الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

جامعة وهران 2 محمد بن أحمد
Université d'Oran 2 Mohamed Ben Ahmed

معهد الصيانة والأمن الصناعي
Institut de Maintenance et de Sécurité Industrielle

Département de Sécurité Industriel et Environnement

Filière : Hygiène et Sécurité Industrielle
Spécialité : Sécurité prévention et intervention

MEMOIRE

Pour l'obtention du diplôme de Master

Thème

Les Arbres de Défaillance Non Cohérents

Réaliser par :

CHAIB Mohammed Amine

AGUEB Tewfik

Présenté devant le jury :

Président : Mme AOUMEUR Yamina

Examinateur : Mme TALBI Zahira

Encadreur : Mme BENOMAR Fatima

Année 2022/2023

Résumé :

L'arbre de défaillance est une technique très connue dans l'analyse des risques, et considéré comme l'une des méthodes les plus utilisées dans la sureté de fonctionnement qui est une science qui vise à assurer le bon fonctionnement du processus industrielles tout au long du cycle de vie de produit.

Un arbre de défaillance est classé comme cohérent et non cohérent selon le système étudié. Les systèmes étudiés peuvent être cohérents là où l'état de défaillance d'un composant peut conduire à la panne du système, et non cohérents là où les deux états de défaillance et de fonctionnement peuvent entrainer la défaillance du système.

Dans ce travail, nous aborderons comment étudier un système non cohérent à l'aide de la méthode d'arbre de défaillance et déterminer sa fiabilité et les éléments qui ont le plus d'impact sur le fonctionnement du système. On utilise le logiciel Isograph.

Mots clés : arbre de défaillance cohérent, arbre de défaillance non cohérent, sureté de fonctionnement, logiciel Isograph.

Abstract :

The fault tree is a technique that is well known in the risk analysis, and among the most used methods in the operating safety which is a science that aims to ensure the proper functioning of industrial processes throughout the product life cycle.

A fault tree is classified as coherent and non-coherent according to the system studied. The systems studied can be coherent where the failure state of a component can lead to system failure, and non coherent where the two failure and function states can cause system failure.

In this work, we will discuss how to study a non-coherent system using the fault tree method and determine its reliability and the elements that have the most impact on the functioning of the system. The analysis is done by Isograph software.

Key words : coherent faut tree, non-coherent faut tree, operating safety, Isograph software.

ملخص :

شجرة الخطأ هي تقنية معروفة جدا في تحليل المخاطر، ومن بين أكثر الطرق المستخدمة في سلامة التشغيل التي هي علم يهدف إلى ضمان الأداء المناسب للعمليات الصناعية خلال دورة حياة المنتج.

تصنف شجرة الخطأ إلى متسقة وغير متسقة وفقا للنظام المدروس. يمكن أن تكون الأنظمة المدروسة متسقة حيث يمكن أن تؤدي حالة فشل أحد المكونات إلى فشل النظام، وغير متسقة حيث يمكن أن تسبب حالتا الفشل والعمل فشل النظام.

في هذا العمل، سنناقش كيفية دراسة نظام غير متسق باستخدام طريقة شجرة الخطأ وتحديد موثوقيته والعناصر التي لها تأثير أكبر على عمل النظام. تم التحليل بناء على برنامج Isograph.

كلمات مفتاحية : شجرة خطأ متسقة، شجرة خطأ غير متسقة، سلامة التشغيل، برنامج Isograph.

Remerciement

Nous voudrions remercier Allah de nous avoir donné l'énergie et la patience pour accomplir cet humble travail.

Tout d'abord, nous tenons à adresser nos sincères salutations et nos remerciements à notre mentor, Mme BENOMAR Fatima, pour tous les conseils, orientations et informations précieux qu'elle nous a donné.

Nous remercions également nos familles pour le soutien financier et moral sans oublier nos collègues et tous ceux qui nous ont aidé de près ou de loin.

Enfin, nous exprimons nos remerciements et notre gratitude aux membres du jury pour leur aimable acceptation et examen de notre travail.

Dédicace

Nous dédions cet humble travail à :

Nos parents et toute la famille pour leur confiance, leurs conseils, grâce à eux nous sommes arrivés ici.

Ainsi qu'à nos amis, et à tous ceux qui nous respectons.

Table des matières

Liste de figures

Liste des tableaux

Liste des Acronymes

ADD	Arbre de défaillance
AMDEC	Analyse des modes de défaillance, de leurs effets et de leur criticité
APR	Analyse préliminaire des risques
BDD	Diagramme de décision binaire (Binary decision diagram)
BDF	Bloc diagramme de fiabilité
ER	Événement redouté
FIP	Facteurs d'importance probabilistes
FDMS	Fiabilité, disponibilité, maintenabilité et sécurité
FFA	Analyse de défaillance fonctionnelle (Functional Failure Analysis)
FTA	Arbre de défaillance (Fault Tree Analysis)
FMEA	Analyse des modes de défaillance et de leurs effets (Failure Modes and Effects Analysis)
HiP-HOPS	Etudes Hiérarchisées d'Origin et de Propagation des dangers (Hierarchically Performed Hazard Origin and Propagation Studies)
L-BDD	Diagramme de décision binaire étiquetée (labelled BDD)
MDT	Durée moyenne d'indisponibilité (Mean Down Time)
MTBF	Durée moyenne entre deux défaillances consécutives d'une entité réparée (Mean Time Between Failure)
MTTF	Durée moyenne de fonctionnement avant la première défaillance (Mean Time To Failure)
MTTR	Durée moyenne de réparation (Mean Time To Repair)
MUT	Durée moyenne de fonctionnement après réparation (Mean Up Time)
SFBDD	Structure fonction binary decision diagram
TDD	Diagramme de décision ternaire (ternary decision diagram)
ZBDD	Diagramme de décision binaire à zéro supprimé (zero-suppressed BDD)

Introduction générale :

Le développement important de l'industrie dans les divers domaines depuis la fin du XIXe siècle, pendant la Seconde Guerre mondiale, et puis la mise en place des réacteurs nucléaires ce qui a conduit à une complexité accrue des processus industriels et augmenter le nombre de machines et d'équipements dans les usines et les ateliers, qui augmente automatiquement le niveau de risque pour les personnes et le milieu environnant, cela a nécessité une révolution dans le domaine de la sécurité, la sûreté et une analyse des risques de manière plus précise et détaillée.

La sûreté de fonctionnement est une science qui permet aux utilisateurs du système de placer une confiance justifiée dans le service qu'il leur délivre [1] est un domaine qui vise à évaluer les risques et assurer le bon fonctionnement du processus de fabrication et de production tout au long du cycle de vie du produit.

Parmi les méthodes d'analyse des risques très connus la méthode d'arbre de défaillance. Bell Téléphone Laboratoires a développé ce concept au début des années soixante pour l'US Air Force pour une utilisation avec le système Minute man. Puis cette méthode a été utilisée par la compagnie Boeing pour analyser la sécurité des systèmes.

L'arbre de défaillance est une modélisation graphique d'un ensemble des événements conduisant à un événement indésirable (défaillance). Au début des années 1970, lorsque cette technique d'analyse déductive est devenue populaire et très utile dans les divers domaines industriels (aéronautique, nucléaire...) des logiciels ADD ont été créés tel que Isograph Fault Trees +. [2]

Dans les arbres de défaillance cohérents l'utilisation des portes logiques telles que "ET" et "OU" est uniquement lors de la construction d'un ADD, lorsque la logique "NOT" est utilisée ou directement impliquée (porte "OU" exclusif, "XOR") l'arbre de défaillance résultant est non cohérent. L'introduction de la porte logique "NOT" rend le système non cohérent car les états de défaillance des composants et les états de fonctionnement peuvent contribuer à la panne du système, ce qui rend les analyses qualitatives et quantitatives plus difficiles.

Dans ce travail, nous visons à déterminer la différence entre un système cohérent et un système non cohérent et comment l'analyse qualitative et quantitative se fait dans un arbre de défaillance non cohérent.

Le premier chapitre va définir les concepts de base de la sûreté de fonctionnement et quelques méthodes d'analyse des risques.

Le deuxième chapitre sera consacré à la méthode d'arbre de défaillance, sa démarche, sa construction, l'analyse qualitative et quantitative.

Dans le troisième chapitre, nous aborderons de la manière dont le système devient incohérent, des raisons qui y conduisent et des méthodes utilisées dans l'étude quantitative et qualitative de l'arbre de défaillance non cohérente.

Le quatrième chapitre sera consacré à l'étude de cas. L'application de la méthode d'arbre de défaillance dans l'étude de la fiabilité d'un système non cohérent.

Nous terminons notre travail par une conclusion générale.

CHAPITRE 1 :

La sûreté de fonctionnement

1. Introduction :

Depuis la révolution industrielle de la fin du XVIII (18-ème) siècle et du début du XIX (19-ème) siècle et le développement terrible des industries qui est la cause qui a entraîné une augmentation significative et notable des accidents du travail et du nombre de pannes lors des processus industriels. Il est devenu nécessaire d'avoir un saut qualitatif significatif dans le domaine de la sécurité et de la sûreté de fonctionnement.

La complexité croissante des systèmes, la réduction des coûts de conception, leur utilisation croissante dans la vie quotidienne ont fait de la sûreté de fonctionnement un élément essentiel dans le développement de tout système industriel. [3]

La sûreté de fonctionnement est un domaine qui propose les mesures et les moyens nécessaires pour améliorer la sécurité et augmenter la fiabilité des systèmes industriels à des moments précis et avec des coûts raisonnables. [4]

L'histoire moderne nous montre l'importance de la sûreté de fonctionnement dans divers systèmes et installations industriels, notamment dans la sensibilisation, la réduction des accidents, la mise en place des mesures préventives nécessaires, le maintien et l'élévation du niveau de sécurité et de fiabilité.

Dans ce chapitre, nous aborderons les principaux concepts de la sûreté de fonctionnement et les méthodes les plus courants d'analyse des risques.

2. Sûreté de fonctionnement :

La sûreté de fonctionnement est souvent appelée la science des défaillances, elle caractérise l'aptitude d'une entité ou un système à accomplir une ou plusieurs fonctions données dans des circonstances particulières [5] et pendant une période de temps déterminée. La sûreté de fonctionnement permet de vérifier les performances du système pour les fonctions pour lesquelles il a été créé, et permet également d'identifier et d'étudier les risques potentiels et d'évaluer leur dangerosité pour les personnes, l'environnement et les équipements. [6]

Elle englobe principalement quatre critères fondamentaux qui sont : la fiabilité, la disponibilité, la maintenabilité et la sécurité (FDMS).

