3.5 Variation de probabilité et fréquence de défaillance pour HSS

3.7 Système de chaudière à vapeur

3.7.1 Description du système et problème posé en DFT

Le système sélectionné ici est un système de génération de vapeur conçu pour produire de la vapeur à une pression spécifique [44]. La Figure 3.6 montre le schéma simple du système de chaudière à vapeur (Steam boiler system (SBS)) considéré. Il est principalement composé de trois sous-systèmes, une chaudière à vapeur alimentée en eau, une chambre de combustion alimentée en carburant et un système de barrières utilisé pour contrôler les paramètres de niveau et de pression afin de garantir une pression nominale et de protéger le système contre les événements indésirables.

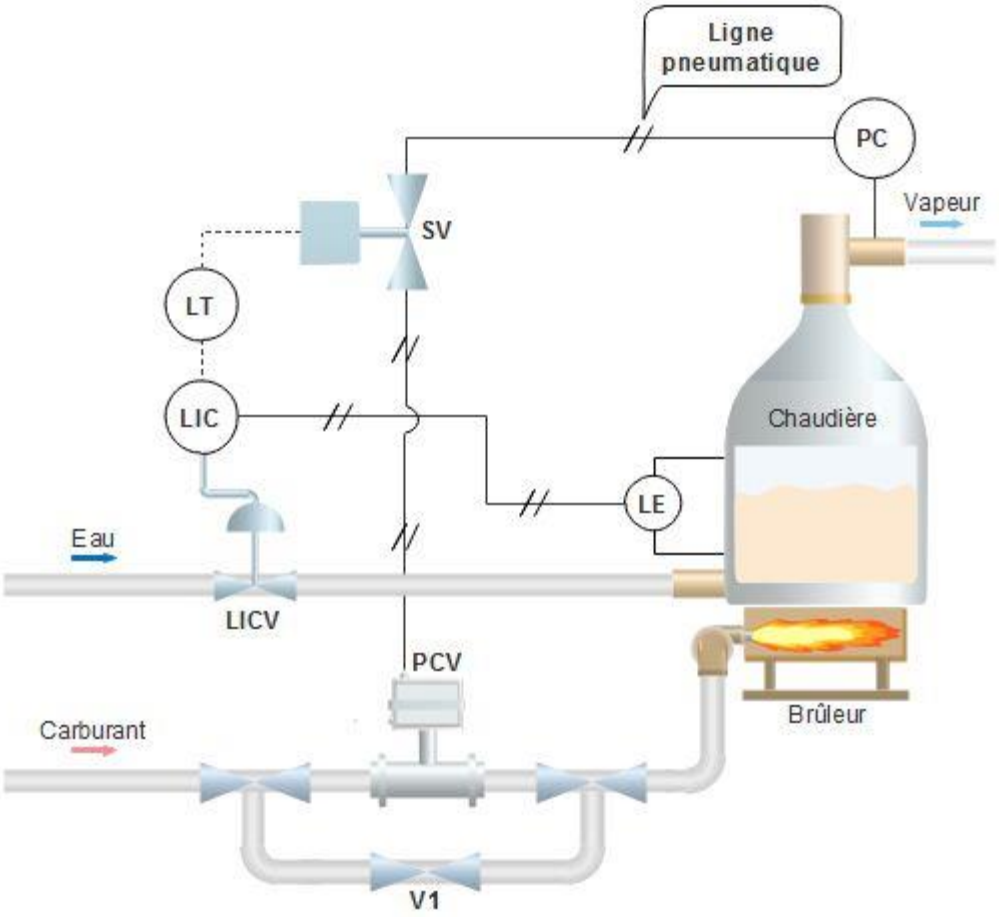

Figure 3.6 Système de chaudière à vapeur (SBS) [68]

Le système de barrières est composé de trois couches de protection comme indiqué dans [28,68] :

Couche 1 (LA_1): Elle est composée d'un émetteur de niveau (LE), d'un contrôleur d'indicateur de niveau (LIC) et d'une vanne de contrôleur d'indicateur de niveau (LICV). Le niveau d'eau dans la chaudière est contrôlé par LE. L'indicateur de niveau (LIC) traduit le signal pneumatique du LE en un signal pneumatique commandant la vanne régulatrice d'eau LICV afin de maintenir le niveau d'eau dans un intervalle compris entre un niveau bas spécifié et un niveau haut spécifié.

Couche 2 (LA2): Elle est composée de LE, LIC, un transmetteur de niveau (LT), une électrovanne (SV) et une vanne de régulation de pression (PCV). Lorsque le niveau d'eau se

rapproche du niveau bas, un signal pneumatique est transmis du LIC au LT, qui traduit le signal pneumatique en un signal électrique qui est envoyé au SV. L'électrovanne commande à nouveau la vanne PCV sur la conduite de carburant. V-1 est une vanne de dérivation installée en parallèle avec le PCV et deux vannes d'isolement afin de simplifier l'inspection et la maintenance de la PCV en fonctionnement normal. Notons que V-1 et les vannes d'isolement ne sont pas prises en compte dans cette étude.

Couche 3 (LA3): elle contient les mêmes vannes que la deuxième couche avec un contrôleur de pression (PC). La pression dans la canalisation de sortie de vapeur est contrôlée par le PC qui est connecté à la vanne SV, puis à la vanne PCV sur la canalisation de carburant.

L'événement indésirable «Rupture de la chaudière à vapeur due à une surpression non contrôlée» se produit si la chaudière n'est pas alimentée en eau et si le brûleur continue à fonctionner. Pour éviter la survenue de cette situation critique, la couche 1 régule le niveau d'eau dans la chaudière à vapeur et les couches 2 et 3 ont pour fonction de couper l'alimentation en combustible du brûleur en cas d'un faible niveau d'eau dans la chaudière ou si la pression augmente au-dessus d'une valeur élevée de pression spécifiée, c'est-à-dire lorsque la première couche est défaillante.

Un scénario LOPA représente le chemin qui mène à la pire conséquence (explosion de la chaudière à vapeur) à travers l'arbre d'événements (voir la Figure 3.7). En règle générale, l'événement indésirable se produit si et seulement si l'ensemble du système de barrières (défaillance de la coupure du carburant) est indisponible lorsque l'événement initiateur (défaillance de la régulation de l'eau) est survenu. Par conséquent, le scénario LOPA est un DFT avec deux événements intermédiaires (système de barrière et événement initiateur) liés à une porte PAND. La Figure 3.7 représente le modèle d'arbre d'événements du scénario d'accident, tandis que la Figure 3.8 montre le DFT équivalent présentant les dépendances fonctionnelles et dynamiques entre les couches. Les taux de défaillance des composants sont rassemblés dans le Tableau 3.3.

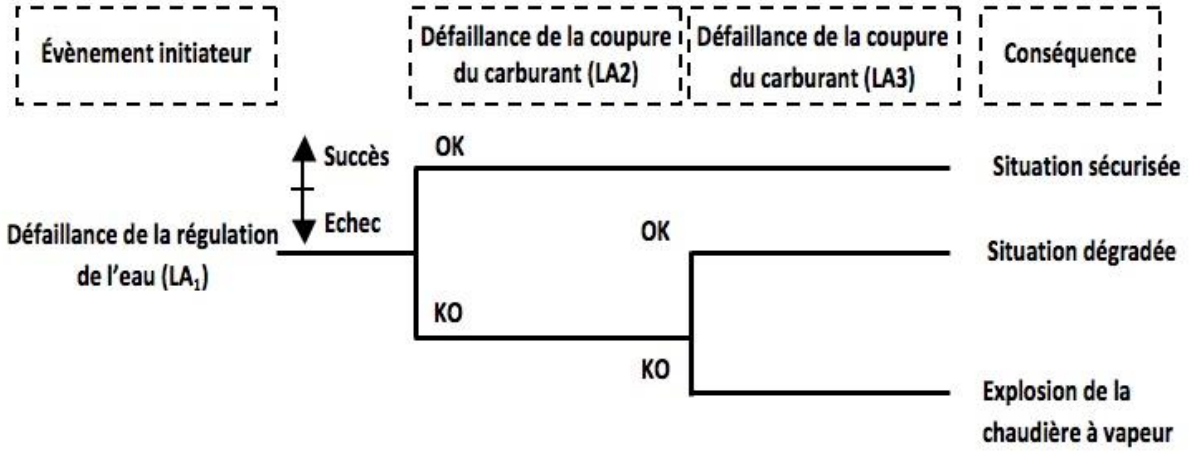

Figure 3.7 Arbre d'événements du scénario d'accident Explosion de la chaudière à vapeur [68]

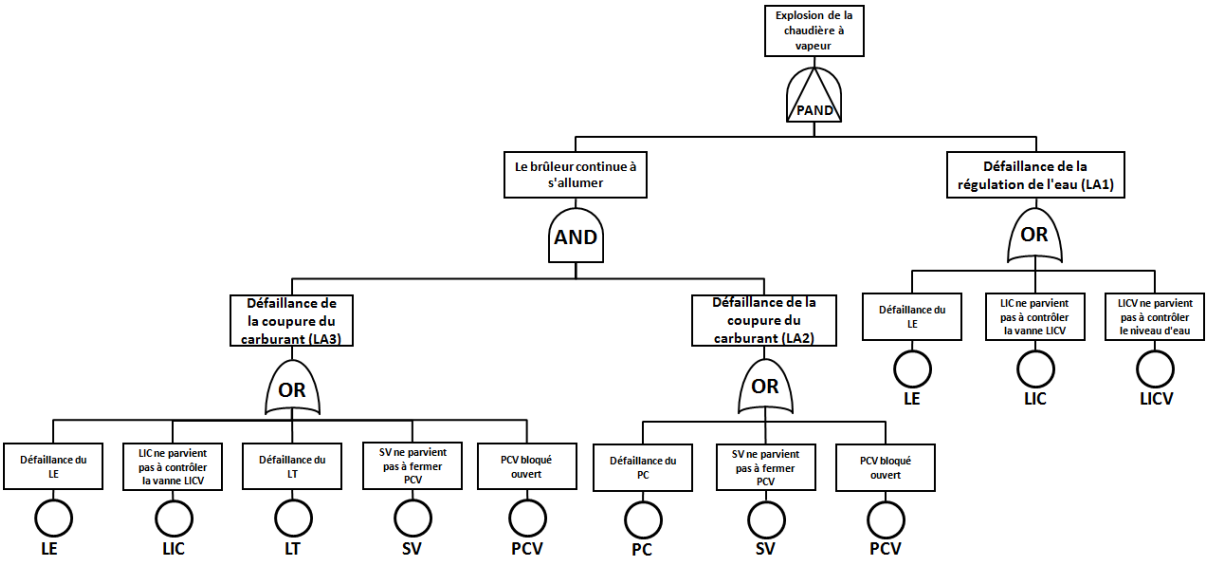

Figure 3.8 DFT modélisant la défaillance du SBS [68]

Tableau 3.3 Taux de défaillance des composants de SBS [28]

Composants	LE	LIC	LICV	LT	PC	SV	PCV
Taux de défaillance λ (h^{-1})	1.3E-6	5E-6	2.7E-6	6E-7	1.6E-6	9E-7	2E-6

3.7.2 Fonction de structure de défaillance du SBS

Premièrement, nous devons définir la forme algébrique de l'événement sommet défaillance du SBS «explosion de la chaudière à vapeur». Nous définissons les symboles algébriques suivants A, B, C, D et E qui représentent la défaillance des composants $(LE\ OR\ LIC)$, $LICV$, LT, $(SV\ OR\ PCV)$ et PC, respectivement. Pas à pas, la fonction de structure finale peut être développée et simplifiée à l'aide des théorèmes fournis dans [8].

$$Défaillance\ du\ SBS = LA_1 \cdot \left[(LA_2 \cdot\ LA_3) \underline{\lhd} LA_1\right]$$

$$= (A+B) \cdot \left[(LA_2 \cdot\ LA_3) \underline{\lhd} (A+B)\right] = (A+B) \cdot \left[\left((A+C+D) \cdot (\mathrm{E}+\mathrm{D})\right) \underline{\lhd} (A+B)\right]$$

$$= (A+B) \cdot \left[\left((A+C+D) \underline{\lhd} (A+B)\right) \cdot \left((\mathrm{E}+\mathrm{D}) \underline{\lhd} (A+B)\right)\right]$$

$$= (A+B) \cdot \left[\left(A \underline{\lhd} (A+B) + C \underline{\lhd} (A+B) + D \underline{\lhd} (A+B)\right) \cdot \left(\mathrm{E} \underline{\lhd} (A+B) + D \underline{\lhd} (A+B)\right)\right]$$

$$Défaillance\ du\ SBS = (A+B) \cdot \left[\left(\left(A \underline{\lhd} A\right)\left(A \underline{\lhd} B\right) + \left(C \underline{\lhd} A\right)\left(C \underline{\lhd} B\right) + \left(D \underline{\lhd} A\right)\left(D \underline{\lhd} B\right)\right) \cdot \left(\left(E \underline{\lhd} A\right)\left(E \underline{\lhd} B\right) + \left(D \underline{\lhd} A\right)\left(D \underline{\lhd} B\right)\right)\right] \quad (3.69)$$

Cette expression peut être simplifiée grâce aux théorèmes (équations (3.4) et (3.5)), après quelques réarrangements, nous obtenons :

$$Défaillance\ du\ SBS = (A+B) \cdot [(E \lhd A)(A \lhd B)(E \lhd B) + (C \lhd A)(C \lhd B)(E \lhd A)(E \lhd B) + (D \lhd A)(D \lhd B)(E \lhd A)(E \lhd B) + (A \lhd B)(D \lhd A)(D \lhd B) + (C \lhd A)(C \lhd B)(D \lhd A)(D \lhd B) + (D \lhd A)(D \lhd B)]$$

Les termes inutiles peuvent être supprimés en appliquant les théorèmes des équations (3.2) et (3.11), finalement il devient :

$$Défaillance\ du\ SBS = (A \lhd B)(E \lhd A) + A \cdot (C \lhd A)(C \lhd B)(E \lhd A)(E \lhd B) + \quad (3.70)$$

$$B \cdot (C \lhd A)(C \lhd B)(E \lhd A)(E \lhd B) + A \cdot (D \lhd A)(D \lhd B) + B \cdot (D \lhd A)(D \lhd B)$$

3.7.3 Détermination des séquences de défaillance

L'équation (3.70) donne cinq termes formant la fonction de structure de la défaillance SBS. Chacune d'elles produit des séquences de défaillance menant à l'événement sommet.