On peut préciser les composants de la sûreté de fonctionnement dans le schéma suivant :

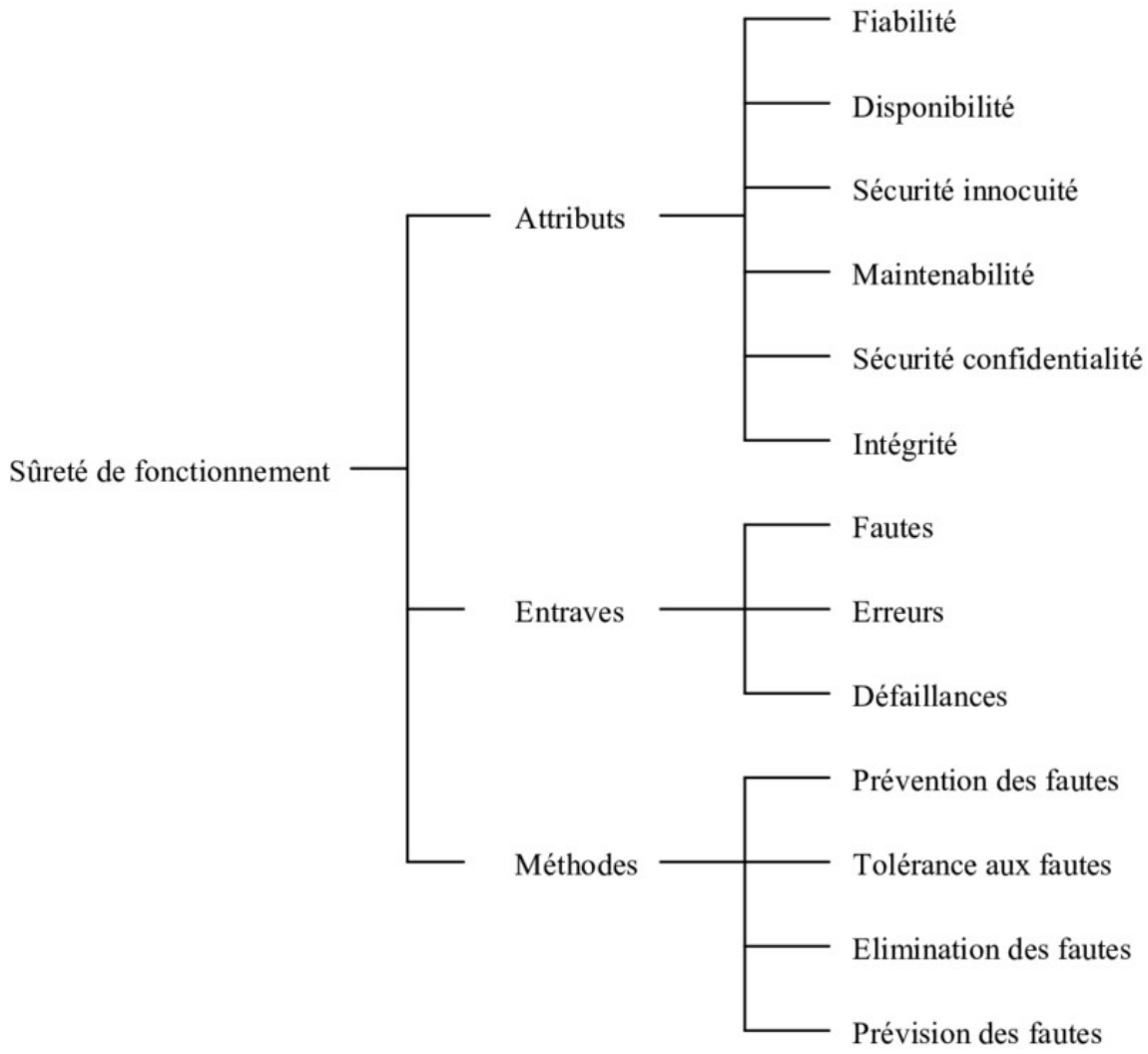


Figure 1 : Taxonomie de la sûreté de fonctionnement

3. Notions de définitions :

1- Fiabilité : est la probabilité qu'a une machine, un composant ou un système complet soit capable d'accomplir, de manière satisfaisante, une fonction requise ou une tâche dans des conditions données et dans une durée de temps bien déterminé. [7]

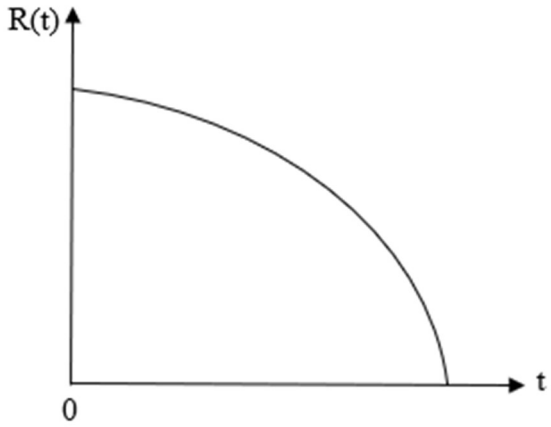


Figure 2 : La fiabilité R(t)

- La fiabilité R(t) est fonction décroissante sur l'intervalle]0, +∞[
- $\lim_{t\to\infty} R(t) = 0$

2- Disponibilité : est l'aptitude d'un dispositif à être capable d'accomplir une fonction requise dans des conditions données, pendant un intervalle de temps sans arrêt et sans panne. Notons qu'un haut niveau de disponibilité exige une très bonne fiabilité et une bonne maintenance [8], donc pour un système non réparable la disponibilité est égale à la fiabilité A(t) = R(t), et d'une façon générale A(t) ≥ R(t).

3- Maintenabilité : caractérise l'aptitude d'un composant à être maintenue ou rétablie d'une façon dans laquelle il peut accomplir sa fonction maintenue dans des conditions données, pendant une durée de temps et en utilisant des procédures et des moyens prescrits. [9]

La maintenabilité est une fonction croissante entre 0 et +∞.

$$\lim_{t\to\infty} M(t) = 1$$

4- Sécurité : est l'aptitude d'une machine à accomplir sa tâche, à être transportée, démontée, maintenue, mise au point [10] sans générer des évènements qui peuvent être considérés comme critiques ou catastrophiques sur la vie humaine.

5- Défaillance : est l'altération ou la cessation d'un dispositif à accomplir sa tâche ou de ne pas assurer correctement sa fonction. Il l'est fait passer un dispositif d'un état d'exploitation normale à état anormale ou panne.

On peut classer les défaillances selon leurs effets : [11]

- Défaillance mineure : elle cause un dommage négligeable au système et à son environnement, elle ne présente aucun risque pour la vie humaine.

- Défaillance éminente (significative) : peu de dommages survient au fonctionnement du système sans risque significatif pour la sécurité des travailleurs.

- Défaillance critique : entraîne la perte d'une ou plusieurs fonctions essentielles du système, sans risque de mort ni de blessures graves chez les travailleurs.

- Défaillance catastrophique : la perte d'une ou plusieurs fonctions essentielles du système. Elle provoque de graves pertes pour le système et les installations, ainsi que le risque de mort et les blessures graves pour les personnes.

6- Risque : est la probabilité qu'une personne subisse un préjudice ou des effets néfastes sur sa santé dans le cas d'exposition à un danger. Ce concept peut également s'appliquer aux situations où il y a une perte de biens ou d'équipements ou des effets nocifs pour l'environnement. [12]

7- Taux de défaillance : est une des caractéristiques de la fiabilité, il représente la probabilité qu'un dispositif tombe en panne pendant la période entre t et dt, sachant qu'il a fonctionné entre 0 et t (n'a pas eu une défaillance dans l'intervalle de temps [0; t]). [13]

$$\lambda(t) = -\frac{1}{R(t)} . \frac{dR(t)}{dt}$$

L'unité de mesure du taux de défaillance est 1/temps.

Le taux de défaillance est représenté dans la courbe suivante :

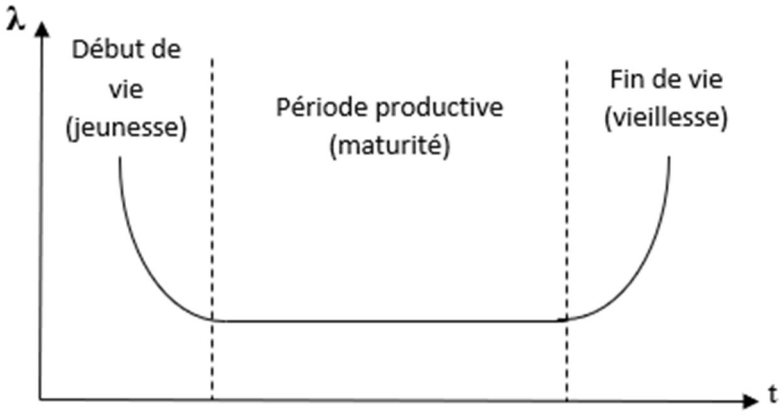


Figure 3 : Courbe en baignoire

8- Taux de réparation : représente la fréquence de réparations (le nombre de réparations divisé par le temps total de réparation), il caractérise l'aptitude d'un bien à être réparé et de l'efficacité de la maintenance durant la phase active d'une intervention : [8]

$$\mu(t) = \frac{1}{1-M(t)} . \frac{dM(t)}{dt}$$

4. Les temps caractéristiques pour la sûreté de fonctionnement :

1- MTTF (mean time to failure) : le temps moyen de fonctionnement jusqu'à la survenue de la première défaillance (le temps avant la premier panne), avec :

$$MTTF[h] = \frac{1}{\lambda}$$

2- MTTR (mean time to repair) : la durée moyenne de réparation ou de la remise en état de fonctionnement, avec : $MTTR[h] = \frac{1}{\mu}$

3- MTBF (mean time between failure) : est la durée moyenne de bon fonctionnement entre deux défaillances consécutives d'un composant réparé

$MTBF[h] = MTTF[h] = \frac{1}{\lambda}$ (dans le cas d'un composant non réparable)

4- MUT (mean up time) : le temps moyen de fonctionnement après la réparation c'est-à-dire le temps entre la remise en service et une nouvelle panne (temps moyen de disponibilité).

5- MDT (mean down time) : le temps moyen de l'indisponibilité (le temps de détection de la panne +le temps de réparation + le temps de la remise en service).

Avec : MTBF = MUT + MDT.

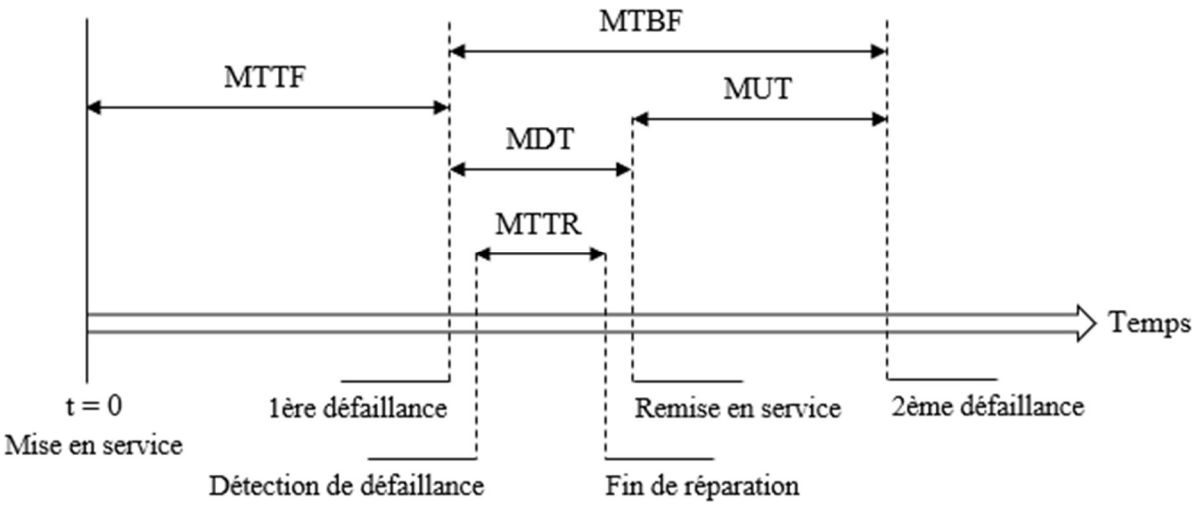


Figure 4 : Les temps caractéristiques pour la sûreté de fonctionnement

5. Quelques méthodes d'analyse des risques :

Il existe de nombreuses méthodes d'analyse, elles sont différentes dans leurs principes et leurs objectifs, mais elles sont impliquées dans l'évaluation et la maitrise des risques.

5.1. Analyse Préliminaire des Risques :

Est un moyen bien connu depuis le début des années 1960, il a ensuite été utilisé dans de nombreuses autres industries.

L'analyse préliminaire des risques permet d'identifier tous les risques potentiels et évènements conduisant à un accident, classer selon leur sévérité et les actions nécessaires pour les éviter. [14]

Cette méthode est beaucoup utilisée dans les premières étapes de la conception d'une installation. Donc, en général la méthode ne nécessite pas des informations approfondies de l'installation étudiée.

Pour faire une analyse préliminaire des risques complet il faut suivre les étapes suivantes : [15]

• Préparation de l'analyse : cette étape est de déterminer le contexte.

• Description et modélisation du système.

• Identifier les différents risques et événements à craindre.

• Analyse des cas dangereux.

• Analyse des conséquences.

• Rechercher les obstacles existants.

• Evaluer d'une manière qualitative ou semi-qualitative l'intensité, la fréquence ou la probabilité.

• Proposer de nouveaux obstacles.

• Rédiger un rapport similaire.

5.2. Diagramme de fiabilité :

Appelé aussi Diagramme de Succès est l'une des anciennes méthodes d'analyse des risques et de calcul de fiabilité des systèmes, elle est utile pour les systèmes non réparables et dans certaines conditions pour les systèmes réparables. Il s'agit d'une représentation graphique qui visualise, sous forme d'un diagramme représentatif les composants du système participants à la mission, chaque composant est représenté par un bloc.

Le bloc qui cause la défaillance du système est monté en série, et le bloc qui cause la défaillance du système s'il est connecté avec un autre bloc est monté en parallèle. [16]

Le BDF représente un système et est utilisé pour déterminer sa fiabilité et il est fonctionnel s'il existe au moins un chemin fonctionnel de source S et de destination D. [17]

On peut trouver trois types de systèmes : série, parallèle et série parallèle.

Dans cette représentation, les systèmes étudiés doivent vérifier les deux hypothèses suivantes:

- Hypothèse d'états binaires.

- les états de fonctionnement et de défaillance des composants doivent être indépendantes. [18]

5.3. Arbre de défaillance :

L'arbre de défaillance (ADD) est une technique d'ingénierie souvent utilisée dans les études de sécurité et de fiabilité des systèmes, la méthode a été élaborée en Etats-Unis au début des années soixante et a été développée au fur des années soixante-dix.

L'ADD est une méthode largement utilisée dans l'analyse des risques, elle a une grande variété de techniques de modélisation et d'analyse avec une large gamme d'outils logiciels. [19]

Il s'agit d'une représentation graphique de combinaisons d'événements qui conduisent à la survenue d'un événement indésirable (panne, défaillance...). [20]

Maintenant, cette méthode est utilisée dans de nombreuses industries telles que nucléaire, chimique, l'industrie automobile ….

5.4. Analyse des modes de défaillances, de leurs effets et de leur criticité :

Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) est l'extension naturelle de l'analyse des modes de défaillance et de leurs effets (AMDE) utilisée pour la première fois dans les années 1960 pour l'analyse de la sécurité dans l'industrie aéronautique. [21]

C'est une méthode d'étude à l'avance les défaillances d'un appareil. C'est analyser les modes de défaillance un par un, en donnant la priorité aux causes d'origine de la défaillance, identifier et mettre en œuvre des mesures correctives selon la criticité observée.

Elle aide à améliorer la fiabilité du produit, du processus et du service actuel d'un moyen de production et à empêcher l'échec lors de la phase de conception. [22]

Cette méthode est structurée autour de quatre étapes de base : [23]

- La mise en place de la méthode :

Elle se fait par un groupe de personnes pluridisciplinaire avec la présence d'une personne maîtrisant cette méthode et à l'aide de toute personne participant à un processus dans l'appareil ou l'installation.

- Analyse des processus :

Il est très important de définir correctement le système étudié en fonction des objectifs souhaités et de diviser le processus en parties pour analyser et étudier.

- Analyse des risques :

Identifier les risques et les modes de défaillance à l'aide de la question « qu'est-ce qui pourrait mal se passer ? ».

Evaluer les risques par une cotation consensuelle.

Hiérarchiser les risques en fonction de leur criticité et déterminer l'acceptabilité des autres risques.

- Domaines d'amélioration proposés et leurs impacts potentiels :

Les retours d'expérience obtenus permettent de connaître l'efficacité de cette méthode sur les systèmes étudiés.

Les types d'AMDEC : [24]

- l'AMDEC organisation : s'applique à tous les niveaux du processus de travail (le système de gestion, le système d'information, le système production...).

- l'AMDEC produit (AMDEC projet) : étudier en détail les produits ou les projets de la phase de conception.

- l'AMDEC processus : s'applique aux processus de fabrication. Elle est utilisée pour analyser et évaluer la criticité de toutes les défaillances possibles d'un produit résultant de son processus. Il peut également être utilisé dans les postes de travail.

- l'AMDEC moyen : s'applique à toutes les machines, appareils de fabrication, logiciels et systèmes de transport internes.

- l AMDEC service : vérifier que la valeur ajoutée est atteinte dans

Le service correspond aux attentes des clients et que le processus de réalisation de service ne provoque pas de défaillances.

- l'AMDEC sécurité : assurer la sécurité des opérateurs dans là où il y a des risques.

6. Comparaison des méthodes :

La méthode	Statique/ dynamique	Qualitatif/ quantitatif	Inductif/ déductif	Objectif
Analyse Préliminaire des Risques (APR)	Dynamique	Qualitatif	Inductif	Identifier les dangers liés au système, déterminer ses causes et évaluer leur gravité et les conséquences correspondent aux situations dangereuses et aux accidents potentiels.
Bloc Diagramme de Fiabilité (BDF)	Statique	Qualitatif quantitatif	Déductif	Une représentation graphique qui vise à visualiser les composants d'un système et les fonctions qu'ils remplissent pour assurer le succès de la fonction principale du système, cette modélisation est utilisée pour déterminer la fiabilité du système.
Arbre De Défaillance (ADD)	Statique	Qualitatif quantitatif	Déductif	Construire une synthèse de tout ce qui peut conduire à un événement indésirable et d'évaluer l'impact de la modification du système, et de comparer les résultats des mesures qui peuvent être envisagées pour réduire l'occurrence d'un événement indésirable étudié.
Analyse des Modes de Défaillances, de leurs Effets et de	Statique	Qualitatif	Inductif	Une approche inductive rigoureuse pour identifier les défaillances dont les conséquences peuvent affecter le fonctionnement du système, les

leur Criticité (AMDEC)				hiérarchiser en fonction de leur niveau de criticité afin de les maîtriser.

Tableau 1 : Comparaison des méthodes

7. Avantages et limites des méthodes de la sûreté de fonctionnement :

La méthode	Avantages	Limites
Analyse Préliminaire des Risques (APR)	- Cette méthode est relativement économique en termes de temps pris et ne nécessite pas un niveau de description très détaillé du système étudié. - Permettre de faire un examen rapide des situations dangereuses sur les installations et devant faire une étude détaillée (dans la phase de conception).	- Ne convient pas pour étudier et caractériser les évènements susceptibles de conduire à un accident majeur pour des systèmes complexes. - Une analyse superficielle et préliminaire pour les installations et équipements qui nécessitent une étude plus fine menée grâce à des méthodes telles que AMDEC et arbres de défaillance.
Bloc Diagramme de Fiabilité (BDF)	-Un modèle facile et simple pour identifier les éléments critiques. - La méthode de bloc diagramme de fiabilité identifie les composants critiques du système, collecte les données de fiabilité des composants et montre comment le système réagit à un mode de défaillance spécifique pour déterminer sa fiabilité globale.	- Difficulté à prendre en compte les éléments multifonctionnels. - Prise en charge de l'indépendance des défaillances des divers éléments.

Arbre De Défaillance (ADD)	- Les ADD sont particulièrement adaptés aux systèmes complexes tels que les centrales nucléaires, les systèmes de communication... - Ils sont plus facile à lire et à comprendre que les autres modèles de fiabilité. - Les résultats obtenus peuvent fournir des données qualitatives ou quantitatives pour le processus d'évaluation des risques.	- La méthode nécessite une connaissance approfondie des scénarios événementiels et du fonctionnement du système. - La méthode nécessite parfois un programme informatique, lorsque le nombre des événements dépasse quelques dizaines d'unités. - Dans le cas des grands arbres les événements peuvent être oubliés, particulièrement pour les systèmes à haut risque.
Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité (AMDEC)	- C'est un outil très puissant, sur champ d'application très large, qui peut également être mis en œuvre dans la conception plus que dans le fonctionnement. - Les résultats obtenus sont spécifiquement détaillées surtout dans la propagation des défaillances et leurs conséquences.	- Il est difficile de prendre en compte les phénomènes combinatoires ou dynamiques et les pannes multiples. - L'analyse est complétée par des autres méthodes comme les arbres de défaillance.

Tableau 2 : Avantages et limites des méthodes

8. Conclusion :

La révolution industrielle et le développement des industries qui était une raison de la complexité croissante des systèmes, la réduction des coûts de conception…, avoir un mauvais côté, une augmentation significative des accidents du travail et des pannes lors des processus de production et de fabrication.

Cette augmentation introduit la sûreté de fonctionnement pour améliorer la sécurité et augmenter la fiabilité des systèmes industriels. Aussi appelée la science des défaillances, la sûreté de fonctionnement permet de vérifier les performances du système et d'identifier les risques potentiels et d'évaluer leur dangerosité pour les personnes, l'environnement et les équipements.

Il existe de nombreuses méthodes d'analyse des risques chacun de sa propre approche d'analyse, comme L'analyse préliminaire des risques (APR), Diagramme de fiabilité ou de succès, l'arbre de défaillance (ADD), analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC).

CHAPITRE 2 :

Les arbres de défaillance

1. introduction :

Un arbre de défaillance ADD ou Fault tree analysis FTA (en anglais) est une technique déductive (de conséquence vers ses causes) utilisée dans l'ingénierie des études de sécurité et de fiabilité des systèmes dans l'industrie, pour l'évaluation de la conception et enfin l'amélioration des systèmes.

La méthode consiste à réaliser les combinaisons possibles des fautes ou pannes (défaillance des équipements, matérielles ou des logiciels, des défaillances de processus, erreurs humaines…) d'un système qui permettent l'occurrence d'un évènement indésirable prédéfini, et les représenter logiquement d'une manière graphique par une arborescence (schéma graphique en forme d'arbre inversé).

Cette méthode est complétée par un traitement mathématique qui permet de quantifier la probabilité d'apparition des défaillances et de l'évènement indésirable. [25]

2. Principe :

L'ADD est utilisé pour l'amélioration des systèmes, il permet de :

- Identifier les scénarios des défaillances élémentaires et trouvez les composants les plus probables de conduire la défaillance d'un système, ou à des accidents.

- Représente l'enchaînement logique des évènements des composants défaillants jusqu'à la panne de système pour une meilleure logistique.

- La possibilité de quantifier l'arbre et obtenir des chiffres qui représentent la fiabilité, taux de défaillance…

- Un outil d'analyse des systèmes qui permet de faire un diagnostic rapide lors qui il est établi.

- Une méthode préventive pour éviter les défaillances ou des changements de conception qui peut réduire le coût.

3. La construction de l'ADD :

L'ADD consiste en des évènements connectés par des portes logiques. Les évènements et les portes ont des symboles graphiques déférents, les évènements contiennent le mode de défaillance.