$[E, A, B]$, $[E, A, \overline{B}]$,
$[E, C, B, A]$, $[E, C, A, \overline{B}]$, $[C, E, A, B]$, $[C, E, B, \overline{A}]$, $[C, E, B, A]$, $[C, E, A, \overline{B}]$, $[E, C, A, B]$, $[E, C, B, \overline{A}]$,
$[D, B, A]$, $[D, A, \overline{B}]$, $[D, A, B]$, $[D, B, \overline{A}]$.

La séquence $[E, A, B]$ absorbe les deux séquences $[E, C, A, B]$ et $[C, E, A, B]$, et les deux séquences $[C, E, A, \overline{B}]$ et $[E, C, A, \overline{B}]$ sont incluses dans $[E, A, \overline{B}]$. Ainsi, les séquences incluses seront supprimées pour que les séquences de défaillance primaires soient triées en trois ensembles, comme suit :

$\{[D, B, A], [D, A, \overline{B}], [D, A, B], [D, B, \overline{A}]\}$, $\{[E, A, B], [E, A, \overline{B}]\}$ et
$\{[E, C, B, A], [E, C, B, \overline{A}], [C, E, B, A], [C, E, B, \overline{A}]\}$.

À partir de ces séquences, l'analyse doit être réalisée avec la détermination des séquences de défaillance disjonctives. Pour éliminer les conjonctions existantes entre les séquences, l'élément D du premier ensemble doit être ajouté aux deux derniers ensembles tout en préservant la propriété d'absorption. À partir de cette condition, il convient de noter que D ne peut en aucun cas être ajouté avant $[B, A]$, $[A, \overline{B}]$, $[A, B]$ et $[B, \overline{A}]$. Par conséquent, nous obtenons les séquences de défaillance disjonctives :

$[D, B, A]$, $[D, A, \overline{B}]$, $[D, A, B]$, $[D, B, \overline{A}]$,
$[E, A, D, B]$, $[E, A, B, D]$, $[E, A, B, \overline{D}]$, $[E, A, D, \overline{B}]$, $[E, A, \overline{B}, \overline{D}]$,
$[E, C, B, D, A]$, $[E, C, B, A, D]$, $[E, C, B, A, \overline{D}]$, $[E, C, B, D, \overline{A}]$, $[E, C, B, \overline{A}, \overline{D}]$,
$[C, E, B, D, A]$, $[C, E, B, A, D]$, $[C, E, B, A, \overline{D}]$, $[C, E, B, D, \overline{A}]$, $[C, E, B, \overline{A}, \overline{D}]$.

3.7.4 Calcul de probabilité de défaillance du SBS

La probabilité de défaillance de l'événement sommet peut être simplement trouvée par la relation suivante :

$$Pr_{(Défaillance\ du\ SBS)} = Pr\left(\sum Séquences\ de\ défaillance\ disjonctives\right) \quad (3.71)$$

Les expressions de probabilité de défaillance fournies dans l'Annexe C sont utilisées pour calculer les probabilités de séquences de défaillance disjonctives déterminées.

3.7.5 Calcul de fréquence de défaillance du SBS

Premièrement, nous devons déterminer les séquences avant défaillance. Une séquence avant défaillance peut être obtenue en considérant la non-occurrence du dernier événement survenu dans une séquence de défaillance disjonctive.

$[D, B, \overline{A}]$, $[D, \overline{A}, \overline{B}]$, $[D, A, \overline{B}]$, $[D, \overline{B}, \overline{A}]$,
$[E, A, D, \overline{B}]$, $[E, A, \overline{D}, \overline{B}]$, $[E, A, B, \overline{D}]$, $[E, A, \overline{B}, \overline{D}]$, $[E, \overline{A}, \overline{B}, \overline{D}]$,
$[E, C, B, D, \overline{A}]$, $[E, C, B, A, \overline{D}]$, $[E, C, B, \overline{A}, \overline{D}]$, $[E, C, B, \overline{D}, \overline{A}]$, $[E, C, \overline{B}, \overline{A}, \overline{D}]$,
$[C, E, B, D, \overline{A}]$, $[C, E, B, A, \overline{D}]$, $[C, E, B, \overline{A}, \overline{D}]$, $[C, E, B, \overline{D}, \overline{A}]$, $[C, E, \overline{B}, \overline{A}, \overline{D}]$.

Dans un deuxième temps, nous éliminons les séquences avant défaillance absorbées. Il en résulte :

$[D, \overline{A}, \overline{B}]$, $[D, \overline{B}, \overline{A}]$, $[E, \overline{A}, \overline{B}, \overline{D}]$, $[E, C, \overline{B}, \overline{A}, \overline{D}]$ et $[C, E, \overline{B}, \overline{A}, \overline{D}]$.

La fréquence de défaillance peut être trouvée en utilisant la relation :

$$\begin{aligned} fr_{(Défaillance\ du\ SBS)} = {} & Pr\left([D, \overline{A}, \overline{B}]\right) \cdot \lambda_A + Pr\left([D, \overline{B}, \overline{A}]\right) \cdot \lambda_B + \\ & Pr\left([E, \overline{A}, \overline{B}, \overline{D}]\right) \cdot \lambda_A + Pr\left([E, C, \overline{B}, \overline{A}, \overline{D}]\right) \cdot \lambda_B + Pr\left([C, E, \overline{B}, \overline{A}, \overline{D}]\right) \cdot \lambda_B \end{aligned} \quad (3.72)$$

3.7.6 Analyse de risque avec LOPA et DFT

L’approche de l’analyse de risque peut être résumée en effectuant les étapes principales suivantes :

- Identifier l'événement initiateur et les couches de protection. Les composants partagés entre la cause initiale et les couches de protection doivent également être déterminés. Modéliser le scénario d'accident avec les éléments identifiés dans un arbre d'événements associé.

- Construire le DFT équivalent en considérant la conséquence du scénario comme l'événement sommet se forme d'une porte PAND connecté à l'événement initiateur et à la défaillance du système de barrières (comptabilisé comme deux événements intermédiaires). Etablir la dépendance entre les couches et l'événement initiateur en utilisant des événements répétés et des portes statiques et dynamiques.

- Enlever les séquences de défaillance et calculer la fréquence exacte de l'accident. Afficher les résultats obtenus dans une feuille de travail récapitulative pour le scénario LOPA.

3.7.7 Résultats numériques

Le scénario du risque est documenté dans une feuille de calcul avec les couches de protection (non IPL) dans le Tableau 3.4. Les critères de tolérance au risque et la réduction de risque nécessaire ne sont pas abordés ici. La fréquence de l'événement initiateur (EI), les PFD pour chaque couche de protection (LA_2 et LA_3) et la PFD agrégée pour toutes les couches de protection (PLs) sont dérivées des portes statiques dans la Figure 3.8. La fréquence de la conséquence est fournie par l'approche analytique proposée.

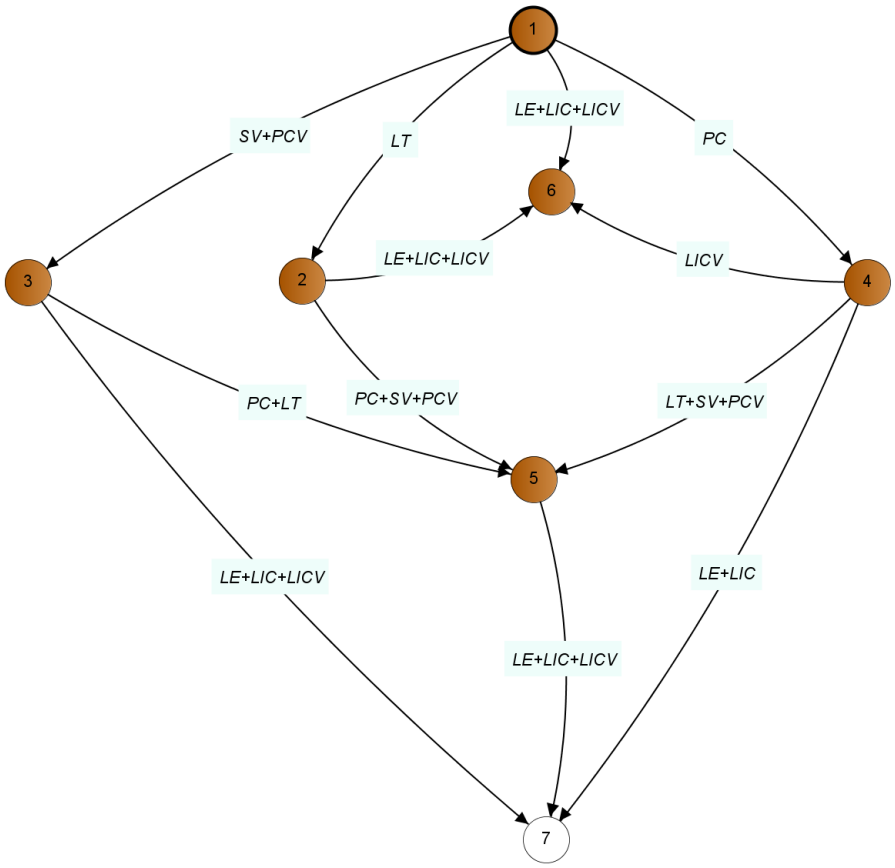

Figure 3.9 Modèle de Markov relatif à la défaillance du SBS [68]

Tableau 3.4 Feuille de calcul LOPA pour le scenario: Explosion de la chaudière à vapeur [68]

Scenario LOPA: Explosion de la chaudière à vapeur							
Evénement Initiateur (EI)				Couches de protection (PLs)			
Description	Fréquence (événement par heure)	Activation d'événements ou de conditions		Description	PFD	Agrégation des PFD pour les PLs	Fréquence de la conséquence (événement par heure)
		Description	Probabilité				
1. Défaillance de la régulation de l'eau (LA_1)	8.3E-6	N/A	1	LA_2: Défaillance de la coupure du carburant à cause d'un niveau bas de l'eau dans la chaudière	8.2E-2	2.6E-2	2.9E-7
				LA_3: Défaillance de la coupure du carburant à cause d'une augmentation de pression	3.9E-2		

Les résultats numériques obtenus à partir de l'approche proposée et du modèle markovien (Figure 3.9) concernant la probabilité et la fréquence de défaillance du SBS sont fournis dans le Tableau 3.5 (pour t = 8760 h). En outre, l'évolution de ces deux mesures en fonction du temps est illustrée dans la Figure 3.10. Il convient de noter que la fréquence de défaillance est obtenue à partir du modèle de Markov par la relation suivante :

$$fr_{(Défaillance\ du\ SBS)} = (E_3 + E_5) \cdot (\lambda_{LE} + \lambda_{LIC} + \lambda_{LICV}) + E_4 \cdot (\lambda_{LE} + \lambda_{LIV}) \quad (3.73)$$

Lorsque toutes les couches de protection et l'événement déclencheur (initiateur) sont supposés indépendants, la fréquence de défaillance du SBS est donnée comme suit :

$$fr_{(Défaillance\ du\ SBS)} = fr_{(EI)} \cdot PFD_{(LA_2)} \cdot PFD_{(LA_3)} \quad (3.74)$$

Lorsque l'événement déclencheur est supposé indépendant des couches de protection, la fréquence de défaillance du SBS peut être trouvée comme suit :

$$fr_{(Défaillance\ du\ SBS)} = fr_{(EI)} \cdot PFD_{(PL_s)} \quad (3.75)$$

Tableau 3.5 Probabilité et fréquence de défaillance du SBS [68]

Modèles	LOPA classique (voir l'équation (**3.75**))	Approche proposée	Modèle de Markov (Référence)
$fr_{(Défaillance\ du\ SBS)}$(h^{-1})	2.1526E-07	2.8782E-07	2.8782E-07
$Pr_{(Défaillance\ du\ SBS)}$	N/A	1.3021E-03	1.3021E-03

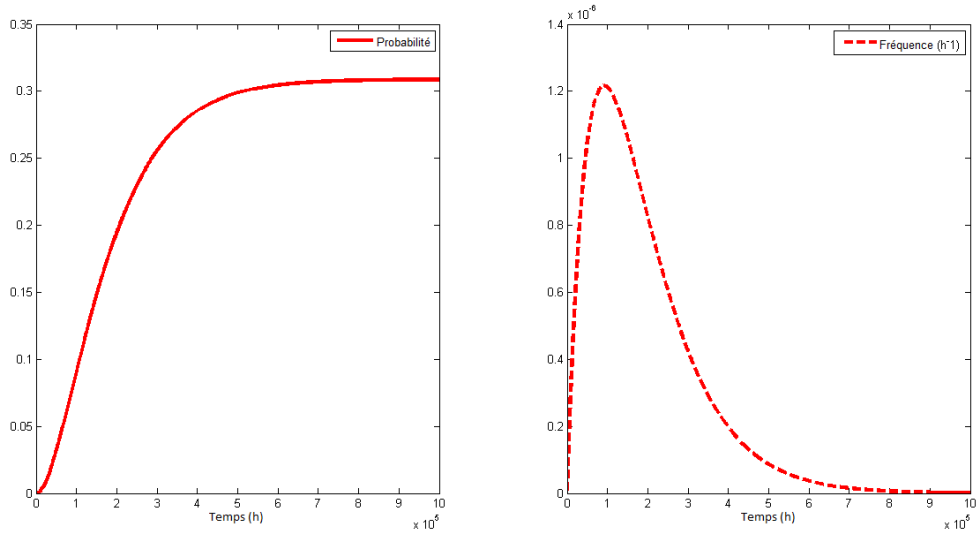

Figure 3.10 Variation de probabilité et fréquence de défaillance du SBS

L'inspection du Tableau 3.5 montre que les différents ensembles de résultats de l'approche proposée (probabilité et fréquence) sont en parfait accord avec les valeurs de référence. Les deux équations ci-dessus donnent des valeurs non conservatives en raison des dépendances existantes entre les PLs et EI, les paramètres $fr_{(EI)}$, $PFD_{(LA_2)}$, $PFD_{(LA_3)}$ et $PFD_{(PL_S)}$ peuvent être dérivés à partir des portes statiques du DFT (Figure 3.8).

Pour un calcul de fréquence précis, l'approche DFT proposée prend en compte les composants partagés et l'ordre d'occurrence des événements. L'utilisation de l'AdD classique n'est appropriée que dans le cas où il existe une stricte indépendance entre les parties constitutives de LOPA. Sinon, les hypothèses communes d'indépendance dans l'analyse LOPA donnent des résultats optimistes.

3.8 Conclusion

Une méthodologie complète a été développée dans ce chapitre afin de traiter les DFT en exprimant la probabilité et la fréquence de ses portes statiques et dynamiques, et donc de son événement sommet ES.