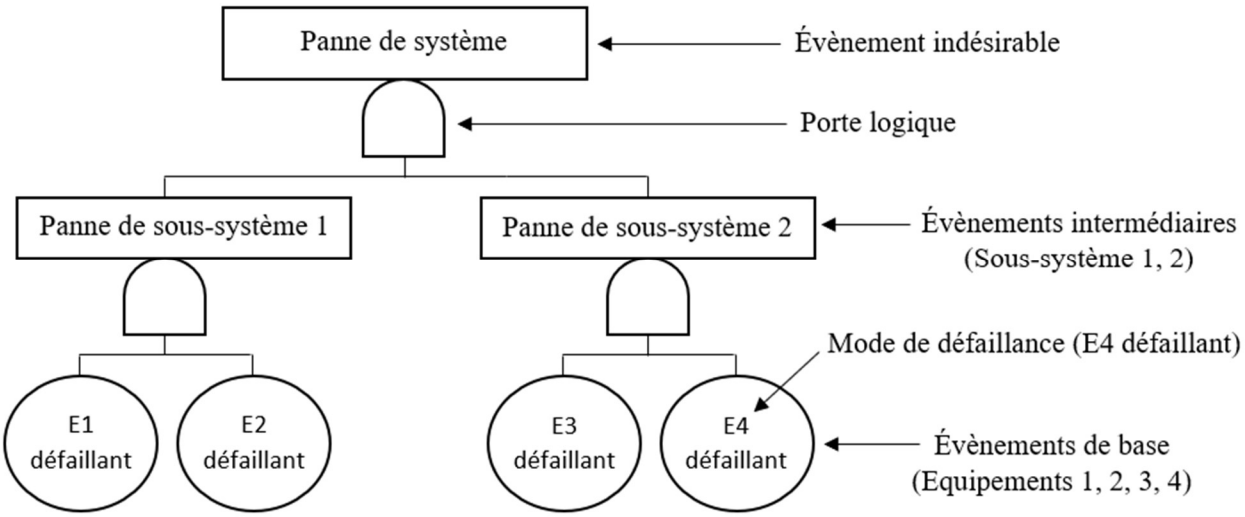


Figure 5 : Schéma représentatif de la construction de l'ADD

3.1. Les évènements :

Un événement représente le dysfonctionnement d'un ou plusieurs, et même tous les composants du système. Il est divisé en trois sections : redouté, intermédiaire, primaire.

L'ADD toujours contient un événement redouté et un ou plusieurs événements primaires, et peut être un ou plusieurs événements intermédiaires si nécessaire.

3.1.1. Evènement redouté (évènement indésirable) :

L'ADD commence par la définition de cet événement indésirable d'une façon explicite et précise, l'événement redouté, ou encore évènement sommet (top event) représente la panne de la fonction principale du système complet ou le sous-système étudié.

Cet événement est crucial et représente La ligne la plus haute de l'ADD.

3.1.2. Evènements intermédiaires :

Les évènements intermédiaires sont la combinaison des évènements moins globaux ou des sous-systèmes inclus dans le système étudié qui peuvent conduire à cet évènement sommet (représente la panne de la fonction du sous-système). Ces évènements intermédiaires peuvent être redéfinis par d'autres évènements intermédiaires plus détaillés. Ils ne sont ni en haut ni au bas de l'arbre.

Cet événement peut être négligé s'il n'y a pas de besoin.

3.1.3. Evènements primaire :

Ces événements sont les éléments de niveau le plus bas dans un diagramme d'ADD. Ils représentent les événements qui se produisent qui conduisent à des évènements de niveau supérieur, et finalement à l'évènement sommet.

Il existe déférents types d'événements primaire : Evènements de base, Maison, Non développé, Répété et conditions.

1- Evènement de base :

Les évènements de bases sont les évènements à la fin de l'ADD, ces évènements sont appelés évènements non développés, qu'il n'est pas utile de développer plus. Les informations sur lesquelles sont insuffisantes pour une autre décomposition (ne pas possible de les détailler). Ils concernent les défaillances (électrique, mécanique, logiciel, des erreurs humaines …) d'un élément du système.

Un événement de base termine une branche d'arbre de défaillance.

2- Événement maison (House) :

Un événement maison est utilisé pour permettre d'activer et de désactiver un événement. Il permet de fixer la probabilité de l'événement à 0 (ne se produira pas) ou à 1 (se produira). Les événements maison sont utilisés pour permettre à des parties d'un ADD d'être inclus dans l'analyse ou non, pour aider à analyser les effets de certaines branches individuellement.

3- Événement non développé :

Un événement non développé est similaire à un événement de base, c'est l'élément de niveau le plus bas dans un ADD. Mais l'événement non développé indique que l'événement pourrait être encore affiné et décomposé (résolution supplémentaire soit possible), cette résolution n'est pas importante pour l'analyse ou n'a pas d'impact sur l'analyse.

Elle est pu également être utilisée pour indiquer qu'une résolution supplémentaire sera effectuée à l'avenir, et l'événement Non développé est un espace réservé jusqu'à ce moment.

4- Événement répété :

Un événement répété est utilisé pour représenter le même événement de base à plusieurs locations dans le diagramme d'ADD. Des événements répétés permettent une analyse plus organisée et plus efficace.

5- Événement de conditionnement :

L'apparition de certains évènements (de base ou autres) peut avoir une conséquence à certaines conditions.

L'événement conditionnement est toujours utilisé en conjonction avec les portes d'inhibition (Connecteurs logiques ci-dessous). L'événement de conditionnement est l'événement qui doit se produire dans un ordre pour que la porte d'inhibition puisse éventuellement se produire.

3.2. Mode de défaillance :

Le mode de défaillance est le texte écrit dans les symboles des évènements qui montre comment et quand les évènements sont défaillants (l'occurrence de la panne) suivent les caractéristiques du système, les conditions de fonctionnement, et les contraintes opérationnelles.

Le mode de défaillance ne signifie pas toujours que le composant est endommagé, par exemple un interrupteur ouvert est considéré comme un mode de défaillance pour un système qui nécessite de l'électricité pour fonctionner.

Exemples des modes de défaillance
- Rupture - Vibration - Changement de position - Bloqué ouvert / fermé - Fuite - Ecoulement réduit - Fonctionnement après le délai - Ne démarre / arrête pas

Tableau 3 : Exemples des modes de défaillance

3.3. Connecteurs logiques :

Les connecteurs logiques (ou portes logiques) sont les liaisons entre les différentes branches ou évènements. Ils sont pour définir précisément le lien logique qui démontre la relation entre les évènements/les entrées qui conduit à la sortie.

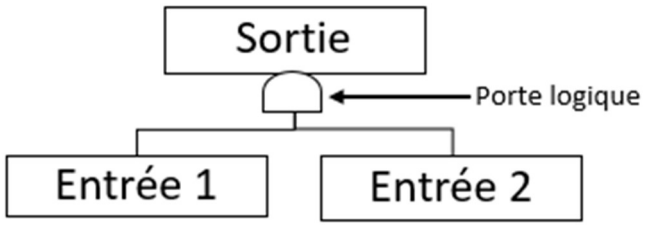


Figure 6 : Schéma de connecteur logique

Les portes :

Porte ET (AND), Porte OU (OR), Porte K/N (VOTE), Porte NOT, Porte NAND, Porte NOR, Porte XOR (Exclusive OR), Porte d'Inhibition, Porte ET prioritaire, Porte de transfert. [26] [27]

Les connecteurs fonctionnent comme suit :

1- Porte ET (AND) : la porte est utilisée lorsque l'évènement en sortie (supérieur) se survient seulement que si tous les évènements en entrées (inférieur) se surviennent.

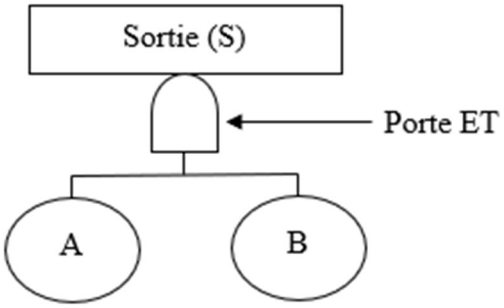


Figure 7 : Schéma de porte ET

L'expression logique : toutes les entrées doivent être vrai pour que la sortie soit vrai.

Tableau logique n°1 : Porte ET

Entrée 1	Entrée 2	Sortie
V	V	V
V	F	F
F	V	F
F	F	F

Tableau 4 : Tableau logique porte ET

V => Vrai : indique l'occurrence de défaillance ou de panne.

F => Faux : indique le fonctionnement (l'absence de défaillance).

Parfois, la défaillance est représentée par 1 dans les tableaux logiques au lieu de Vrai, et le fonctionnement par 0 au lieu de Faux.

L'expression Booléenne :

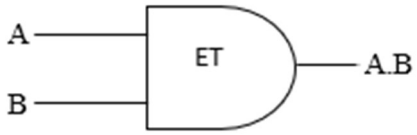


Figure 8 : L'expression Booléenne de la porte ET

S = A ET B = A.B

2- Porte OU (OR) : la porte est utilisée lorsque l'évènement en sortie (supérieur) se survient si un des évènements en entrées (inférieur) se surviennent.

L'expression logique : au moins une des entrées doit être vrai pour que la sortie soit vrai.

Tableau logique n°2 : Porte OU

Entrée 1	Entrée 2	Sortie
V	V	V
V	F	V
F	V	V
F	F	F

Tableau 5 : Tableau logique porte OU

L'expression Booléenne : S = A OU B = A+B

3- Porte K/N (VOTE) : c'est un vote majoritaire, la porte est utilisée lorsque l'évènement en sortie (supérieur) se survient uniquement si un nombre défini d'entrées K parmi les N évènements en entrées (inférieur) se surviennent. Les portes de vote sont désignées avec le nombre d'entrées requises K et le nombre total d'entrées N.

Cette porte généralise les deux portes précédentes : une porte OU est une porte 1/N et une porte ET est une porte N/N (mentionnée dans l'expression logique des portes ET et OU).

L'expression logique : la sortie est vrai uniquement si le nombre requis d'entrées K est vrai.

Tableau logique n°3 : Porte 2/3 (où 2 des 3 entrées doivent se produire pour que la sortie se produise)

Entrée 1	Entrée 2	Entrée 3	Sortie
V	V	V	V
V	V	F	V
V	F	V	V
V	F	F	F
F	V	V	V
F	V	F	F
F	F	V	F
F	F	F	F

Tableau 6 : Tableau logique porte K/N (Vote)

L'expression Booléenne : Porte 2/3 pour les trois entrées A, B, C

La porte dépend de l'expression logique, les situations possibles sont :

S = A ET B OU A ET C OU B ET C = A.B + A.C + B.C

4- Porte NOT : la porte est utilisée lorsque l'évènement en sortie (supérieur) se survient si l'évènement en entrée (inférieur) ne se survient pas. La porte NOT ne peut avoir qu'une seule entrée.

L'expression logique : si l'entrée est vrai, la sortie est faux. Si l'entrée est faux la sortie est vrai.

Tableau logique n°4 : Porte NOT

Entrée	Sortie
V	F
F	V

Tableau 7 : Tableau logique porte NOT

L'expression Booléenne : S = NOT A = $\overline{A}$

5- Porte NAND (NOT AND) : la porte est utilisée pour indiquer que l'évènement en sortie (supérieur) se survient si au moins un des évènements en entrées (inférieur) ne se survient pas. La porte NAND fonctionne comme une combinaison d'une porte ET(AND) et porte NOT.

L'expression logique : au moins une des entrées est faux pour que la sortie soit vrai.

Tableau logique n°5 : Porte NAND

Entrée 1	Entrée 2	Sortie
V	V	F
V	F	V
F	V	V
F	F	V

Tableau 8 : Tableau logique porte NAND

L'expression Booléenne : S = NOT (A ET B) = NOT (A) ET NOT (B) = $\overline{A.B}$

6- Porte NOR (NOT OR) : la porte est utilisée lorsque l'évènement en sortie (supérieur) se survient si tous les évènements en entrées (inférieur) ne se surviennent pas. La porte NOR fonctionne comme une combinaison d'une porte OU (OR) et porte NOT.

L'expression logique : si une entrée est vrai la sortie est faux.

Tableau logique n°6 : Porte NOR

Entrée 1	Entrée 2	Sortie
V	V	F
V	F	F
F	V	F
F	F	V

Tableau 9 : Tableau logique porte NOR

L'expression Booléenne : S = NOT (A OU B) = NOT (A) OU NOT (B) = $\overline{A+B}$

7- Porte XOR (Exclusive OR) : la porte est utilisée lorsque l'évènement en sortie (supérieur) se survient si un évènement en entrée (inférieur) ne se survient pas, et qu'un se survienne.

L'expression logique : si une, et une seule entrée est vrai la sortie est vrai.

Tableau logique n°7 : Porte XOR

Entrée 1	Entrée 2	Sortie
V	V	F
V	F	V
F	V	V
F	F	F

Tableau 10 : Tableau logique porte XOR

L'expression Booléenne : S = (A ET NOT B) OU (NOT A ET B) = $(A.\overline{B}) + (\overline{A}.B) = A \oplus B$

Le symbole $\oplus$ est un plus (+) dans un cercle pour représenter l'expression de la porte XOR et la porte X-NOR.

8- Porte X-NOR (Exclusive NOR) : la porte est utilisée lorsque l'évènement en sortie (supérieur) se survient si les deux évènements en entrée (inférieur) sont identiques, les deux évènements en entrées ne se surviennent pas ou les deux évènements en entrées se surviennent.

L'expression logique : si les deux entrées sont vrai ou les deux entrées sont faux la sortie est vrai.

Tableau logique n°8 : Porte X-NOR

Entrée 1	Entrée 2	Sortie
V	V	V
V	F	F
F	V	F
F	F	V

Tableau 11 : Tableau logique porte X-NOR

L'expression Booléenne : S = (A ET B) OU (NOT A ET NOT B) = $(A.B) + (\overline{A}.\overline{B}) = \overline{A \oplus B}$

Le symbole ⊕ est un plus (+) dans un cercle pour représenter l'expression de la porte XOR et la porte X-NOR.

9- Porte d'Inhibition : la porte est utilisée lorsque l'évènement en sortie (supérieur) se survient si tous les évènements en entrées (inférieur) se survient, et que la condition est remplie. Les portes d'inhibition sont toujours désignées avec une condition.

L'expression logique : si toutes les entrées et la condition est vrai la sortie est vrai.

Tableau logique n°9 : Porte d'Inhibition

Entrée 1	Entrée 2	Condition	Sortie
V	V	V	V
V	V	F	F
V	F	V	F
V	F	F	F
F	V	V	F
F	V	F	F
F	F	V	F
F	F	F	F

Tableau 12 : Tableau logique porte d'Inhibition

L'expression Booléenne : S = A ET B ET Con = A.B.Con

Con : est la condition

10- Porte ET prioritaire : la porte est utilisée lorsque l'évènement en sortie (supérieur) se survient si tous les évènements en entrées (inférieur) se surviennent dans un ordre particulier. Les portes ET prioritaire sont désignées avec un ordre de produire.

L'expression logique : si toutes les entrées doivent être vrai pour que la sortie soit vrai, et les entrées doivent se surviennent dans l'ordre.

Tableau logique n°10 : pour l'ordre de l'entrée 1 s'est produite en premier, l'entrée 2 s'est produite en second :

Entrée 1	Entrée 2	Sortie
V. produite en premier	V. produite en second	V
V. produite en second	V. produite en premier	F
V	F	F
F	V	F
F	F	F

Tableau 13 : Tableau logique porte ET prioritaire

11- Porte de transfert :

De nombreux outils de création de diagrammes d'arbres de défaillances utilisent également une porte de transfert, il n'y a pas de logique associée à une porte de transfert.

Lors de la construction de gros arbres de défaillances, il est pratique d'utiliser des portes de transfert, elle est peut-être utilisée pour diviser les grands diagrammes d'arbres de défaillances en sous-diagrammes pour l'organisation et la facilité d'utilisation. La porte de transfert représente un lien vers un autre diagramme d'arbre de défaillance complet qui est un enfant du diagramme parent. Ces portes signalent que la suite de l'arbre est développée sur une autre page permettant de rendre la lecture et la validation de l'arbre plus aisée.

Une porte de transfert peut également être utilisée pour représenter une logique répétée dans un diagramme. Par exemple, il peut y avoir plusieurs endroits où un événement particulier et sa branche apparaissent dans un diagramme. Vous pouvez décomposer cet événement et sa branche dans un sous-diagramme, puis le lier à ce sous-diagramme à l'aide d'une porte de transfert dans votre arbre de défaillance principal.

3.4. Symbole graphique :

Les symboles des évènements et des connecteurs logiques : [26] [27]

3.4.1. Symboles des évènements :

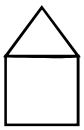
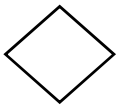
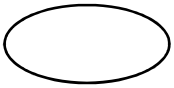
Symbole	Evènements
	Evènement redouté / intermédiaire
	Evènements de base
	Événement maison (House)
	Événement non développé
	Événement répété
	Événement de conditionnement

Tableau 14 : Symboles graphique des événements

Le symbole d'un événement répété est le même que celui d'un événement de base, l'événement répété est désigné par une couleur différente de celle d'un événement de base.

3.4.2. Symboles des Connecteurs logiques :

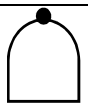
Symbole	Porte
	Porte ET (AND)
	Porte OU (OR)
	Porte K/N (VOTE)
	Porte NOT
	Porte NAND
	Porte NOR
	Porte XOR (Exclusive OR)
	Porte X-NOR (Exclusive NOR)
	Porte d'Inhibition
	Porte ET prioritaire
	Porte de transfert

Tableau 15 : Symboles graphique des portes

Le symbole de certaines portes peut varier selon la source.

4. Exemple d'un ADD :

L'analyse de système d'éclairage dans une salle de classe avec un événement redouté donné comme Absence d'éclairage :

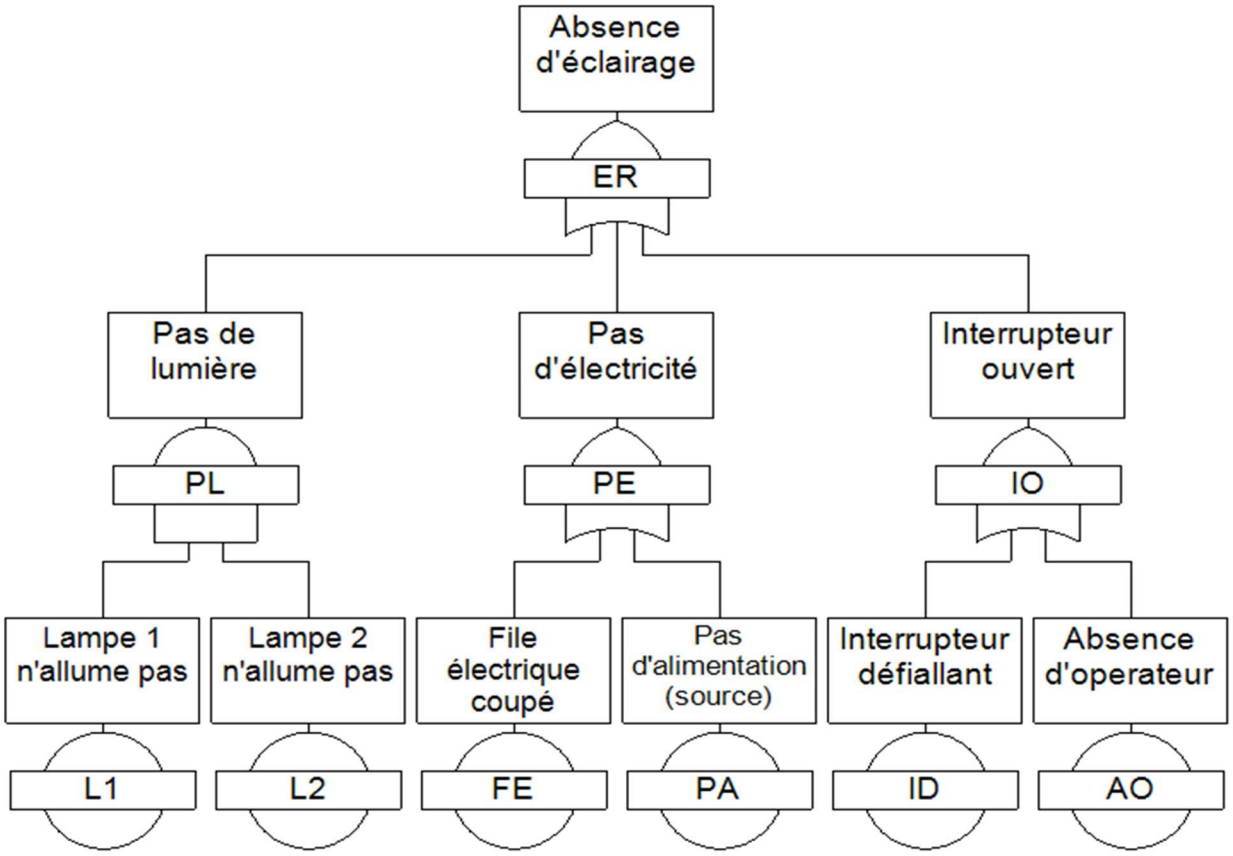


Figure 9 : Exemple d'un ADD

5. Les règles de construction :

- La définition des événements est notée par le mode de défaillance, et écrit dans le symbole de l'événement.

- Respecter les classements des événements qui conduisent à la panne (événement élémentaire à événements intermédiaires à l'événement sommet).

- Éviter la connexion directe de deux portes, mais créer un événement intermédiaire, il n'y a pas des règles à ajouter.

- Éviter les cycles logiques (un événement au-dessous lui-même, deux événements sous une porte ET).

- Dans les ADD cohérents tous les évènements inclus sont en mode de défaillance, et contribuent à l'évènement redouté.

- Il est préférable d'éviter l'incohérence.

6. Méthodologie :

Le principe est de décomposer le système en des sous-systèmes en relation avec les zones, les déférentes fonctions…, qui aide à la compréhension de système et facilite l'intervention rapide en cas de panne.

On crée des niveaux successifs, chacun des évènements (sous-systèmes) est une conséquence d'un ou plusieurs évènements du niveau inférieur.

6.1. Démarche :

- Le point de départ est l'évènement redouté (évènement sommet). Il est essentiel qu'il soit unique et bien identifier.

- Identifier l'ensemble des évènements intermédiaires (sous-système), et poursuivre niveau par niveau jusqu'aux évènements en combinaison d'évènements non décomposés (évènements de bases). Ces évènements sont le niveau inférieur de l'arbre.

- La ligne inférieure présentant les combinaisons susceptibles de produire l'évènement de la ligne supérieure.

- Pour la définition des évènements figurés dans l'arbre, un texte bref mais aussi apportant toutes les précisions utiles (mode de défaillance) pour définir ces évènements.

- Chaque combinaison d'évènements est connectée par des opérateurs logiques (portes). La porte choisie dépend de la relation entre les évènements.

6.2. Notions :

- On recommande l'utilisation exclusive des connecteurs ET, OU qui préserve la simplicité et permet de rester dans le cadre des ADD cohérents.

- Dans certaines situations il est pratique d'utiliser des connecteurs plus complexes comme des connecteurs voteurs, conditionnels…, pour traduire le comportement de système.

- Le même évènement sommet d'un ADD peut avoir plus d'une représentation.

- L'introduire des connecteurs NON, OU exclusif rend l'ADD dans la version non-cohérent et complexe le traitement mathématique.