Premièrement, nous avons expliqués comment une forme canonique minimale peut être écrite en utilisant trois opérateurs (+, · et ◁). En basant sur la fonction de structure du DFT, le traitement qualitatif a été obtenu avec la détermination d'ensembles de coupes minimales et de séquences de défaillances disjonctives offrant les chemins possibles vers l'événement sommet. La deuxième contribution concerne le calcul de la fréquence de défaillance de toute DFT résultant de la détermination de séquences avant défaillance. Ensuite, la fréquence de défaillance de chaque porte dynamique a été détaillée. Il a été montré que leurs expressions correspondantes sont parfaitement conformes à celles obtenues par la conversion des expressions de probabilité associées en tenant compte de la distribution exponentielle des événements d'entrée. Enfin, nous avons illustré l'utilité de cette approche au moyen de deux exemples de travail concernant le calcul de probabilité et de fréquence. Afin de vérifier la validité et l'exactitude de la méthodologie proposée, les résultats obtenus ont été comparés à ceux dérivés par l'approche markovienne. Une similitude parfaite entre les deux ensembles de résultats a été obtenue.

L'approche proposée pourrait être considéré comme un prolongement de l'analyse qualitative et quantitative de tout DFT, permettant de déterminer les séquences de défaillance et de calculer la fréquence de défaillance à partir de la détermination de la fonction de structure de son événement sommet grâce au modèle algébrique approprié de toutes les portes dynamiques (PAND, FDEP, SEQ et SPARE), où toute distribution de défaillance pour les événements de base peut être envisagée.

En mappant les scénarios d'accident et les défaillances des systèmes dans un modèle DFT, l'approche proposée peut servir à calculer d'une part la probabilité et la fréquence de défaillance des systèmes liés à la sécurité (en particulier les SIS), qui présentent des interactions statiques et dynamiques entre leurs parties constitutives, et d'autre part, une fréquence précise des scénarios d'accident (en particulier des scénarios LOPA) sans supposer l'indépendance entre les couches de protection.

Chapitre 4

Réseaux Bayésiens Temporels Discontinus

4.1 Introduction

Le Réseau Bayésien est un outil probabiliste de raisonnement basé sur des relations de causalité qui factorise la distribution de probabilité jointe d'un ensemble de variables en prenant en compte les dépendances locales et réduisant de manière significative la complexité de modélisation du système et le temps de calcul [80].

Dans ce chapitre, le réseau bayésiens temporel discontinu est synthétisé [9,81]. L'expression "Les réseaux bayésiens temporels discontinus" est la traduction en anglais de l'appellation "The discrete-time bayesian networks (DTBN)" développée par Boudali et Dugan [9].

Du point de vue modélisation, le DTBN peut représenter les dépendances entre les composants avec la possibilité d'une évaluation temporelle continue du modèle. Du point de vue analyse, toute tâche imputable à évaluer la probabilité a posteriori peut être mise en œuvre, telle que le calcul de l'indisponibilité du système, les facteurs d'importance (sensibilité), la prédiction de l'état du système et le diagnostique.

4.2 Les réseaux bayésiens temporels discontinus

Ce formalisme a été conçu pour modéliser et analyser la fiabilité des systèmes dynamiques dont certains composants ou événements représentent des dépendances fonctionnelles et temporelles. L'idée est de faire translater les portes (statiques et dynamiques) de l'arbre de défaillances dynamique (DFT) en vu d'obtenir une représentation bayésienne spécifique par considérer :

- Chaque événement de base comme un nœud racine.

- Chaque porte comme un nœud intermédiaire représentant la fille seulement de deux nœuds parents.

1) Modélisation temporelle : Toutes les variables du réseau ont $(n+1)$ états, où les premiers n états sont les intervalles résultant de la discrétisation du temps de mission T et la variable prend sa valeur de probabilité de défaillance. L'état $(n+1)$ décrit la non-occurrence de l'événement (défaillance) au cours du temps pris.

2) La définition des tables de probabilité conditionnelle (TPC) : Il y a deux possibilités :

a) Evénement de base (EB) : La probabilité que A se produit à la $i^{ème}$ intervalle est :

$$Pr(A = i) = P\big((i-1)\Delta < t_A < i\Delta\big) = F_A(i\Delta) - F_A((i-1)\Delta) \quad (4.1)$$

$$P(A = n+1) = 1 - \sum_i F_A(i\Delta) \quad (4.2)$$

Où t_A est l'instant d'occurrence de l'événement A, F_A est la distribution cumulative de défaillance correspond à cet événement et Δ représente la durée de temps pris pour l'intervalle i. La TPC d'un événement de base A à l'aide de DTBN est donné par le Tableau 4.1.

Tableau 4.1 TPC générale pour un événement de base

$\boldsymbol{i}$	$]\mathbf{0}, \Delta]$	$]\mathbf{0}, \mathbf{2}\Delta]$	$\cdots$	$]\mathbf{0}, \boldsymbol{T} = \boldsymbol{n}\Delta]$	$]\boldsymbol{T}, \infty]$
$\boldsymbol{Pr(A = i)}$	P_1	P_2	$\cdots$	P_n	$1 - \sum P_i$

b) Evénement intermédiaire : Les tables de probabilité de ces événements sont déterminés selon la porte à la quelle l'événement intermédiaire représente [9,81].

4.2.1 Tables de probabilité conditionnelle : niveau de discrétisation $n = 2$

4.2.1.1 Cas des portes statiques

La table de probabilité pour la porte AND est donnée par le Tableau suivant :

Tableau 4.2 TPC pour la porte AND

A	$]0,\Delta]$			$]0,T]$			$]T,\infty]$		
B	$]0,\Delta]$	$]0,T]$	$]T,\infty]$	$]0,\Delta]$	$]0,T]$	$]T,\infty]$	$]0,\Delta]$	$]0,T]$	$]T,\infty]$
$Pr_{AND}(i =]0,\Delta])$	1	0	0	0	0	0	0	0	0
$Pr_{AND}(i =]0,T])$	0	1	0	1	1	0	0	0	0
$Pr_{AND}(i =]T,\infty])$	0	0	1	0	0	1	1	1	1

La table de probabilité pour la porte OR est donnée par le Tableau suivant :

Tableau 4.3 TPC pour la porte OR

A	$]0,\Delta]$			$]0,T]$			$]T,\infty]$		
B	$]0,\Delta]$	$]0,T]$	$]T,\infty]$	$]0,\Delta]$	$]0,T]$	$]T,\infty]$	$]0,\Delta]$	$]0,T]$	$]T,\infty]$
$Pr_{OR}(i =]0,\Delta])$	1	1	1	1	0	0	1	0	0
$Pr_{OR}(i =]0,T])$	0	0	0	0	1	1	0	1	0
$Pr_{OR}(i =]T,\infty])$	0	0	0	0	0	0	0	0	1

Pour le cas de la porte K parmi N (KooN), cette porte est considérée comme une combinaison de portes logiques AND et OR comme motionné dans la Figure 3.1.

4.2.1.2 Cas des portes dynamiques

La table de probabilité pour la porte PAND est donnée par le Tableau suivant :

Tableau 4.4 TPC pour la porte PAND

A	$]0,\Delta]$			$]0,T]$			$]T,\infty]$		
B	$]0,\Delta]$	$]0,T]$	$]T,\infty]$	$]0,\Delta]$	$]0,T]$	$]T,\infty]$	$]0,\Delta]$	$]0,T]$	$]T,\infty]$
$Pr_{PAND}(i=]0,\Delta])$	1	0	0	0	0	0	0	0	0
$Pr_{PAND}(i=]0,T])$	0	1	0	0	1	0	0	0	0
$Pr_{PAND}(i=]T,\infty])$	0	0	1	1	0	1	1	1	1

Pour la porte SEQ, la TPC correspondante à cette porte est donnée par le Tableau suivant :

Tableau 4.5 TPC pour la porte SEQ

A	$]0,\Delta]$			$]0,T]$			$]T,\infty]$		
B	$]0,\Delta]$	$]0,T]$	$]T,\infty]$	$]0,\Delta]$	$]0,T]$	$]T,\infty]$	$]0,\Delta]$	$]0,T]$	$]T,\infty]$
$Pr_{SEQ}(i=]0,\Delta])$	0	0	0	0	0	0	0	0	0
$Pr_{SEQ}(i=]0,T])$	0	1	0	0	0	0	0	0	0
$Pr_{SEQ}(i=]T,\infty])$	1	0	1	1	1	1	1	1	1

Pour la porte SPARE, la TPC de l'événement de secours B est donnée par le Tableau ci-après, où P_i et $P_{i\alpha}$ représentent la probabilité de défaillance de l'élément de secours en mode actif et en mode dormant pour la $i^{ème}$ intervalle respectivement.

Tableau 4.6 TPC pour l'événement de secours de la porte SPARE

A	$]0,\Delta]$	$]0,T]$	$]T,\infty]$
$Pr_B(i=]0,\Delta])$	Pr_1	$Pr_{1\alpha}$	0
$Pr_B(i=]0,T])$	Pr_2	Pr_2	0
$Pr_B(i=]T,\infty])$	$1-\sum Pr_i$	$1-\sum Pr_i-\sum Pr_{i\alpha}$	1

L'événement de secours et l'événement primaire dans la porte SPARE (WSP) sont connectés par une porte AND comme motionné dans la Figure 4.1.

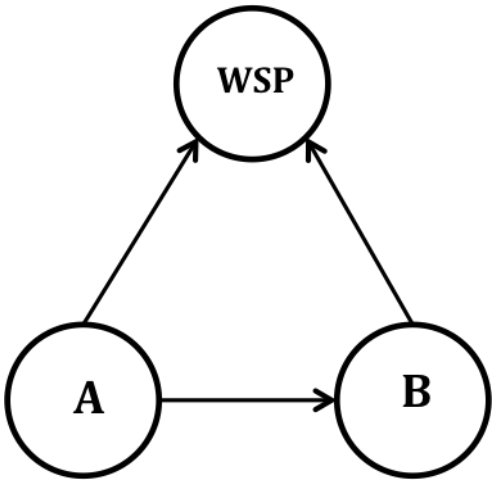

Figure 4.1 DTBN équivalent à la porte SPARE (WSP)

Pour le cas de la porte CSP, la TPC adoptée est la même pour la porte SEQ car les deux événements primaire et de secours ont une dépendance séquentielle entre eux avec des distributions de probabilité identiques.

4.2.2 Tables de probabilité : cas général

La généralisation des tables de probabilité conditionnelle est obtenue par l'élaboration des algorithmes typiques. Ces algorithmes doivent être capables de générer n'importe quelle table de probabilité en fonction d'un niveau de discrétisation (Nombre des états) choisi. Etant donné que ces algorithmes sont rédigés se forme des programmes en MATLAB [82].

Dans le cas des deux portes AND et OR le même programme source est utilisé pour générer les tables de probabilité correspondantes (voir Figure 4.2). La réalisation de ce code donne des tableaux composés de zéros et uns sous MATLAB.

```
% choix du niveau de discrétisation
n;
n=n+1;

% le programme
i=1:n^2;
j=1:n;
OR(i,j)=zeros;
for j=1:n;
  for i=n*(j-1)+j:(n*j);
OR(i,j)=ones;
  end
  for k=j:(n-1);
    for i=n*k+j;
    OR(i,j)=ones;
    end
  end
end

% résultats
OR
AND=rot90(rot90(OR))
```

Figure 4.2 Programme source sous MATLAB relatif aux portes AND et OR

Le programme source dans la Figure 4.2 est divisé en trois parties : la première concerne la définition du niveau de discrétisation, la seconde représente l'ensemble des instructions à exécuter par l'ordinateur (en langage MATLAB) et la troisième partie décrit les résultats finaux à afficher (les TPC).

Pour le cas des portes dynamiques PAND et SEQ, les programmes sources correspondants sont représentés dans les Figures 4. 3 et 4.4 respectivement. La formulation des deux programmes est semblable au cas du programme source des portes statiques (AND et OR).

```
% choix du niveau de discrétisation
n;
n=n+1;

% le programme
PAND(i,j)=zeros;
for j=1:n;
   for i=n*(j-1)+j+1:(n*j);
        PAND(i,n)=ones;
   end
   for k=1:j;
     for i=(n*(k-1)+1):(n*(k-1)+k);
PAND(i,k)=ones;
     end
   end
end

% résutats
PAND
```

Figure 4.3 Programme source sous MATLAB relatif à la porte PAND

```
% choix du niveau de discrétisation
n;
n=n+1;

% le programme
SEQ(i,j)=zeros;
for j=1:n;
   for i=n*(j-1)+j:(n*j);
      SEQ(i,n)=ones;
   end
end
for j=2:n;
   for k=(j-1):(n-1);
     for i=(n*k+1):(n*k+k);
SEQ(i,k+1)=ones;
     end
   end
end

% résutats
SEQ
```

Figure 4.4 Programme source sous MATLAB relatif à la porte SEQ

Il nous reste que définir la TPC générale qui correspond à la porte WSP. Le programme source relatif à cette porte est représenté dans la Figure 4.5.

```
% temps de mission, lambda et alpha*lambda
T;
lambda1;
lambda2;

% n est le niveau de discrétisation n=(T/delta)
delta;
n= T/delta;

% programme
i=1:n;
Q=lambda1*delta;
w=lambda2*delta;
a(i)=exp(-Q*(i-1))-exp(-Q*i);
for i=1:n
  for j=1:n
i;
j;
    if i>=j
seq(i,j)=exp(-w*(i-1))-exp(-w*i);
    else
    seq(i,j)=exp(-(w/2)*(i-1))-exp((-w/2)*i);
    end
  end
end
s=sum(seq);
P=sum(s.*a)
seq(n+1,:)=1-s;
seq(end,n+1)=1;

% résultats
WARM=(flipud(rot90(seq)))
```

Figure 4.5 Programme source sous MATLAB relatif à la porte WSP

La formulation du programme relatif à la porte WSP est différent à ceux relatifs aux portes (AND, OR, PAND et SEQ) car la TPC résultant est fonction des probabilités de défaillance de l'élément de secours en mode actif et en mode dormant. En plus de la détermination du niveau de discrétisation, il est intéressant de définir les paramètres de distribution pour l'événement de secours (temps de mission, lambda en mode actif et lambda en mode dormant).