7. Les analyses complémentaires :

La construction de l'arbre de défaillance est une phase importante de la méthode car sa complétude conditionne celle de l'analyse qualitative ou quantitative.

7.1. Analyse qualitative :

7.1.1. Définition :

Lors de la construction de l'ADD, des connaissances et une compréhension importante sont acquises concernant les causes de l'événement redouté, d'évaluations supplémentaires servent à affiner davantage les informations fournies par l'ADD.

L'ADD vise à identifier les relations fortuites entre les composants du système, lors de l'analyse qualitative toutes les causes possibles de défaillance du système sont identifiées, deux types d'exploitation qualitative peuvent être réalisés :

- Premièrement, l'ADD lui-même est une évaluation qualitative des événements et une analyse des différentes combinaisons de défaillances par l'identification des scénarios critiques qui conduisent à l'événement redouté ou à la défaillance du système.

- La deuxième évaluation qualitative fournit des informations plus ciblées sur les défaillances du système qui peuvent généralement se produire de plusieurs manières uniques, pour les ADD cohérente, chaque cause possible de défaillance du système est appelée un ensemble des coupes minimales, qui est une ou une combinaison de défaillance des composants capable de provoquer une défaillance du système. Les composants inclus dans les coupes sont des événements de base, si tous les événements de base dans les coupes se produisent, l'événement sommet est garanti de se produire.

Une fois un ADD est construit pour un système, le principal résultat qualitatif est l'obtention de l'ensemble des coupes minimales de l'événement sommet.

7.1.2. Les coupes minimales :

7.1.2.1. Définition :

L'une des sorties de l'ADD les plus utiles pour la conception et l'analyse de la fiabilité et de la sécurité est l'ensemble des coupes minimales qui peuvent définir les modes de défaillance, où un ensemble des coupes minimales est une collection d'événements de base qui peuvent provoquer l'événement sommet. Un ADD pour les systèmes industriels est généralement très grand et contient des milliers d'ensembles des coupes, et par une manipulation supplémentaire l'ensemble des coupes minimales sont obtenues, non seulement pour l'événement sommet mais aussi pour l'un des événements intermédiaires de l'ADD.

Un ensemble des coupes minimales ou un ensemble des défaillances minimales est les plus petites combinaisons possibles d'événements de base qui sont nécessaires et suffisantes pour produire une défaillance du système, si un événement de base est supprimé d'un ensemble des coupes minimales, l'événement supérieur ne se produira pas.

En d'autres termes, une coupe minimale est équivalente à la défaillance d'un événement de base.

Les coupes minimales sont déterminées par l'élimination des causes redondantes (l'élimination des coupes minimales répétées) dans un ensemble des coupes, ce qui conduit à une quantité importante d'informations :

- Un ordre d'une coupe minimale peut être obtenu pour identifier les points de vulnérabilité du système grâce à l'organisation des coupes.

- Une cause répétée est appelée une cause commune de défaillance.

- Un ADD simplifié, les ensembles des coupes minimales permettent la construction d'une version de taille réduite d'un ADD pour une compréhension, une visualisation et une analyse ultérieure potentielle plus faciles. Cette procédure est l'inverse de méthode d'obtention des coupes minimales (des coupes minimales vers l'ADD) sans la récupération des coupes minimales éliminé par cette méthode.

- Ajouter, ils peuvent également être utilisés pour évaluer la probabilité d'événements, la vulnérabilité et l'importance d'une coupe ou d'un événement de base spécifique dans une défaillance du système.

La propriété de l'ensemble des coupes minimales est qu'elles ne peuvent contenir aucune autre coupe. Elles sont suffisantes pour représenter la défaillance du système. [28]

7.1.2.2. Méthode d'obtention des coupes minimales :

L'ensemble des coupes minimales d'un ADD cohérent sont obtenues en convertissant la forme du diagramme en une expression logique pour l'événement sommet, ce processus connu comme l'approche descendante (The top-down approach) commence par la porte supérieure et étend chaque porte en substituant dans les entrées qui se trouvent directement en dessous, les entrées sont connectées par une expression de loi booléenne selon la porte qui a été remplacée.

Ce processus qui traduit l'ADD en équations booléennes est répété jusqu'à ce que l'expression ne comporte que des défaillances de composants de base. Les lois de l'algèbre booléenne sont également appliquées dans la mesure du possible pour simplifier l'expression en supprimant toute redondance dans l'expression en la laissant sous la forme minimale requise.

Autres méthodes peuvent être utilisées pour obtenir un ensemble des coupes minimales, telles que la méthode BDD…

Les lois de l'algèbre booléenne pour simplification :

Lois	Produit	Somme
Commutativité	$A.B = B.A$	$A+B = B+A$
Associativité	$(A.B).C = A(B.C) = A.B.C$	$(A+B)+C = A+(B+C)$ $= A+B+C$
Distributivité	$A.(B+C) = A.B+A.C$	$A+B.C = (A+B).(A+C)$
Idempotence	$A.A = A$	$A+A = A$
Absorption	$A.(A+B) = A$	$A+A.B = A$
Complément	$A.\overline{A} = 0$	$A+\overline{A} = 1$
Identités	$A.1 = A$	$A+0 = A$
Annulation	$A.0 = 0$	$A+1 = 1$
Négation (lois de DE Morgan)	$\overline{A.B} = \overline{A} + \overline{B}$	$\overline{A+B} = \overline{A}.\overline{B}$
Double négation	$\overline{\overline{A}} = A$	

Tableau 16 : Les lois de l'algèbre booléenne pour simplification

Exemple :

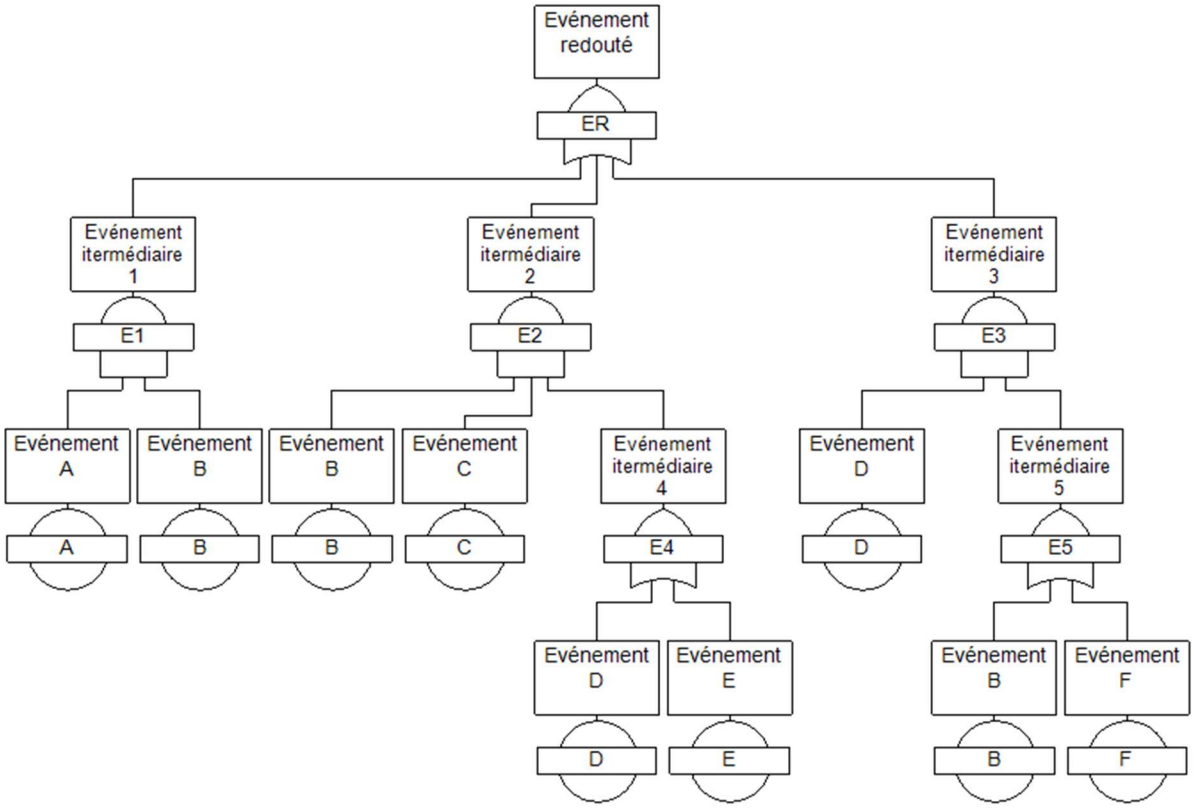


Figure 10 : Schéma d'un ADD pour l'obtention des coupes minimales

Les évènements intermédiaires :

E1 = A*B

E2 = B*C*E4

E4 = D + E

E3 = D*E5

E5 = B + F

L'équation de l'événement redouté :

ER = E1 + E2 + E3

ER = A*B + B*C*E4 + D*E5

ER = A*B + B*C*(D + E) + D*(B + F)

ER = A*B + B*C*D + B*C*E + D*B + D*F , B*C*D + D*B = D*B (loi d'absorption)

ER = A*B + B*D + D*F + B*C*E

ER = A*B + D*(B + F) + B*C*E

L'ADD simplifié :

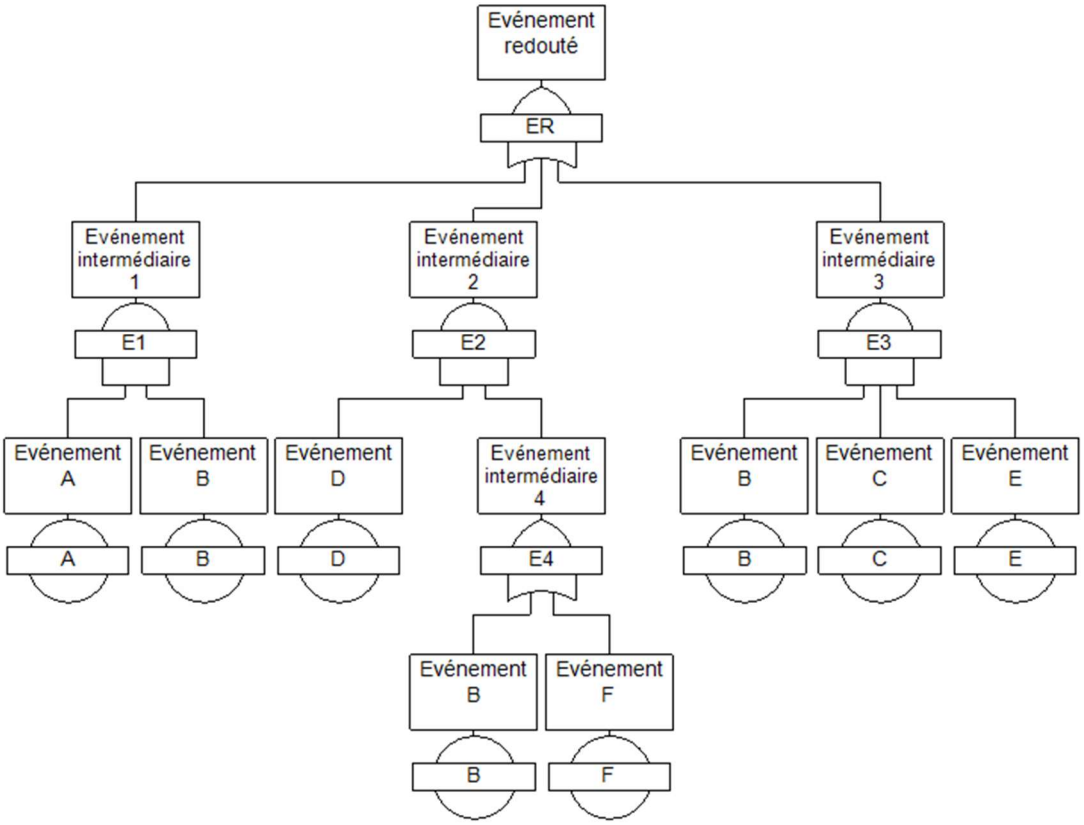


Figure 11 : Schéma d'un ADD simplifié

7.1.2.3. Ordre des coupes minimales :

Un ordre ou un cardinal d'une coupe minimale est déterminé par le nombre des composants dans l'ensemble des coupes minimales, l'ordre un représente une coupe minimale à un composant, ordre deux représente un ensemble de coupes minimales à deux composants. Généralement, l'ensemble des coupes minimales d'ordre inférieur est le plus susceptible de contribuer à la défaillance du système lorsqu'il exige moins des composants.