4.2.3 Algorithme général de construction du DTBN

La construction du modèle bayésien DTBN se fait à l'aide de la boite à outils (BNT toolbox de MATLAB) [83]. L'algorithme de base pour créer un DTBN est représenté dans la Figure 4.6.

```
Début

  Définir le chemin de la boite à outils
  Mettre les données nécessaires aux composants
  Établir les TPC des noeuds
  Décrire le nombre de noeuds
  Numéroter des noeuds
  Définir des arcs
  Affecter des TPC aux noeuds
  Construire le Graphe
  Calculer les probabilités marginales
  Calculer la probabilité du chemin le plus probable
  Établir le calcul de diagnostique
  Établir le calcul de requête
  Calculer les facteurs d'importance

Fin
```

Figure 4.6 Pseudo-code pour un DTBN général

Le Pseudo-code de la figure précédente décrit l'ensemble des étapes nécessaires pour l'élaboration d'un programme DTBN sous MATLAB. Pour conclure, la création de n'importe quel DTBN est effectué en procédant les étapes suivantes :

4.2.3.1 Mettre les données nécessaires du modèle bayésien

- Définir le dossier apportant la boite à outils (BNT toolbox) dans l'ordinateur.

- Décrire les taux de défaillance et de réparation des composants, le temps de mission, le niveau de discrétisation et le nombre d'intervalles.

- Etablir les TPC des nœuds parents.

- Etablir les TPC des nœuds fils (les TPC relatives aux portes statiques et dynamiques). On fait appelle à ces tables depuis un programme séparé (voir Figures 4.2-4.5).

4.2.3.2 Dérouler les instructions relatives à la boite à outils

- Décrire le nombre total des nœuds.

- Numéroter les nœuds.

- Relier les nœuds entre eux avec des arcs.

- Etablir les tailles des nœuds, identifier la nature discrète des nœuds et définir le modèle graphique.

- Affecter les TPC aux nœuds.

4.2.3.3 Afficher les résultats

- Construire le Graphe (les nœuds du graphe s'affichent des numéros à l'intérieur).

- Calculer les probabilités marginales pour le système et les sous systèmes.

- Calculer la probabilité du chemin le plus probable dans le réseau bayésien.

- Calculer la probabilité d'échec ou de succès d'un composant en connaissant l'instant de défaillance du système (Diagnostique).

- Calculer la probabilité de défaillance du système sachant la défaillance ou le succès d'un ou plusieurs composants (Requête).

- Calculer les facteurs d'importance pour les composants.

4.3 Calcul de probabilités a postériori avec les DTBN

Le but principal d'utiliser les réseaux bayésiens dans les études de fiabilité, n'est pas seulement de calculer l'indisponibilité des systèmes, ou de prendre en compte certaines dépendances entre les composants, mais aussi de calculer les probabilités a postériori étant donné un ensemble d'événements observés. Pour implémenter notre démarche bayésienne (DTBN) et voir leur intérêt en terme des paramètres à calculer et de prise en compte des

dépendances fonctionnelles et séquentielles, nous considérons le système HSS [54,84] présenté par la Figure 3.2. La Figure 4.7 représente le graphe bayésien modélisant la défaillance du système et convertissant la DFT de la Figure 3.3.

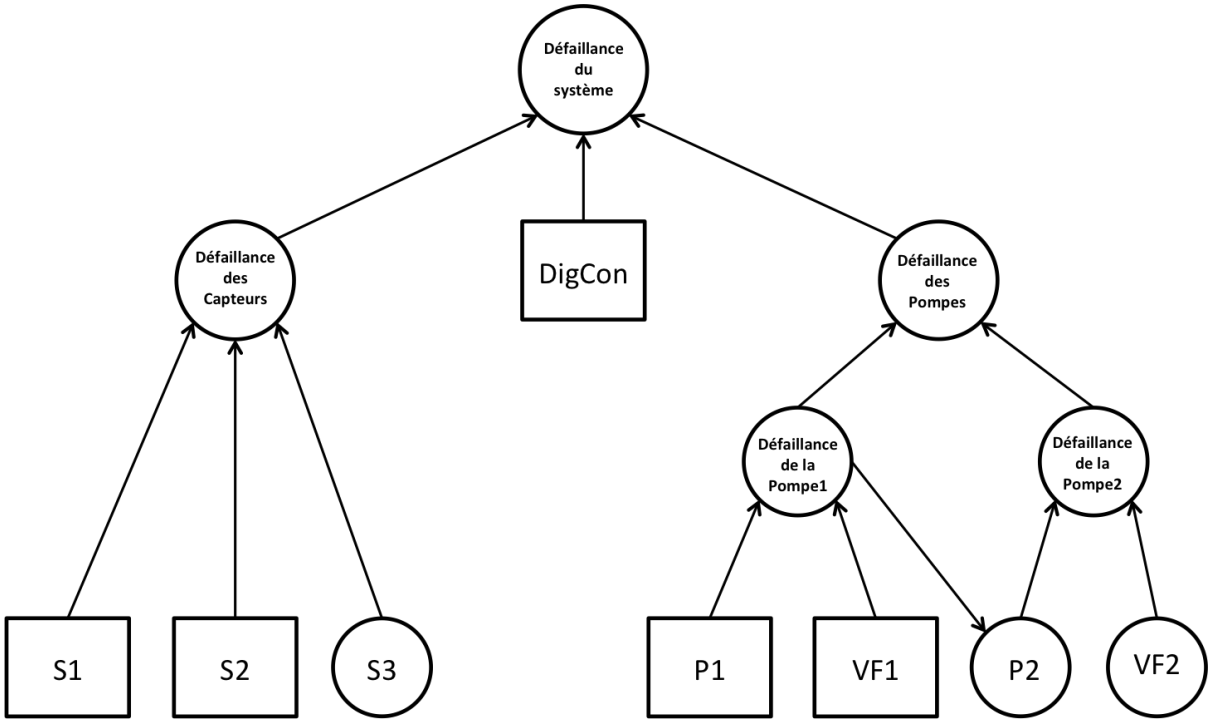

Figure 4.7 Modèle bayésien représentant la défaillance du HSS

Le programme source utilisé pour modéliser la défaillance du système HSS est représenté dans l'Annexe D.1. L'hors de l'exécution du programme le graphe de la Figure 4.8 est apparu. Les calculs abordés dans cette section par le programme DTBN sont comparés avec les résultats trouvés par les (GCTBN : Generalized Continuous Time Bayesian Network) qui est un formalisme bayésien spécifique basé sur un processus stochastique [62,85].

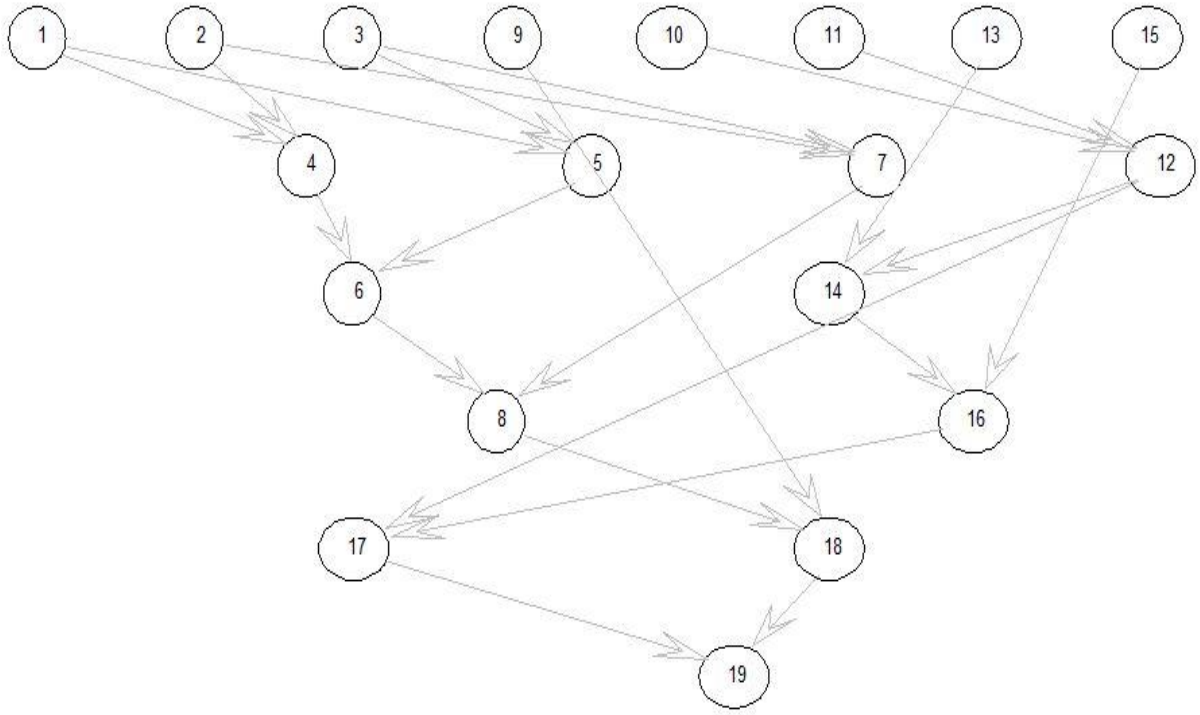

Figure 4.8 Modèle bayésien représentant la défaillance du HSS affiché par DTBN

4.3.1 Calcul de fiabilité et disponibilité

Il est essentiel de noter que les événements représentés par des rectangles sont subis aux opérations de maintenance (cas d'indisponibilité) avec $\mu = 0.01h^{-1}$ et que le niveau de discrétisation $N = 10$ et le temps de mission $T = 1000$. Le Tableau 4.9 représente les valeurs trouvées par la boite à outils BNT toolbox de MATLAB [83], en les comparant aux résultats dans [54].

Tableau 4.7 Dé-fiabilité et Indisponibilité par DTBN

T=1000 N=10	Dé-fiabilité		Indisponibilité	
	DTBN	Réf [54]	DTBN	Réf [54]
Système	0.02653	0.02653	0.00208	0.00204
Capteurs	0.02544	0.02544	0.00196	0.00193
Pompes	1.14E-4	1.14E-4	1.18E-5	1.1E-5

4.3.2 Requête dans un DTBN

Une requête est l'inférence de probabilités $P(X/e)$. Où e est l'ensemble des variables observées ou non, et X est l'ensemble des variables pour les quelles on fait une requête. Supposant que les deux composants S_1 et S_2 sont subis à un test régulier, des observations tirées au cours du temps comme suit : $\sigma_1 = \{\bar{S}_2^{100}, \bar{S}_3^{200}, \bar{S}_2^{300}, \bar{S}_3^{400}, S_2^{500}, S_3^{600}\}$, où $\bar{S}_i^t$ et S_i^t représentent le fonctionnement et la défaillance du composant S_i sur un instant t respectivement. Le Tableau 4.8 décrit les valeurs $P(Défaillance\ du\ système/\sigma_1)$.

Tableau 4.8 Dé-fiabilité du Système Conditionnée en σ_1

N=10	DTBN	Réf [54]
T=200 h	4.01E-4	4.02E-4
T=400 h	8.8E-4	8.08E-4
T=500 h	0.0587	0.05873
T=600 à 1000 h	1	1.000

D'après le Tableau 4.8, les résultats obtenus par notre modèle (DTBN) sont similaires à ceux trouvés par le modèle GCTBN équivalent, seulement pour $T = 400h$ la valeur obtenue est à cause du choix de niveau de discrétisation $N = 10$, donc $\bar{S}_2^{300}$ revient $\bar{S}_2^{320}$. Pour éviter ce type de suppositions, nous recommandons que le choix des dates de testes périodiques doit respecter le niveau de discrétisation.

4.3.3 Diagnostique

Une autre possibilité que les DTBN offrent est le diagnostique, comme pour la requête, une série d'observations sur le système est considérée : $\sigma_2 = \{\overline{Défaillance\ du\ système}^{400}, Défaillance\ du\ système^{600}\}$, où les éléments de l'ensemble représentent le système en fonctionnement à $t = 400h$ et en panne à $t = 600h$ respectivement. Le Tableau 4.9 reprend les valeurs des S_1 et VF_1 conditionnées en σ_2.

Tableau 4.9 Dé-fiabilité des Composants Conditionnée en σ_2

N=10	S_1		VF_1	
	DTBN	Réf [54]	DTBN	Réf [54]
T=500 h	0.04594	0.04595	0.00497	0.00497
T=1000 h	0.6592	0.6589	0.0137	0.0136

Ces résultats prouvent que le DTBN est un outil parfait de diagnostique.

4.3.4 Calcul d'importance

Abordons maintenant le calcul du facteur d'importance marginal (MIF) [86]. Le Tableau 4.10 représente les valeurs MIF pour les composants S_1 et VF_1 avec comparaison.

Tableau 4.10 Facteurs d'Importance des Composants

T=1000	MIF	
N=10	DTBN	Réf [54]
S_1	0.17202	0.17205
VF_1	0.01011	0.01018

4.4 Evaluation des scénarios d'accident à l'aide des DTBN

On revient à l'exemple SBS du 3ème chapitre (voir Figure 3.6), le scénario d'accident tiré de ce système est représenté par l'arbre d'événements dans la Figure 3.7. L'exécution du programme source représentant le modèle bayésien DTBN décrit dans l'Annexe D.2 affiche le graphe de la Figure 4.9. Ce modèle est consacré à l'évaluation de la probabilité de survenance du scénario d'accident et des barrières de sécurité. Les résultats obtenus sont rassemblés dans le Tableau 4.11 et comparés à ceux trouvés dans le chapitre précédent.