Un ensemble des coupes est les événements nécessaires pour conduire au résultat indésirable, le moindre ordre de l'ensemble des coupes représente le composant le plus vulnérable du système. Et ainsi, permettre que l'allocation des ressources soit priorisée en tant qu'objectifs d'amélioration de la sécurité et du système.

Certains systèmes critiques nécessitent au moins l'ordre deux (la combinaison des deux événements) ou plus.

Les coupes minimales d'ordre un représentent tous les événements de base capables de produire l'événement indésirable seulement, elles sont nommées un seul point de défaillance (Single point failure).

Considérer les coupes minimales du dernier exemple (Figure : ADD pour l'obtention des coupes minimales) :

ER = A*B + B*D + D*F + B*C*E

{A, B} ; {B, D} ; {D, F} : coupes minimales d'ordre 2 (parce que les coupes contiennent deux composants)

{B, C, E} : coupes minimales d'ordre 3

7.1.2.4. Un seul point de défaillance :

Un seul point de défaillance correspond à une coupe minimale d'ordre un, un ensemble des coupes minimales avec un seul événement de base identifié comme un seul point de défaillance (Single point failure), l'occurrence d'une défaillance ponctuelle unique peut à elle seule provoquer l'événement indésirable pour se produire.

Les seuls points de défaillance sont les plus préoccupants, Ils sont les défaillances du système les plus vulnérables. Un seul point de défaillance peut être un composant important sans lequel un système ne peut pas fonctionner, et souvent des connecteurs faibles (tuyaux, fils…), ou simplement une erreur humaine.

Les ingénieurs ciblent ces composants et se concentrent sur la mise à niveau ou la mise en place des mesures préventives pour éviter les accidents.

7.1.3. Cause commune de défaillance :

Un ensemble des coupes minimales ayant des événements (composants) identiques où les mêmes caractéristiques sont connues comme une cause commune de défaillance, qui peut impliquer une défaillance dépendante et annuler une redondance. C'est lorsque plus d'une fonction échoue (événement se produit) à la suite d'un seul événement initiateur.

7.1.4. Application qualitative :

Application sur la figure 1 :

L'equation :

ER = PL + PE + IO

ER = (L1 * L2) + (FE + PA) + (ID + AO)

ER = L1*L2 + FE + PA + ID + AO

Les coupes minimales :

FE, PA, ID, AO : coupes minimales d'ordre 1.

L1*L2 : coupes minimales d'ordre 2.

Résultats :

- FE, PA, ID, AO sont un seul point de défaillance puisque n'importe laquelle de leurs occurrences mène à l'événement sommet.

- L1, L2 sont des composants identiques, ils peuvent être une cause commune de défaillance.

7.2. Analyse quantitative :

Dans l'analyse quantitative on cherche à calculer la probabilité d'occurrence de l'événement redouté ER à partir des probabilités d'occurrence des événements de base, on fixe un instant t quelconque et on estime la probabilité d'occurrence de tous les évènements qu'on obtient d'après l'arbre de défaillance pour déterminer la probabilité de l'évènement redouté ER.

7.2.1. Calcul de probabilités d'occurrence :

Pour les calculs on doit convertir les portes logiques « ou », « et » à des opérations mathématiques :

- La porte logique « ou » devient un processus de combinaison entre les évènements :
  Exemple : $P(AUB) = P(A) + P(B) – P(A \cap B)$.
  Si A et B sont indépendantes ($P(A \cap B) = 0$) donc : $P(AUB) = P(A) + P(B)$.
- La porte logique « et » devient un processus de multiplication entre les évènements :
  Exemple : $P(A \cap B) = P(A) \times P(B)$.

Retour à l'exemple précédent :

ER = L1 X L2 + FE + PA + ID + AO.

Donc : P(ER) = P(L1) X P(L2) + P(PA) + P(ID) + P(AO).

Pour trouver les probabilités d'occurrence on besoins de taux de défaillance λ pour chaque composant peuvent tomber dans la défaillance.

Avec : $P(A) = \frac{\lambda_A}{\lambda_A + \mu}$

7.2.2. Calcul de la fiabilité R(t), de l'infiabilité F(t), de la disponibilité A(t) et de l'indisponibilité Q(t) :

1- La fiabilité R(t) :

La fiabilité d'un composant caractérise son aptitude à accomplir sa fonction :

$R(t) = 1 – (1 - e^{-\lambda t}) = e^{-\lambda t}$

2- L'infiabilité F(t) :

L'infiabilité est le complémentaire de la fiabilité : $F(t) = 1 - R(t) = 1 - e^{-\lambda t}$.

3- La disponibilité A(t) :

La disponibilité d'un composant caractérise son aptitude à être en état de fonctionnement à un instant t quelconque : $A(t) = 1 - \frac{\lambda}{\lambda+\mu}$.

4- L'indisponibilité Q(t) :

L'indisponibilité est le complémentaire de la disponibilité : $Q(t) = 1 - A(t) = \frac{\lambda}{\lambda+\mu}$.

Remarque :

Dans le cas d'un composant non réparable la fiabilité R(t) et la disponibilité A(t) sont équivalentes donc : $F(t) = 1 - R(t) = 1 - A(t) = Q(t)$.

7.2.3. La fiabilité de système $R_T(t)$:

_ La fiabilité d'un système mise en série représente la somme des fiabilités de ses composants $R_i(t)$: $R_T(t) = \sum_i^n R_i(t)$.

Pour un système avec des composants identiques : $R_T(t) = nR_i(t)$.

Avec n est le nombre total des composants.

_ La fiabilité d'un système mise en parallèle représente le produit des fiabilités de ses composants $R_i(t)$: $R_T(t) = \prod_i^n R_i(t)$.

Pour un système avec des composants identiques : $R_T(t) = R_i(t)^n$.

Avec n est le nombre total des composants.

7.2.4. Facteurs d'importance probabilistes (FIP) :

1- Facteur d'importance Marginale (Birnabaum) :

Appelé aussi le facteur d'importance de Birnabaum, il est considéré comme l'un des plus anciens facteurs d'importance connus, ce facteur peut être défini comme la probabilité pour

qu’un système S soit en état de fonctionnement avec i est un composant critique et le composant i est en fonctionnement :

$$Bi(t) = \frac{\delta Q(t)}{\delta qi(t)}$$

Avec :

qi(t) est la probabilité d’occurrence du composant i.

Q(t) est la probabilité d’occurrence du système.

Aussi on peut définir comme la variation de la fiabilité du système S en fonction de la fiabilité d'un composant i. [19]

Il est considéré comme l'un des plus anciens facteurs d'importance connus, ce facteur peut être défini comme la probabilité pour qu’un système S soit en état de fonctionnement avec i est un composant critique et le composant i est en fonctionnement. [19]

2- Facteur d’importance Critique (Lambert) :

Ce facteur est relié avec le facteur d'importance de Birnabaum, il représente la probabilité que le composant i ait provoqué la défaillance du système sachant que i est défaillant.

$$Ci(t) = \frac{qi(t)}{Q(t)} . \frac{\delta Q(t)}{\delta qi(t)}$$

$$Ci(t) = \frac{qi(t)}{Q(t)} . Bi(t)$$

Ce facteur peut aussi représenter la probabilité que la coupe minimale ait provoqué la défaillance du système sachant qu'il est défaillant (il indique le poids respectif de chaque coupe minimale dans la survenue de défaillance). [29]

Ce facteur nous aide à déterminer les éléments les plus influents sur la performance du système et quels éléments devraient être améliorés en priorité pour augmenter la fiabilité du système.

3- Facteur d'importance Diagnostic :

Appelé aussi le facteur d'importance de Fussel-Vesely est la probabilité que le composant i soit en panne sachant que le système est en panne.

$$VFi(t) = \frac{qi(t)}{Q(t)}$$

Ce facteur est très utile dans la hiérarchie des Activités Diagnostic. [30]

4- Facteur d'importance diagnostique pour les coupes minimales :

C'est la probabilité que la coupe minimale c ait provoqué la défaillance sachant que le système est défaillant. Il consiste à déterminer la capacité de chaque coupe minimale à la contribution de la défaillance du système. [31]

$$VFc(t) = \frac{Qc(t)}{Q(t)}$$

Avec :

Qc(t) est la probabilité d'occurrence du coupe minimale c.

8. Avantage et limite :

8.1. Avantage :

L'analyse par l'arbre de défaillance présente un certain nombre d'avantages par rapport aux autres méthodes :

- la forme graphique constitue un moyen efficace de représentation logique qui facilite la compréhension des systèmes.

- la méthode déductive permet de focaliser uniquement sur les événements contribuant à l'apparition des défaillances.

- l'orientation des événements.

- la considération des défaillances n'inclut pas seulement sur les composants, mais aussi les logicielles, des erreurs humaines, même la nature d'environnement.

- les deux types d'exploitation qualitative et quantitative de l'arbre qui permet de hiérarchiser les composants et déterminer les points faibles vulnérables du système.

- permet de réaliser des calculs rapides et exacts des variétés des probabilités.

8.2. Limite :

L'utilisation de l'arbre de défaillance est difficile lors des certains cas :

- l'indépendance des événements effectuer les calculs des probabilités.

- l'apparition des événements temporelle.

- l'anticipation des événements, tous les événements sont prévus pas atteint.

- la dégradation de l'état des composants, l'arbre considère l'état de fonctionnement et l'état de défaillance pas l'état intermédiaire.

- la taille de l'arbre des grands systèmes réduit la lisibilité et la compréhension, requis la division en sous-arbres et les transféré.

- le temps de construction, est coûteux lorsque les systèmes critiques sont définis avec prudence.

9. Logiciels des ADD :

L'analyse des ADD est possible par plusieurs logiciels, un logiciel d'analyse des ADD est un outil qui permet le dessin d'un ADD et le représentée graphiquement, et même signalé des erreurs de fausses constructions, il permet aussi d'attacher des données et des probabilités comme le taux de défaillance à chaque événement de basse.

Puis, le logiciel effectué l'analyse qualitative et quantitative et fournit les résultats, une analyse d'un ADD simple et petit est faite dans quelques secondes.

Il existe des variétés des logiciels, dont :

- Isograph

- Arbre analyste

- GRIF

10. Conclusion :

Un ADD ou FTA (Fault tree analysis en anglais) est une technique d'ingénierie utilisée dans l'industrie pour l'amélioration des systèmes.

L'ADD recueille les scénarios possibles des pannes du système, et représenter l'enchaînement logique des évènements graphiquement par une arborescence (schéma graphique en forme d'arbre inversé). Complétée par un traitement mathématique qui permet l'obtention des probabilités d'apparition de ces pannes du système.

L'ADD consiste en des évènements qui est le dysfonctionnement d'un ou plusieurs composants du système, ce dysfonctionnement est noté par un texte (mode de défaillance) montre comment et quand les évènements sont défaillants. Les évènements sont connectés par des liens logiques qui démontrent la relation entre elles appeler portes logiques. Les évènements et les portes à des symboles graphiques déférents.