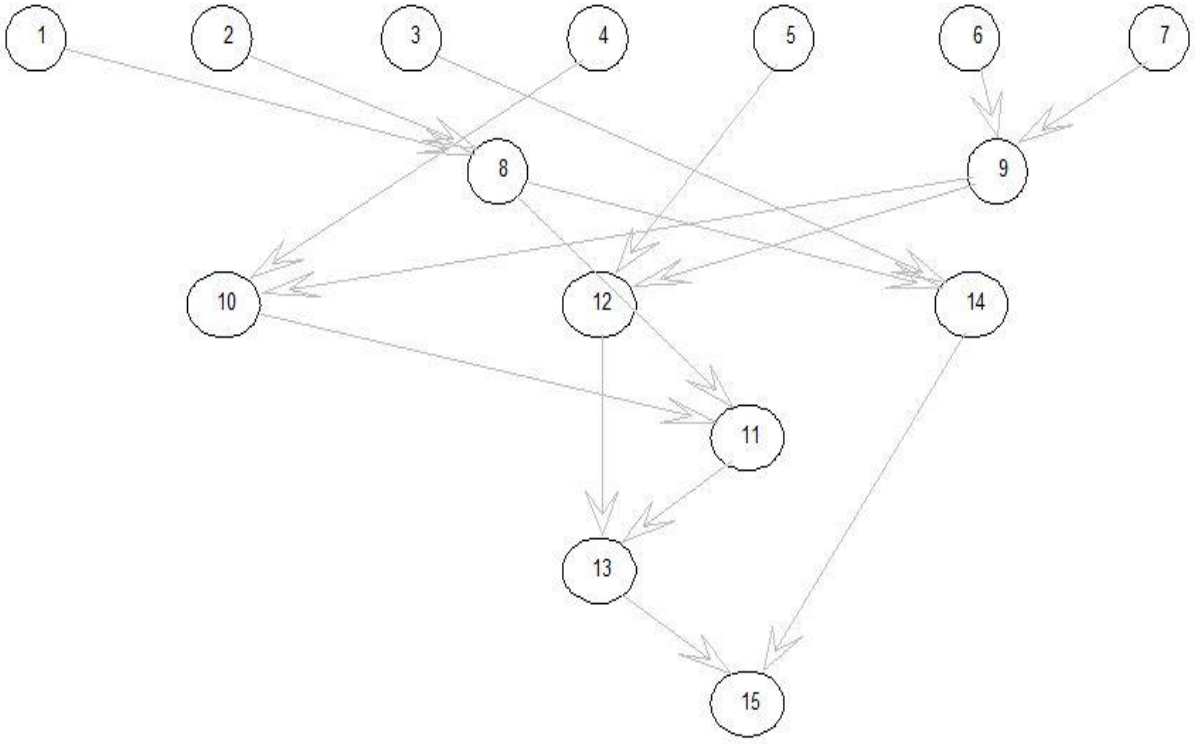

Figure 4.9 Modèle bayésien représentant la défaillance du SBS affiché par DTBN

Tableau 4.11 Probabilités pour le scénario d'accident et ses barrières obtenues par DTBN

Modèles	PFD (LA2)	PFD (LA3)	PFD (PLs)	$Pr_{(Défaillance\ du\ SBS)}$
DTBN (N=10)	8.2266E-02	3.8653E-02	2.5880E-02	1.4339E-03
DTBN (N=20)	8.2266E-02	3.8653E-02	2.5880E-02	1.3679E-03
AdD simple	8.2266E-02	3.8653E-02	2.5880E-02	N/A
Tableau 3.5	N/A	N/A	N/A	1.3021E-03

Les résultats exposés dans le Tableau 4.11 montrent les paramètres du scénario d'accident calculés en exécutant le programme DTBN équivalent (voir Annexe D.2) et en les comparant avec des valeurs de référence obtenues à l'aide d'un AdD simple ou à partir de la démarche analytique présentée dans le Chapitre 3.

Le modèle DTBN montre des résultats en parfaite adéquation avec les résultats obtenus à l'aide d'un arbre de défaillance simple (sans considérer le caractère dynamique). Pour la

probabilité d'occurrence du scénario (explosion de la chaudière à vapeur) équivalent à l'événement (défaillance du SBS), le modèle bayésien donne différentes valeurs pour deux niveaux de discrétisation (N=10 et N=20). Lorsqu'on augmente le nombre d'intervalles (niveau de discrétisation), la valeur de probabilité approche de la valeur exacte ou de référence. Donc, le modèle bayésien DTBN donne des valeurs de probabilités approchées aux cas de l'existence des dépendances dynamiques (l'événement initiateur connecté avec l'ensemble des barrières par une relation PAND (voir Figure 3.8)). Il est nécessaire de noter que l'augmentation excessive du niveau de discrétisation N cause un problème de mémoire insuffisante au sein du programme MATLAB.

4.5 Evaluation des PDF et PFH en considérant les défaillances détectées et non-détectées

Dans cette section, nous développons le modèle bayésien DTBN permettant d'évaluer les indicateurs du SIS sur ses deux modes de fonctionnement (PFDmoy en faible demande et PFH en demande élevée ou continue) en incluant les défaillances dangereuses détectées et non détectées. La norme CEI 61508 distingue les défaillances dangereuses des défaillances sécurisées. Ces dernières sont en dehors de notre objectif. La défaillance dangereuse (D) pour un composant du SIS est divisée en deux catégories : défaillance détectée (DD) et défaillance non détectée (DND). La restauration de la défaillance détectée est caractérisée par un taux de réparation μ. La défaillance non détectée peut être révélée pendant un test de preuve (TP) qui est effectue chaque une période de temps. Un autre type de tests : les tests de course partielle (TCP), s'il sont considérés, les défaillances non détectées sont révélées durant le TCP et les défaillances qui n'ont pas encore détectées restent cachées jusqu'au prochain test de preuve (TP) [87]. La Figure 4.10 représente le modèle markovien pour un composant sujet des défaillances détectées et non détectées en considérant que le TP est parfait et les révélations sont effectuées instantanément.

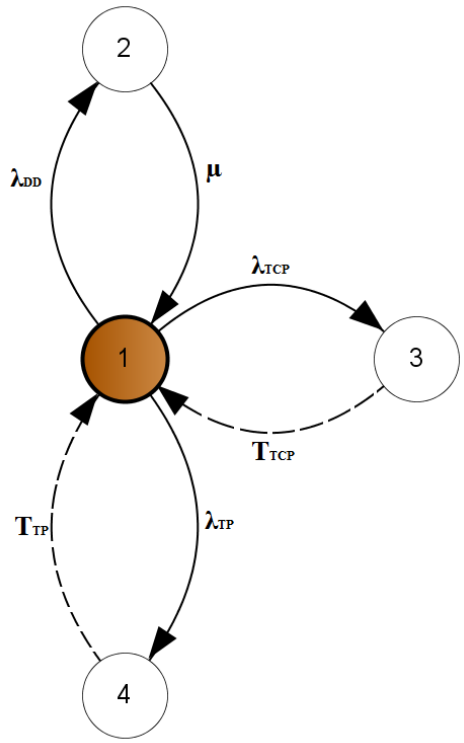

Figure 4.10 modèle de Markov pour un composant sujet à des DD et DND

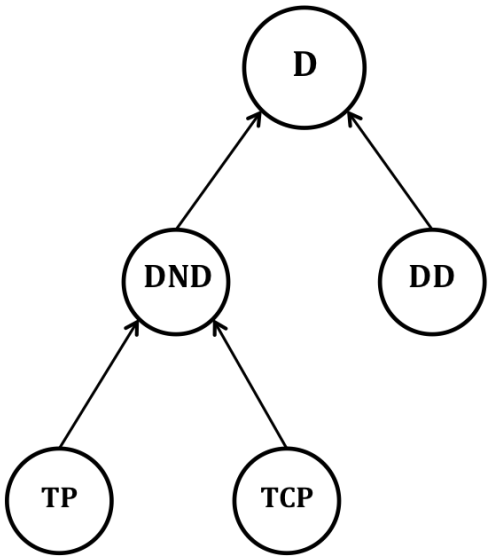

Figure 4.11 Modèle bayésien représentant le mécanisme de la défaillance dangereuse

Le modèle bayésien équivalent est donné par la Figure 4.11 ci dessus. D'après le graphe markovien de la Figure 4.10, la défaillance dangereuse se produit par au moins une des trois branches indiquées par les taux de défaillance λ_{DD}, λ_{TCP} et λ_{TP}. Afin de modéliser le modèle DTBN équivalent, nous adoptons les données suivantes : $\lambda_{DD} = 5 \cdot 10^{-3}$, $\mu = 0.125$ et $\lambda_{TCP} = \lambda_{TP} = 2 \cdot 10^{-4}$. Les durées des tests périodiques sont choisies de deux mois et six mois pour TCP et TP respectivement. Le programme source décrivant le modèle DTBN avec un temps de mission d'une année et un niveau de discrétisation N=10 est figuré dans l'Annexe D.3. Les distributions de probabilités relatives aux nœuds racines (Figure 4.11) sont données comme suit :

$$P_{DD} = \frac{\lambda_{DD}}{\lambda_{DD} + \mu} \cdot \left[1 - e^{-(\lambda_{DD}+\mu).t}\right] \tag{4.3}$$

$$P_{TCP} = 1 - e^{-\lambda_{TCP}.\left[t - E(\frac{t}{TCP}).TCP\right]} \tag{4.4}$$

$$P_{TP} = 1 - e^{-\lambda_{TP}.\left[t - E(\frac{t}{TP}).TP\right]} \tag{4.5}$$

Le calcul de la valeur PFD renvoie au calcul de probabilité de défaillance dangereuse effectué directement par le programme DTBN. Pour la PFH, le calcul se fait via l'obtention de la fréquence de défaillance dangereuse à l'aide de la formule suivante :

$$fr_D = (1 - P_D) \cdot (\lambda_{DD} + \lambda_{TCP} + \lambda_{TP}) \tag{4.6}$$

Où : P_D est la probabilité de défaillance dangereuse et $(1 - P_D)$ décrit la disponibilité du composant soumis seulement à des défaillances dangereuses.

Le calcul des valeurs moyennes (PFDmoy et PFHmoy) se fait numériquement en calculant des valeurs instantanées suffisantes tout au long du temps de mission. La Figure 4.12 représente les variations de PFD et PFH au cours de temps.

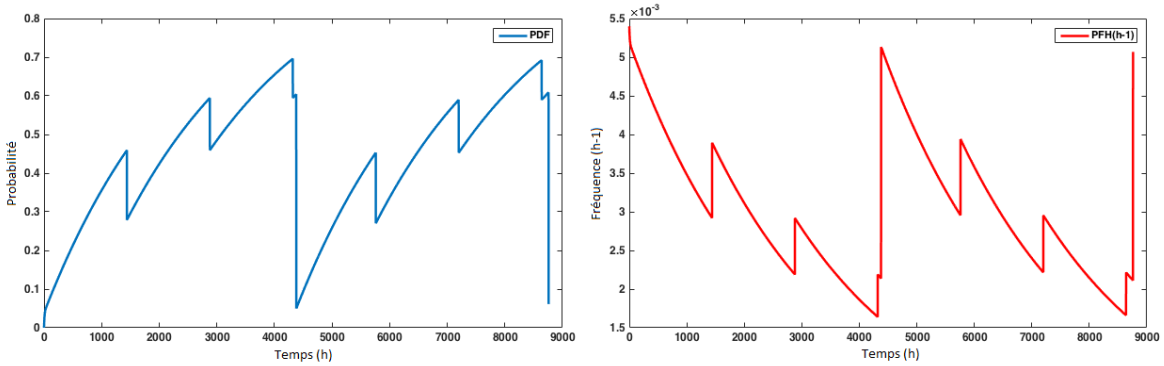

Figure 4.12 Variation de PFD et PFH au cours de temps

4.6 Conclusion

Nous avons développés dans ce chapitre les réseaux bayésiens temporels discontinus (DTBN) pour l'évaluation de la fiabilité des systèmes dynamiques. Dans un premier temps, nous avons discutés l'utilité de cette approche sur deux points : l'exactitude des résultats obtenus et le pouvoir d'effectuer des inférences bayésiennes en termes de probabilités a postériori telles que le diagnostique, la requête et le calcul d'importance. Deuxièmement, les DTBN sont testés sur l'évaluation des probabilités des scénarios d'accident et les PFD des barrières misent en jeux. A la fin, les DTBN sont utilisés pour modéliser la distribution probabiliste des composants sujet à des défaillances détectées et non-détectées.

La prise en compte des deux dimensions de probabilité et de fréquence, des dépendances fonctionnelles et séquentielles et les tests périodiques appliqués sur les composants des SIS rend ce formalisme bayésien puissant pour résoudre les DFT, déterminer les niveaux SIL des systèmes relatifs à la sécurité et particulièrement les SIS et évaluer la performance des barrières de sécurité pour atténuer les effets des scénarios d'accident. Le DTBN peut aussi modéliser les défaillances dangereuses détectées et non détectées des composants du SIS testés périodiquement en vu d'extraire les valeurs de PFD et PFH correspondantes.

Conclusions générales et recommandations

Après avoir choisi d'enclore chaque chapitre de cette thèse avec une conclusion spécifique, nous n'avons qu'en souligner les grands lignes pour offrir une conclusion générale.

Rappelons tout d'abord que, le problème d'intégration des dépendances fonctionnelles et séquentielles et des contraintes dans les lieux réels d'exploitation reste au cœur des préoccupations des analystes des risques et de sécurité. Réduire un risque à un niveau acceptable ou tolérable, en utilisant plusieurs barrières de sécurité, nécessite d'évaluer l'efficacité de ces barrières. Les normes CEI 61508 et CEI 61511, qui traitent la sécurité fonctionnelle des systèmes relatifs à la sécurité se basent sur le concept de niveau d'intégrité de sécurité (SIL) qui spécifie les exigences de la fonction de sécurité implémentée au niveau du système instrumenté de sécurité (SIS). La quantification de ces exigences traduit la probabilité moyenne de défaillance à la demande (PFDmoy) pour un SIS fonctionnant en mode faible demande, et la probabilité de défaillance dangereuse par heure (PFH) pour un SIS fonctionnant en en mode forte demande.

Le premier objectif de ce travail doctoral était de développer une démarche compréhensive pour le traitement des DFT. Ce modèle a la capacité d'évaluer les performances des systèmes relatifs à la sécurité, de calculer la fréquence des scénarios LOPA avec la considération de toute dépendance entre les événements de base représentant les composants des systèmes à analyser ou bien les éléments des scénarios étudiés. La vérification de l'exactitude de notre approche a été effectue grâce à une comparaison avec les résultats obtenus à l'aide des modèles markoviens correspondants.

La deuxième contribution de ce travail a montré l'application des réseaux bayésiens temporels discontinus (DTBN) pour l'évaluation des performances probabilistes des systèmes

relatifs à la sécurité, l'analyse des scénarios d'accidents et la modélisation des composants du SIS périodiquement testés. Le DTBN pourrait également être utilisé comme un outil inductif pour analyser les défaillances du système à la lumière des nouvelles observations. On peut conclure que l'utilisation des réseaux bayésiens dynamiques, particulièrement les DTBN, dans le calcul du risque évite non seulement des problèmes tels que représentent les méthodes usuelles comme les chaines de Markov, les méthodes algébriques, ou celles à base stochastique, mais permet également à l'analyste d'évaluer la probabilité a postériori.

Nous espérons que notre contribution doctorale ait un meilleur entendement et que les deux modèles présentés aux Chapitres 3 et 4 résolvant les DFT s'avèrent utile. Dans un travail futur, nous essayerons d'aller au-delà de ce que nous avons entrepris surtout en ce qui concerne l'intégration des contraintes supplémentaires caractérisant des conditions réelles d'exploitation dans les analyses de fiabilité et sécurité telles que les politiques de maintenance et les défaillances de cause commune.

Annexe A

Fréquences de défaillance pour des portes dynamiques

La fréquence de défaillance de chaque porte dynamique est développée pour obtenir les expressions de fréquence données dans la section 3.4 en fonction de la formule suivante:

$$fr([A,B]) = Pr\left([A,\overline{B}]\right) \cdot \lambda_B$$

A.1 Fréquence de défaillance pour la porte PAND (Figure 2.1a)

La sortie de la porte PAND est vraie si les deux événements A et B se sont produits, et A s'est produit avant B.

$$\begin{aligned} fr(PAND) &= \lambda_B \cdot \left(1 - F_B(t)\right) \cdot \int_0^t \lambda_A e^{-\lambda_A \tau_A}\, d\tau_A \\ &= \lambda_B \cdot e^{-\lambda_B t} \cdot \left(1 - e^{-\lambda_A t}\right) \\ &= \lambda_B \cdot \overline{b} \cdot a \end{aligned}$$

A.2 Fréquence de défaillance pour la porte Spare (Figure 2.1c)

Cette porte modélise la présence d'un composant principal et d'un composant de secours (initialement à l'état dormant (veille)). Lorsque le composant principal tombe en panne, le composant de secours passe de l'état inactif à l'état de fonctionnement.

La fréquence de défaillance de cette porte est obtenue en faisant la somme des fréquences des deux séquences disjonctives:

$$fr(Spare) = Pr\left([B_d,\overline{A}]\right) \cdot \lambda_A + Pr\left([A,\overline{B_a}]\right) \cdot \lambda_B$$

$$\text{Où : } \begin{cases} fr([B_d,A]) = Pr\left([B_d,\overline{A}]\right) \cdot \lambda_A \\ fr([A,B_a]) = Pr\left([A,\overline{B_a}]\right) \cdot \lambda_B \end{cases}$$

$$\Leftrightarrow \begin{cases} fr([B_d, A]) = \lambda_A \cdot \left(1 - \int_0^t \lambda_A e^{-\lambda_A t_A}\, dt_A\right) \cdot \left(\int_0^t f_{B_d}(t_B)\, dt_B\right) \\ fr([A, B_a]) = \lambda_B \cdot \left(e^{-\alpha\, \lambda_B t_A} - \int_{t_A}^t \lambda_B e^{-\lambda_B (t_B - (1-\alpha) t_A)}\, dt_B\right) \cdot \int_0^t f_A(t_A) dt_A \end{cases}$$

$$\Leftrightarrow \begin{cases} fr([B_d, A]) = \lambda_A \cdot e^{-\lambda_A t} \cdot \left(\int_0^t \alpha\, \lambda_B e^{-\alpha\, \lambda_B t_B}\, dt_B\right) \\ fr([A, B_a]) = \lambda_B \cdot e^{-\lambda_B (t - (1-\alpha) t_A)} \cdot \left(\int_0^t \lambda_A e^{-\lambda_A t_A} dt_A\right) \end{cases}$$

Après quelques réarrangements, nous obtenons:

$$\Leftrightarrow \begin{cases} fr([B_d, A]) = \lambda_A \cdot e^{-\lambda_A t}\left(1 - e^{-\alpha\, \lambda_B t}\right) \\ fr([A, B_a]) = \lambda_B \cdot e^{-\lambda_B t} \cdot \frac{\lambda_A}{\lambda_A - (1-\alpha)\lambda_B}\left(1 - e^{-\lambda_A t} \cdot e^{(1-\alpha)\lambda_B t}\right) \end{cases}$$

Par conséquent, il en résulte:

$$\begin{aligned} fr(Spare) &= \lambda_A \cdot e^{-\lambda_A t}\left(1 - e^{-\alpha\, \lambda_B t}\right) + \lambda_B \cdot e^{-\lambda_B t} \cdot \frac{\lambda_A}{\lambda_A - (1-\alpha)\lambda_B}\left(1 - e^{-\lambda_A t} \cdot e^{(1-\alpha)\lambda_B t}\right) \\ &= \lambda_A \cdot \left(e^{-\lambda_A t} - e^{-\lambda_A t} \cdot e^{-\alpha\, \lambda_B t}\right) + \frac{\lambda_A \cdot \lambda_B}{\lambda_A - (1-\alpha)\lambda_B}\left(e^{-\lambda_B t} - e^{-\lambda_A t} \cdot e^{-\alpha \lambda_B t}\right) \\ &= \lambda_A \cdot \left(\overline{a} - \overline{a} \cdot \overline{b_\alpha}\right) + \frac{\lambda_A \cdot \lambda_B}{\lambda_A - (1-\alpha)\lambda_B}\left(\overline{b} - \overline{a} \cdot \overline{b_\alpha}\right), \text{pour } \lambda_B \neq \tfrac{\lambda_A}{1-\alpha} \end{aligned}$$

A.3 Fréquence de défaillance pour la porte SEQ (Figure 2.1d)

Pour cette porte, les événements d'entrée sont forcés de se produire dans un ordre spécifique (de gauche à droite). L'événement de sortie se produit lorsque le dernier événement d'entrée se produit.

$$\begin{aligned} fr(SEQ) &= \lambda_B \cdot \left(1 - \int_{t_A}^t \lambda_B e^{-\lambda_B (t_B - t_A)}\, dt_B\right) \cdot \int_0^t \lambda_A e^{-\lambda_A t_A}\, dt_A \\ &= \lambda_B \cdot e^{-\lambda_B (t - t_A)} \cdot \int_0^t \lambda_A e^{-\lambda_A t_A}\, dt_A = \lambda_B \cdot \lambda_A \cdot e^{-\lambda_B t} \cdot \int_0^t e^{-(\lambda_A - \lambda_B) t_A}\, dt_A \\ &= \frac{\lambda_A \cdot \lambda_B}{\lambda_A - \lambda_B} \cdot \left(e^{-\lambda_B t} - e^{-\lambda_A t}\right) \\ &= \frac{\lambda_A \cdot \lambda_B}{\lambda_A - \lambda_B} \cdot \left(\overline{b} - \overline{a}\right), \text{pour } \lambda_A \neq \lambda_B \end{aligned}$$

Annexe B

Expressions de probabilité pour les portes dynamiques

Les expressions de probabilité introduites dans la sous-section 3.5.3 pour chaque porte dynamique permettront de fournir les fréquences de défaillance correspondantes.

B.1 Expression de probabilité pour la Porte PAND

$$Pr(PAND) = \int_0^t \left(\int_0^{\tau_B} \lambda_A e^{-\lambda_A \tau_A}\, d\tau_A\right) \lambda_B e^{-\lambda_B \tau_B} d\tau_B$$
$$= \int_0^t \left(1 - e^{-\lambda_A \tau_B}\right) \lambda_B e^{-\lambda_B \tau_B} d\tau_B$$
$$= \int_0^t \lambda_B e^{-\lambda_B \tau_B} d\tau_B - \int_0^t \lambda_B e^{-(\lambda_A+\lambda_B)\tau_B} d\tau_B$$
$$= \left(1 - e^{-\lambda_B t}\right) - \frac{\lambda_B}{\lambda_A+\lambda_B}\left(1 - e^{-(\lambda_A+\lambda_B)t}\right)$$

L'expression de probabilité se trouve comme suit:

$$Pr(PAND) = b - \frac{\lambda_B}{\lambda_A+\lambda_B}\left(1 - \overline{a}\cdot\overline{b}\right)$$
$$= b - \frac{\lambda_B}{\lambda_A+\lambda_B}\left(a + \overline{a} - \overline{a}\cdot\overline{b}\right)$$
$$= b - \frac{\lambda_B}{\lambda_A+\lambda_B}\left(a + \overline{a}\cdot b\right)$$

B.2 Expression de probabilité pour la Porte Spare

$$Pr(Spare) = Pr([B_d, A]) + Pr([A, B_a])$$
$$\begin{cases} Pr([B_d, A]) = \int_0^t \left(\int_0^{t_A} f_{B_d}(t_B)\, dt_B\right) f_A(t_A) dt_A \\ Pr([A, B_a]) = \int_0^t \left(\int_{t_A}^t f_{B_a}(t_B, t_A)\, dt_B\right) f_A(t_A) dt_A \end{cases}$$
$$\Leftrightarrow \begin{cases} Pr([B_d, A]) = \int_0^t \left(\int_0^{t_A} \alpha\, \lambda_B e^{-\alpha\, \lambda_B t_B}\, dt_B\right) \lambda_A e^{-\lambda_A t_A} dt_A \\ Pr([A, B_a]) = \int_0^t \left(\int_{t_A}^t \lambda_B e^{-\lambda_B (t_B - (1-\alpha) t_A)}\, dt_B\right) \lambda_A e^{-\lambda_A t_A} dt_A \end{cases}$$

Après intégration, nous obtenons:

$$\begin{cases} Pr([B_d, A]) = 1 - e^{-\lambda_A t} - \frac{\lambda_A}{\lambda_A + \alpha\lambda_B}\left(1 - e^{-(\lambda_A + \alpha\lambda_B)t}\right) \\ Pr([A, B_a]) = \frac{\lambda_A}{\lambda_A + \alpha\lambda_B}\left(1 - e^{-(\lambda_A + \alpha\lambda_B)t}\right) - \frac{\lambda_A}{\lambda_A - (1-\alpha)\lambda_B}\left(e^{-\lambda_B t} - e^{-(\lambda_A + \alpha\lambda_B)t}\right) \end{cases}$$

$$Pr(Spare) = 1 - e^{-\lambda_A t} - \frac{\lambda_A}{\lambda_A - (1-\alpha)\lambda_B}\left(e^{-\lambda_B t} - e^{-(\lambda_A + \alpha\lambda_B)t}\right)$$

$$= a - \frac{\lambda_A}{\lambda_A - (1-\alpha)\lambda_B}\overline{b} + \frac{\lambda_A}{\lambda_A - (1-\alpha)\lambda_B}\overline{a} \cdot \overline{b_\alpha}\text{ , pour } \lambda_B \neq \frac{\lambda_A}{1-\alpha}$$

Pour $\lambda_B = \frac{\lambda_A}{1-\alpha}$, nous avons:

$$\begin{cases} Pr([B_d, A]) = 1 - e^{-\lambda_A t} - \frac{\lambda_A}{\lambda_B}\left(1 - e^{-\lambda_B t}\right) \\ Pr([A, B_a]) = \frac{\lambda_A}{\lambda_B}\left(1 - e^{-\lambda_B t}\right) - \lambda_A t\, e^{-\lambda_B t} \end{cases}$$

Après avoir fait la somme, nous obtenons:

$$Pr(Spare) = 1 - e^{-\lambda_A t} - \lambda_A \cdot t\, e^{-\lambda_B t} = a - \lambda_A \cdot t\, \overline{b}\text{ , pour } \lambda_B = \frac{\lambda_A}{1-\alpha}$$

B.3 Expression de probabilité pour la Porte SEQ

$$Pr(SEQ) = \int_0^t \left(\int_{t_A}^t \lambda_B e^{-\lambda_B(t_B - t_A)}\, dt_B\right) \lambda_A e^{-\lambda_A t_A} dt_A$$

$$= 1 - e^{-\lambda_A t} - \frac{\lambda_A}{\lambda_A - \lambda_B}\left(e^{-\lambda_B t} - e^{-\lambda_A t}\right)$$

$$= a - \frac{\lambda_A}{\lambda_A - \lambda_B} \cdot \overline{b} + \frac{\lambda_A}{\lambda_A - \lambda_B} \cdot \overline{a}\text{ , pour } \lambda_A \neq \lambda_B$$

Pour $\lambda_A = \lambda_B = \lambda \Rightarrow a = b = 1 - e^{-\lambda t}$, nous obtenons:

$$Pr(SEQ) = \int_0^t \left(\int_{t_A}^t \lambda \cdot e^{-\lambda(t_B - t_A)}\, dt_B\right) \lambda \cdot e^{-\lambda t_A} dt_A$$

$$= 1 - (1 + \lambda \cdot t)\, e^{-\lambda t}\text{, pour } \lambda_B = \lambda_A = \lambda$$

Annexe C

Expressions de probabilité des séquences de défaillance disjonctives

Les expressions de probabilité de défaillance suivantes sont utilisées pour calculer les probabilités de séquences de défaillance disjonctives liées à la défaillance du SBS. Les séquences disjonctives sont des séquences mutuellement exclusives qui ne peuvent pas se produire en même temps. Elles sont obtenues en supprimant les conjonctions entre les séquences de défaillance originales.

$$Pr([B_1, B_2, B_3]) = \frac{\lambda_1}{\lambda_1+\lambda_2} \cdot (1 - \overline{b_3}) - \frac{\lambda_3}{\lambda_2+\lambda_3} \cdot \left(1 - \overline{b_2} \cdot \overline{b_3}\right) + \frac{\lambda_2 \cdot \lambda_3}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_3)} \cdot \left(1 - \overline{b_1} \cdot \overline{b_2} \cdot \overline{b_3}\right)$$

$$Pr([B_1, B_2, B_3, B_4]) = \frac{\lambda_1 \cdot \lambda_2}{(\lambda_2+\lambda_3)(\lambda_1+\lambda_2+\lambda_3)}\left(1 - \overline{b_4}\right) - \frac{\lambda_1 \cdot \lambda_4}{(\lambda_1+\lambda_2)(\lambda_4+\lambda_3)}\left(1 - \overline{b_3} \cdot \overline{b_4}\right) + \frac{\lambda_3 \cdot \lambda_4}{(\lambda_2+\lambda_3)(\lambda_2+\lambda_3+\lambda_4)}\left(1 - \overline{b_2} \cdot \overline{b_3} \cdot \overline{b_4}\right) - \frac{\lambda_2 \cdot \lambda_3 \cdot \lambda_4}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_3)(\lambda_1+\lambda_2+\lambda_3+\lambda_4)}\left(1 - \overline{b_1} \cdot \overline{b_2} \cdot \overline{b_3} \cdot \overline{b_4}\right)$$

$$Pr([B_1, B_2, B_3, B_4, B_5]) = \frac{\lambda_1 \cdot \lambda_2 \cdot \lambda_3}{(\lambda_3+\lambda_4)(\lambda_2+\lambda_3+\lambda_4)(\lambda_1+\lambda_2+\lambda_3+\lambda_4)}\left(1 - \overline{b_5}\right) - \frac{\lambda_1 \cdot \lambda_2 \cdot \lambda_5}{(\lambda_2+\lambda_3)(\lambda_1+\lambda_2+\lambda_3)(\lambda_4+\lambda_5)}\left(1 - \overline{b_4} \cdot \overline{b_5}\right) + \frac{\lambda_1 \cdot \lambda_4 \cdot \lambda_5}{(\lambda_1+\lambda_2)(\lambda_3+\lambda_4+\lambda_5)(\lambda_3+\lambda_4)}\left(1 - \overline{b_3} \cdot \overline{b_4} \cdot \overline{b_5}\right) - \frac{\lambda_3 \cdot \lambda_4 \cdot \lambda_5}{(\lambda_2+\lambda_3)(\lambda_2+\lambda_3+\lambda_4)(\lambda_2+\lambda_3+\lambda_4+\lambda_5)}\left(1 - \overline{b_2} \cdot \overline{b_3} \cdot \overline{b_4} \cdot \overline{b_5}\right) + \frac{\lambda_2 \cdot \lambda_3 \cdot \lambda_4 \cdot \lambda_5}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_3)(\lambda_1+\lambda_2+\lambda_3+\lambda_4)(\lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5)}\left(1 - \overline{b_1} \cdot \overline{b_2} \cdot \overline{b_3} \cdot \overline{b_4} \cdot \overline{b_5}\right)$$

$$Pr\left([B_1, \cdots, \overline{B_n}]\right) = Pr([B_1, \cdots, B_{n-1}]) \cdot \overline{b_n}$$

Annexe D

Programmes sources décrivant les modèles DTBN dans le Chapitre 4

D.1 Programme source décrit le DTBN relatif au système HSS

Ce programme calcul pour un niveau de discrétisation N=10, la probabilité du système et des sous systèmes, Le chemin le plus probable, le diagnostique, et le facteur d'importance MIF.

```
    % Début
% Chemin ou dossier de la toolbox
cd C:\Users\2011\Downloads\Compressed\FullBNT-1.0.7
addpath(genpath(pwd))

% Données (tableau 3.1) (taux de défaillance des composants)
T=1000;
lambdaS=1E-4;
lambdaP=1E-6;
lambdaVF=1E-5;

delta=100;

Q1=lambdaS*delta;
Q2=lambdaP*delta;
Q3=lambdaVF*delta;

% n est le niveau de discrétisation n=(T/delta)
n= T/delta;
i=1:n;

% TPC des composants (TPC du DigCon = P)
S= exp(-Q1*(i-1))-exp(-Q1*i);
S=[S 1-sum(S)];

P= exp(-Q2*(i-1))-exp(-Q2*i);
P=[P 1-sum(P)];

VF= exp(-Q3*(i-1))-exp(-Q3*i);
```

```
VF=[VF 1-sum(VF)];

%  Nombre de noeuds
N = 19;
dag = zeros(N,N);

% Numérotation des noeuds
s1 = 1; s2 = 2; s3 = 3; and1 = 4; and2 = 5; or1 = 6; and3 = 7; Sensors = 8;
DigCon = 9; p1 = 10; vf1 = 11; p1fault = 12; p2 = 13; seq = 14; vf2 = 15;
p2fault = 16; pfault = 17; or_sdig = 18; system = 19;

% Définition des arcs entre les noeuds
dag(s1,and1) = 1;
dag(s2,and1) = 1;
dag(s1,and2) = 1;
dag(s3,and2) = 1;
dag(s2,and3) = 1;
dag(s3,and3) = 1;
dag(and1,or1) = 1;
dag(and2,or1) = 1;
dag(or1,Sensors) = 1;
dag(and3,Sensors) = 1;
dag(Sensors,or_sdig) = 1;
dag(DigCon,or_sdig) = 1;
dag(p1,p1fault) = 1;
dag(vf1,p1fault) = 1;
dag(p1fault,seq) = 1;
dag(p2,seq) = 1;
dag(seq,p2fault) = 1;
dag(vf2,p2fault) = 1;
dag(p2fault,pfault) = 1;
dag(p1fault,pfault) = 1;
dag(pfault,system) = 1;
dag(or_sdig,system) = 1;

% Tailles des noeuds + nature discrète des noeuds + modèle graphique

discrete_nodes = 1:N;
node_sizes = (n+1)*ones(1,N);
bnet = mk_bnet(dag, node_sizes, 'discrete', discrete_nodes);

% Affectation des TPC aux noeuds
bnet.CPD{s1} = tabular_CPD(bnet, s1, S);
bnet.CPD{s2} = tabular_CPD(bnet, s2, S);
bnet.CPD{s3} = tabular_CPD(bnet, s3, S);
bnet.CPD{and1} = tabular_CPD(bnet, and1, AND);
bnet.CPD{and2} = tabular_CPD(bnet, and2, AND);
bnet.CPD{and3} = tabular_CPD(bnet, and3, AND);
bnet.CPD{or1} = tabular_CPD(bnet, or1, OR);
bnet.CPD{Sensors} = tabular_CPD(bnet, Sensors, OR);
bnet.CPD{p1} = tabular_CPD(bnet, p1, P);
bnet.CPD{p2} = tabular_CPD(bnet, p2, P);
```

```
bnet.CPD{vf1} = tabular_CPD(bnet, vf1, VF);
bnet.CPD{vf2} = tabular_CPD(bnet, vf2, VF);
bnet.CPD{DigCon} = tabular_CPD(bnet, DigCon, P);
bnet.CPD{p1fault} = tabular_CPD(bnet, p1fault, OR);
bnet.CPD{seq} = tabular_CPD(bnet, seq, SEQ);
bnet.CPD{p2fault} = tabular_CPD(bnet, p2fault, OR);
bnet.CPD{pfault} = tabular_CPD(bnet, pfault, AND);
bnet.CPD{or_sdig} = tabular_CPD(bnet, or_sdig, OR);
bnet.CPD{system} = tabular_CPD(bnet, system, OR);

% Construction du Graphe
G = bnet.dag;
draw_graph(G);

% Calcul des probabilités du système et des sous-systèmes
engine = jtree_inf_engine(bnet);
evidence = cell(1,N);
[engine, ll] = enter_evidence(engine, evidence);
m = marginal_nodes(engine, [system]);
o = marginal_nodes(engine, [Sensors]);
s = marginal_nodes(engine, [pfault]);

result1=m.T;
result1(end,:)=[]
P_system=sum(result1)

result2=o.T;
result2(end,:)=[]
P_Sensors=sum(result2)

result3=s.T;
result3(end,:)=[]
P_pfault=sum(result3)

% Le chemin le plus probable (mpe)
evidence = cell(1,N);
[engine, ll] = enter_evidence(engine, evidence);
[mpe, ll] = calc_mpe(engine, evidence);
P_mpe=exp(ll)

% Diagnostique pour les composants S1 et VF1 sachant la défaillance du
système à T=600
evidence = cell(1,N);
evidence{system} = 6;
[engine, ll] = enter_evidence(engine, evidence);
m1 = marginal_nodes(engine, [s1]);
P_eve_s1=m1.T;
P_eve_s1=1-P_eve_s1(end,:)

m2 = marginal_nodes(engine, [vf1]);
P_eve_vf1=m2.T;
P_eve_vf1=1-P_eve_vf1(end,:)
```

```
% MIF pour le composant S1

% P(system/s1failure)
evidence = cell(1,N);
soft_ev=cell(1,T);
soft_ev{s1}=[0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0.1 0]
[engine, ll2] = enter_evidence(engine, cell(1,T), 'soft', soft_ev);
o1 = marginal_nodes(engine, [system]);
P_soft_ev1=o1.T;
P_system_1=P_soft_ev1(end,:)

% P(system/s1succes)
evidence = cell(1,N);
soft_ev=cell(1,T);
soft_ev{s1}=[0 0 0 0 0 0 0 0 0 0 1];
[engine, ll2] = enter_evidence(engine, cell(1,T), 'soft', soft_ev);
o2 = marginal_nodes(engine, [system]);
P_soft_ev2=o2.T;
P_system_2=P_soft_ev2(end,:)

MIF_s1=P_system_2-P_system_1

    % Fin
```

D.2 Programme source décrit le DTBN relatif au système SBS

Le programme suivant calcul la probabilité du scénario d'accident, la probabilité de l'événement initiateur et la probabilité de l'ensemble des barrières pour N=10.

```
    % Début
cd /Users/julienne/Documents/MATLAB
addpath(genpath(pwd))

T=8760;
lambdaLE=1.3E-6;
lambdaLIC=5E-6;
lambdaLICV=2.7E-6;
lambdaLT=6E-7;
lambdaPC=1.6E-6;
lambdaSV=9E-7;
lambdaPCV=2E-6;

delta=876;

Q1=lambdaLE*delta;
```

```
Q2=lambdaLIC*delta;
Q3=lambdaLICV*delta;
Q4=lambdaLT*delta;
Q5=lambdaPC*delta;
Q6=lambdaSV*delta;
Q7=lambdaPCV*delta;

n= T/delta;
i=1:n;

LE=(exp(-Q1*(i-1))-exp(-Q1*i));
LE=[LE 1-sum(LE)];

LIC=(exp(-Q2*(i-1))-exp(-Q2*i));
LIC=[LIC 1-sum(LIC)];

LICV=(exp(-Q3*(i-1))-exp(-Q3*i));
LICV=[LICV 1-sum(LICV)];

LT= exp(-Q4*(i-1))-exp(-Q4*i);
LT=[LT 1-sum(LT)];

PC= exp(-Q5*(i-1))-exp(-Q5*i);
PC=[PC 1-sum(PC)];

SV= exp(-Q6*(i-1))-exp(-Q6*i);
SV=[SV 1-sum(SV)];

PCV= exp(-Q7*(i-1))-exp(-Q7*i);
PCV=[PCV 1-sum(PCV)];

N = 15;
dag = zeros(N,N);
Le = 1; Lic = 2; Licv = 3; Lt = 4; Pc = 5; Sv = 6; Pcv = 7; or1 = 8;
or3 = 9; or4 = 10; La2 = 11; La3 = 12; and = 13; or2 = 14; system = 15;

dag(Le,or1) = 1;
dag(Lic,or1) = 1;
dag(or1,or2) = 1;
dag(Licv,or2) = 1;
dag(Sv,or3) = 1;
dag(Pcv,or3) = 1;
dag(Lt,or4) = 1;
dag(or3,or4) = 1;
dag(or1,La2) = 1;
dag(or4,La2) = 1;
dag(Pc,La3) = 1;
dag(or3,La3) = 1;
dag(La2,and) = 1;
dag(La3,and) = 1;
dag(or2,system) = 1;
dag(and,system) = 1;
```

```
discrete_nodes = 1:N;
node_sizes = (n+1)*ones(1,N);
bnet = mk_bnet(dag, node_sizes, 'discrete', discrete_nodes);

bnet.CPD{Le} = tabular_CPD(bnet, Le, LE);
bnet.CPD{Lic} = tabular_CPD(bnet, Lic, LIC);
bnet.CPD{Licv} = tabular_CPD(bnet, Licv, LICV);
bnet.CPD{Lt} = tabular_CPD(bnet, Lt, LT);
bnet.CPD{Pc} = tabular_CPD(bnet, Pc, PC);
bnet.CPD{Sv} = tabular_CPD(bnet, Sv, SV);
bnet.CPD{Pcv} = tabular_CPD(bnet, Pcv, PCV);
bnet.CPD{or1} = tabular_CPD(bnet, or1, OR);
bnet.CPD{or2} = tabular_CPD(bnet, or2, OR);
bnet.CPD{or3} = tabular_CPD(bnet, or3, OR);
bnet.CPD{or4} = tabular_CPD(bnet, or4, OR);
bnet.CPD{La2} = tabular_CPD(bnet, La2, OR);
bnet.CPD{La3} = tabular_CPD(bnet, La3, OR);
bnet.CPD{and} = tabular_CPD(bnet, and, AND);
bnet.CPD{system} = tabular_CPD(bnet, system, PAND);

G = bnet.dag
draw_graph(G)

% Calcul des probabilités
engine = jtree_inf_engine(bnet);
evidence = cell(1,N);
[engine, ll] = enter_evidence(engine, evidence);
m = marginal_nodes(engine, [system]);
o = marginal_nodes(engine, [and]);
s = marginal_nodes(engine, [or2]);

result1=m.T;
result1(end,:)=[]
P_scénario=sum(result1)

result2=o.T;
result2(end,:)=[]
P_barrières=sum(result2)

result3=s.T;
result3(end,:)=[]
P_EI=sum(result3)

    % Fin
```

D.3 Programme source décrit le DTBN relatif à un composant sujet à DD et DND

Le programme suivant calcul la probabilité et la fréquence de défaillance dangereuse

d’un composant sujet à des défaillances détectées (DD), test de preuve (TP) et test de course partielle (TCP).

```
    % Début

cd C:\Users\2011\Downloads\Compressed\FullBNT-1.0.7
addpath(genpath(pwd))

T=8760;
lambdaTP=0.0002;
lambdaTCP=0.0002;
lambdaDD=0.005;
mu=0.125;
delta=876;

Q1=lambdaTP*delta;
Q2=lambdaTCP*delta;
Q3=(lambdaDD+mu)*delta;

% n est le nombre d'intervals n=(T/delta)
n= T/delta;
i=1:n;


TP= exp(-Q2*(mod((i-1),4380)))-exp(-Q2*(mod(i,4380)));
TP=[TP 1-sum(TP)]

TCP= exp(-Q1*(mod((i-1),730)))-exp(-Q1*(mod(i,730)));
TCP=[TCP 1-sum(TCP)]

DD= (lambdaDD/(lambdaDD+mu))*(exp(-Q3*(i-1))-exp(-Q3*i));
DD=[DD 1-sum(DD)]

N = 5;
dag = zeros(N,N);
tp = 1; tcp = 2; or_gate1 = 3; dd = 4; or_gate2 = 5;

dag(tp,or_gate1) = 1;
dag(tcp,or_gate1) = 1;
dag(or_gate1,or_gate2) = 1;
dag(dd,or_gate2) = 1;

discrete_nodes = 1:N;
node_sizes = (n+1)*ones(1,N);
bnet = mk_bnet(dag, node_sizes, 'discrete', discrete_nodes);

bnet.CPD{tp} = tabular_CPD(bnet, tp, TP);
bnet.CPD{tcp} = tabular_CPD(bnet, tcp, TCP);
bnet.CPD{dd} = tabular_CPD(bnet, dd, DD);
```

```
bnet.CPD{or_gate1} = tabular_CPD(bnet, or_gate1, OR);
bnet.CPD{or_gate2} = tabular_CPD(bnet, or_gate2, OR);

engine = jtree_inf_engine(bnet);
evidence = cell(1,N);
[engine, ll] = enter_evidence(engine, evidence);
o = marginal_nodes(engine, [or_gate2]);

result2=o.T;
result2(end,:)=[]
Pr_D=sum(result2)

Fr_D=(1-Pr_D)*(lambdaTP+lambdaTCP+lambdaDD)

    % Fin
```

Bibliographie

1. IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission. 2010.

2. IEC 61511. Functional Safety – Safety Instrumented Systems for the Process Industry Sector. International Electrotechnical Commission. 2003.

3. CCPS. Layer of protection analysis: Simplified process risk assessment. Joint Publication of the Center for Chemical Process Safety, American Institute of Chemical Engineers. 2001.

4. IEC 61025. Fault tree analysis. International Electrotechnical Commission. 2006.

5. Stamatelatos M, W. Vesely W. Fault tree handbook with aerospace applications. NASA Office of Safety and Mission Assurance, Version 1.1. Washington DC. 2002.

6. Dugan J, Bavuso S, Boyd M. Dynamic fault-tree models for fault-tolerant computer systems. IEEE Transactions on Reliability. 1992;41(3):363-377.

7. Naim P, Henri P, Wuillemin K, Leray P, Pourret O, Becker A. *Réseaux Byésien*. Paris: Eyrolles; 2007.

8. Merle G, Roussel J, Lesage J. Algebraic determination of the structure function of Dynamic Fault Trees. *Reliability Engineering & System Safety*. 2011;96(2):267-277.

9. Boudali H, Dugan J. A discrete-time Bayesian network reliability modeling and analysis framework. *Reliability Engineering & System Safety*. 2005;87(3):337-349.

10. Timms C.R. IEC 61511/An Aid to Comah and Safety Case Regulations Compliance. *Measurement and Control*. 2004;37(4):115-122.

11. Smith D.J, Simpson K.G. L. Safety Critical Systems Handbook. A Straightforward Guide to Functional Safety: IEC 61508 and Related Standards. Elsevier Ltd. 2011.

12. Desroches A, Courtois M, Vesseron P, Gourisse D. *Concepts Et Méthodes Probabilistes De Base De La Sécurité*. Paris: Lavoisier - Tec & Doc; 1995.

13. OHSAS 18001. Système de management de la santé et de la sécurité au travail-Spécification. British Standard Occupational Health and Safety Assessment Series. 2007.

14. Villemeur A. *Reliability, Availability, Maintainability And Safety Assessment*. Chichester: Wiley; 1992.

15. Gouriveau R. Analyse de risques, formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision [Thèse de doctorat]. Institut National Polytechnique de Toulouse, 2003.

16. ISO. Management du risque : Vocabulaire, Principes directeurs pour l'utilisation dans les normes. Organisation internationale de normalisation. 2009.

17. Innal F. Contribution à la Modélisation des Systèmes Instrumentés de Sécurité et à l'évaluation de leurs Performances - Analyse critique de la norme CEI 61508 [Thèse de doctorat]. Université de Bordeaux 1, 2008.

18. ISO. Aspects liés à la sécurité : Principes directeurs pour les inclure dans les normes. Organisation internationale de normalisation. 2014.

19. HSE. Reducing Risk, Protecting People, Discussion Document HMSO. Health and Safety Executive. 1999.

20. Fal E, Ldurka J. Conception et évaluation de la sécurité fonctionnelle des systèmes instrumentés de process industriels. INERIS. 2000.

21. Dunjó J, Fthenakis V, Vílchez J, Arnaldos J. Hazard and operability (HAZOP) analysis. A literature review. *J Hazard Mater*. 2010;173(1-3):19-32.

22. IEEE-Std-500. IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Station. 1984.

23. Center for Chemical Process Safety (CCPS). Guidelines for Process Equipment Reliability Data with Data Tables. American Inst. of Chem. Eng. (AIChE). 1989.

24. Offshore Reliability Data (OREDA). Offshore Reliability Data Handbook, 4th edition. 2002.

25. Simon C, Sallak M, Aubry J.F SIL allocation of SIS by aggregation of experts opinions. Safety and Reliability Conference. In: Stavanger, 2007.

26. Innal F, Dutuit Y, Rauzy A, Signoret J. New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*. 2010;224(2):75-86.

27. Jin H, Summers A. Dependent, independent, and pseudo-independent protection layers in risk analysis. *Process Safety Progress*. 2015;35(3):286-294..

28. Innal F, Cacheux P, Collas S et al. Probability and frequency calculations related to protection layers revisited. *J Loss Prev Process Ind*. 2014;31:56-69.

29. Ge D, Lin M, Yang Y, Zhang R, Chou Q. Quantitative analysis of dynamic fault trees using improved Sequential Binary Decision Diagrams. *Reliability Engineering & System Safety*. 2015;142:289-299.

30. PTC. Windchill FTA. http://www.ptc.com/product/relex/fault-tree. Accédé 2019.

31. Khakzad N, Khan F, Amyotte P. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering & System Safety*. 2011;96(8):925-932.

32. Murphy K. Dynamic Bayesian Networks: Representation, Inference and Learning [Ph.D Thesis]. UCBerkley, Computer Science Division, 2002.

33. Shafiee Kamalabad M, Grzegorczyk M. Improving nonhomogeneous dynamic Bayesian networks with sequentially coupled parameters. *Stat Neerl*. 2018;72(3):281-305..

34. Portinale L, Raiteri D, Montani S. Supporting reliability engineers in exploiting the power of Dynamic Bayesian Networks. *International Journal of Approximate Reasoning*. 2010;51(2):179-195.

35. Dutuit Y, Rauzy A. Approximate estimation of system reliability via fault trees. *Reliability Engineering & System Safety*. 2005;87(2):163-172.

36. Cocozza-Thivent C. *Processus Stochastiques Et Fiabilité Des Systèmes*. Paris: Springer; 1997.

37. Yevkin O. An Efficient Approximate Markov Chain Method in Dynamic Fault Tree Analysis. *Quality and Reliability Engineering International*. 2015;32(4):1509-1520.

38. Ridley L, Andrews J. Optimal design of systems with standby dependencies. *Quality and Reliability Engineering International*. 1999;15(2):103-110.

39. Sullivan K. J, Dugan J. B, Coppit D. The Galileo fault tree analysis tool. 29th Annual International Symposium on Fault-Tolerant Computing. In: Los Alamitos, 1999:232-235.

40. Dugan J, Sullivan K, Coppit D. Developing a low-cost high-quality software tool for dynamic fault-tree analysis. *IEEE Trans Reliab*. 2000;49(1):49-59.

41. Chebila M, Innal F. Unification of Common Cause Failures' Parametric Models Using a Generic Markovian Model. *Journal of Failure Analysis and Prevention*. 2014;14(3):426-434.

42. Dutuit Y, Rauzy A. A linear-time algorithm to find modules of fault trees. *IEEE Trans Reliab*. 1996;45(3):422-425.

43. Pagès A, Gondran M. *Fiabilité Des Systèmes*. Paris: Eyrolles; 1980.

44. Høyland A, Rausand M. *System Reliability Theory*. Hoboken: John Wiley & Sons, Inc.; 2009.

45. Fussell J, Aber E, Rahl R. On the Quantitative Analysis of Priority-AND Failure Logic. *IEEE Trans Reliab*. 1976;R-25(5):324-326.

46. Neil M, Marquez D. Availability modelling of repairable systems using Bayesian networks. *Engineering Applications of Artificial Intelligence*. 2012;25(4):698-704.

47. Liu D, Zhang C, Xing W, Li R. Bayesian Networks Based Reliability Analysis of Phased-Mission Systems. *Chinese Journal of Computers*. 2009;31(10):1814-1825.

48. Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering & System Safety*. 2001;71(3):249-260.

49. Langseth H, Portinale L. Bayesian networks in reliability. *Reliability Engineering & System Safety*. 2007;92(1):92-108.

50. Jensen F. *An Introduction To Bayesian Networks*. New York, N.Y: Springer; 1998.

51. Jensen F, Nielsen T. *Bayesian Networks And Decision Graphs*. New York, NY: Springer New York; 2007.

52. Weber P, Munteanu P, Jouffe L. Dynamic Bayesian Networks Modelling the Dependability of Systems with Degradations and Exogenous Constraints. *IFAC Proceedings Volumes*. 2004;37(4):207-212.

53. HAMAIDIA M, INNAL F, KARA M. Un modèle bayésien pour résoudre la fiabilité des systèmes dynamiques. 3ème Conférence Internationale de Mécanique. A Annaba; 2017.

54. Codetta-Raiteri D. Applying Generalized Continuous Time Bayesian Networks to a reliability case study. *IFAC-PapersOnLine*. 2015;48(21):676-681.

55. Montani S, Portinale L, Bobbio A, Codetta-Raiteri D. Radyban: A tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks. *Reliability Engineering & System Safety*. 2008;93(7):922-932.

56. Hugin Expert Hugin Expert. Hugin.com. https://www.hugin.com. Accédé 2019.

57. Yuge T, Yanagi S. Quantitative analysis of a fault tree with priority AND gates. *Reliability Engineering & System Safety*. 2008;93(11):1577-1583.

58. Liu D, Zhang C, Xing W, Li R, Li H. Quantification of Cut Sequence Set for Fault Tree Analysis. *High Performance Computing and Communications*. 2007:755-765.

59. Xing L, Shrestha A, Dai Y. Exact combinatorial reliability analysis of dynamic systems with sequence-dependent failures. *Reliability Engineering & System Safety*. 2011;96(10):1375-1385.

60. Ge D, Li D, Chou Q, Zhang R, Yang Y. Quantification of Highly Coupled Dynamic Fault Tree Using IRVPM and SBDD. *Quality and Reliability Engineering International*. 2014;32(1):139-151.

61. Rauzy A. Sequence Algebra, Sequence Decision Diagrams and Dynamic Fault Trees. *Reliability Engineering & System Safety*. 2011;96(7):785-792.

62. Arnold F, Belinfante A, Van der Berg F, Guck D, Stoelinga M. Dftcalc: a tool for efficient fault tree analysis (extended version). Technical Report TR-CTIT-13-13, CTIT, University of Twente, Enschede. 2013.

63. Merle G, Roussel J, Lesage J, Perchet V, Vayatis N. Quantitative Analysis of Dynamic Fault Trees Based on the Coupling of Structure Functions and Monte Carlo Simulation. *Quality and Reliability Engineering International*. 2014;32(1):7-18.

64. Durga Rao K, Gopika V, Sanyasi Rao V, Kushwaha H, Verma A, Srividya A. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. *Reliability Engineering & System Safety*. 2009;94(4):872-883.

65. Chiacchio F, Compagno L, D'Urso D, Manno G, Trapani N. Dynamic fault trees resolution: A conscious trade-off between analytical and simulative approaches. *Reliability Engineering & System Safety*. 2011;96(11):1515-1526.

66. Cheshmikhani E, Zarandi H. Probabilistic analysis of dynamic and temporal fault trees using accurate stochastic logic gates. *Microelectronics Reliability*. 2015;55(11):2468-2480.

67. Ejlali A, Miremadi S. G. Time-to-failure tree. Annual Reliability and Maintainability Symposium. In: Tampa; 2003:148-152.

68. Hamaidia M, Kara M, Innal F. Probability and Frequency Derivation Using Dynamic Fault Trees. *Process Safety Progress*. 2018;37(4):535-552.

69. Ni J, Tang W, Xing Y. A Simple Algebra for Fault Tree Analysis of Static and Dynamic Systems. *IEEE Trans Reliab*. 2013;62(4):846-861.

70. Walker M, Papadopoulos Y. Qualitative temporal analysis: Towards a full implementation of the Fault Tree Handbook. *Control Eng Pract*. 2009;17(10):1115-1125.

71. Merle G. Analyse algébrique des arbres de défaillance dynamiques, contribution aux analyses qualitative et quantitative [Thèse de doctorat]. Ecole Normale Supérieure De Cachan, 2010.

72. Rauzy A. Mathematical foundations of minimal cutsets. *IEEE Trans Reliab*. 2001;50(4):389-396.

73. Tang Z, Dugan J. B. Minimal cut set/sequence generation for dynamic fault trees. Annual Reliability and Maintainability Symposium. In: Los Angeles; 2004:207-213.

74. HAMAIDIA M, INNAL F. Failure Sequences to Solve Dynamic Fault Trees. 4ème Conférence Internationale sur la Maintenance et la Sécurité Industrielle. A Skikda; 2017.

75. Merle G, Roussel J, Lesage J. Quantitative Analysis of Dynamic Fault Trees Based on the Structure Function. *Quality and Reliability Engineering International*. 2013;30(1):143-156.

76. Dutuit Y, Rauzy A. Approximate estimation of system reliability via fault trees. *Reliability Engineering & System Safety*. 2005;87(2):163-172.

77. Singh C. Calculating the Time-Specific Frequency of System Failure. *IEEE Trans Reliab*. 1979;R-28(2):124-126.

78. Singh C. Rules for Calculating the Time-Specific Frequency of System Failure. *IEEE Trans Reliab*. 1981;R-30(4):364-366.

79. GRIF-Workshop, Graphical interface for reliability forecasting software, http://grif-workshop.com. Accédé 2019.

80. Weber P, Medina-Oliva G, Simon C, Iung B. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence*. 2012;25(4):671-682.

81. Khakzad N, Khan F, Amyotte P. Risk-based design of process systems using discrete-time Bayesian networks. *Reliability Engineering & System Safety*. 2013;109:5-17.

82. MathWorks - Makers of MATLAB and Simulink. Mathworks.com. https://www.mathworks.com. Accédé 2019.

83. Murphy K. The Bayes net toolbox for MatLab. *Operational Research*. 1999;43(4):633-640.

84. Bobbio A, Codetta-Raiteri D, Montani S, Portinale L. Reliability Analysis of Systems with Dynamic Dependencies. In: Pourret O, Naim P, Marcot B, ed. *Bayesian Networks: A Practical Guide To Applications*. John Wiley & Sons; 2008:225–238.

85. Codetta-Raiteri D, Portinale L. A Petri Net based tool for the analysis of Generalized Continuous Time Bayesian Networks. In: Gribaudo M, Iacono M, ed. *Theory and Application of Multi-Formalism Modeling*. Information Science Reference; 2013: 118-143.

86. Birnbaum Z.W. On the importance of different components in a multicomponent system. In: Krishnaiah P. R, ed. *Multivariate Analysis*. Academic Press; 1969: 591-592.

87. Chebila M, Innal F. Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH. *J Loss Prev Process Ind*. 2015;34:167-176.