La construction des ADD commence par la définition de l'évènement redouté, encore, la décomposition de système en des sous-systèmes pour identifier les évènements intermédiaires, et poursuivre niveau par niveau jusqu'aux évènements de basse. Puis, la connexion des évènements par des portes logiques selon la relation entre les évènements.

Cette construction est restreinte à certaines règles pour éviter l'incohérence et pour une meilleure conception.

Après la construction aussi appelée analyse qualitative qui permet de l'obtention de l'ensemble des coupes minimales pour identifier les points de vulnérabilité du système, un traitement mathématique ou analyse quantitative consisté de calcul de probabilités d'occurrence des défaillances des évènements.

Comme les autres méthodes, l'ADD à des avantages d'utilisation et des limites, et même des logiciels pour les modéliser.

CHAPITRE 3 :

Les arbres de défaillance non cohérents

1. Introduction :

Les arbres de défaillances sont classés selon leur fonction logique (portes), l'utilisation des portes ET et OU uniquement lors de la construction résultant un arbre de défaillance cohérent, et lorsque la logique NOT est utilisée ou directement impliquée (porte OU exclusif, XOR…) l'arbre de défaillance résultant est non cohérent.

L'introduction de la logique NOT dans un arbre de défaillance est généralement déconseillée car les états de défaillance des composants et les états de fonctionnement peuvent contribuer à la panne du système, ce qui rend les analyses qualitatives et quantitatives plus difficiles que les versions cohérentes du fait du manque de fourniture d'informations supplémentaires sur le système et son efficacité. De plus, la maintenance des systèmes non cohérentes est plus compliquée.

Mais il a été soutenu que la logique NOT est bénéfique dans certains cas et même essentielle pour une meilleure compréhension des systèmes complexes.

2. La porte NOT :

La porte NOT liée à un composant signifie que lorsque le composant fonctionne le système est dans l'état défaillant, et lorsque le composant tombe en panne le système est restauré à l'état non défaillant. Cela est généralement dû à une mauvaise construction.

La logique NOT étend le calcul pour obtenir les probabilités des défaillances, ce qui peut prendre du temps et ne pas être très efficace et augmenter le problème. Parce que la probabilité d'une négation de défaillance (fonctionnement) d'un événement est toujours proche d'un (P ($\overline{D}$) $\approx$ 1) qui peut être ignoré en toute sécurité en tant que composante fiable.

Autrement, la logique NOT est considérée comme essentielle [32] pour une analyse réussie et significative afin de représenter certains systèmes avec plus de précision et d'efficacité, comme dans le cas des systèmes multitâches affectée plusieurs opérations, ou dans certains cas pour la négation d'existence d'une condition qui pourrait produire dans le futur, ou lorsque les états de réussite des événements font partie intégrante de la technique d'analyse.

L'arbre de défaillance peut devenir cohérent si la logique NOT est éliminée de la structure de l'arbre, mais il est toujours préférable de revoir la conception plutôt que de recourir à la nécessité d'une modélisation non cohérente.

3. Non cohérence :

L'état du système ne change pas comme le font les conditions des composants en incluant la porte NOT, que l'état de fonctionnement d'un composant peut contribuer à la panne du système (sous-système 1, schéma suivant). Cela complique la compréhension du système puisque la réparation d'un composant défaillant peut conduire à une défaillance du système, et la défaillance d'un composant à une performance réussit du système.

An autre cas d'incohérence si l'ADD contient les deux états (fonctionnement/défaillance) d'un élément, par exemple un système qui comporte deux évènements comme une cause de panne où un évènement contient la défaillance d'un élément A et autres causes de défaillance, et l'autre évènement représente l'état de fonctionnement d'élément A et autres causes de défaillance.

Ces cas nous font perplexe dans la manière de traiter les éléments comme l'élément A, notamment en cas de panne parce que la réparation de cet élément A peut conduire à l'évènement indésirable lorsque l'état de fonctionnement d'élément A est conclu comme une cause de panne.

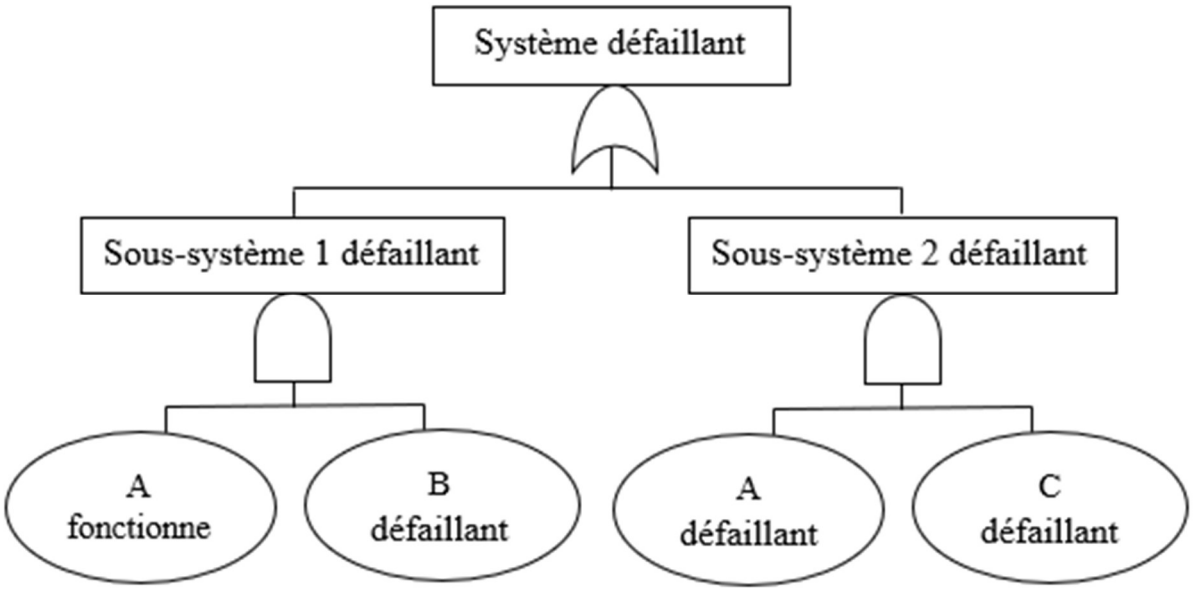


Figure 12: les cas de non cohérence

Afin d'améliorer les systèmes, l'ADD est destinée pour trouver les équipements vulnérables, l'amélioration de cet équipement est l'amélioration du système. L'amélioration est par la réparation des équipements endommagés ou par le remplacement des équipements faible par des équipements plus fiables qui prolongent le temps de fonctionnement. Dans des cas où le fonctionnement ou la réparation des équipements peut conduire à une panne du système crée une incohérence entre l'objectif des ADD et la méthode d'analyse.

Mais parfois l'incohérence facilite la compréhension, généralement pour les systèmes qui ont besoin d'un composant arrêté ou un évènement manquant afin de fonctionner. Pour un système compliqué qui affecté plusieurs opérations grâce aux composants utilisés, la bonne marche d'une opération ne se produit que lorsqu'une autre opération s'arrête, la négation de fonctionnement de cette opération est souhaitée pour un bon fonctionnement du système, et le fonctionnement de toutes les opérations en même temps peut conduire à un dommage indésirable.

Et aussi en sens large un mieux fonctionnement de certains systèmes est dû à l'absence des situations externe non souhaitée comme la pluie…, en cas de mauvais fonctionnement causé par ces situations les composants du système sont focalisés pour restaurer le bon fonctionnement, en négligeant ces situations externes car ils n'ont pas été inclus comme une cause de mauvais fonctionnement.

4. L'état de système en fonction d'état des composants :

L'état de système (fonctionnement/défaillance) se change de façon différente en fonction de changement d'état des composants de système pour une structure d'ADD cohérent et non cohérent.

4.1. Structure cohérente :

La structure d'un ADD cohérent augmente (non décroissante). Si l'état d'un composant X se détériore (de fonctionnement vers la défaillance), l'état du système Q reste le même ou se détériore également. Il y a trois possibilités [32] :

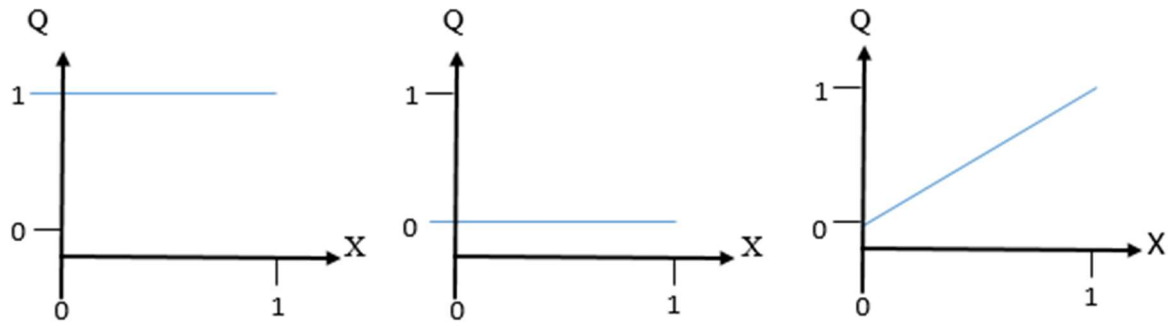


Figure 13 : Structure non décroissantes

0 = représente le fonctionnement , 1 = représente la défaillance

- La figure gauche : l'état de composant X se détériore (de 0 à 1), l'état du système Q reste le même en 1.

- La figure dans le milieu : l'état de composant X se détériore (de 0 à 1), l'état du système Q reste le même en 0.

- La figure droite : l'état de composant X se détériore (de 0 à 1), l'état du système Q se détériore également (de 0 à 1).

L'expression logique de la structure non décroissante [33] :

$Q(X=1) \geq Q(X=0)$

Et aussi pour certains composants :

$Q(X=1) \neq Q(X=0)$, comme la figure droite

4.2. Structure non cohérente :

La structure d'un ADD est non cohérente si le système Q est dans un état défaillant lorsque le composant X fonctionne, et qu'il est restauré dans un état de fonctionnement lorsque le composant X tombe en panne.

Voir la figure suivante [32] :

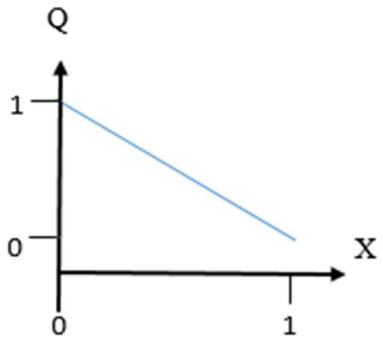


Figure 14 : Structure non cohérente

L'état de système Q est 1 lorsque l'état de composant X est 0, et l'état de système Q est 0 lorsque l'état de composant X est 1.

L'expression logique de la structure non cohérente :

$X \neq Q(X)$

5. Les causes de non cohérence :

La structure non cohérente est due à [32] :

- La nature des systèmes, certains systèmes exigent la négation d'un événement pour fonctionner comme une erreur humaine…, ou l'arrêt d'une ou plusieurs opérations.

- L'échec du système dans certaines circonstances, comme la redondance où un événement de base participe dans plusieurs combinaisons de défaillance induisent à la panne du système ou plusieurs coupes minimales.

- La mauvaise conception d'un système.

6. Exemples des ADD non cohérents :

1. Alimentation électrique : [34]

La probabilité de fonctionnement d'une alimentation électrique placée en extérieur est considérablement plus faible dans une situation de temps orageux, ignorer la négation de cette situation entraîne une analyse quantitative incorrecte.

2. Débordement d'un réservoir de stockage de produit liquide :

Analyse d'un débordement d'un réservoir alimenté en produit liquide :

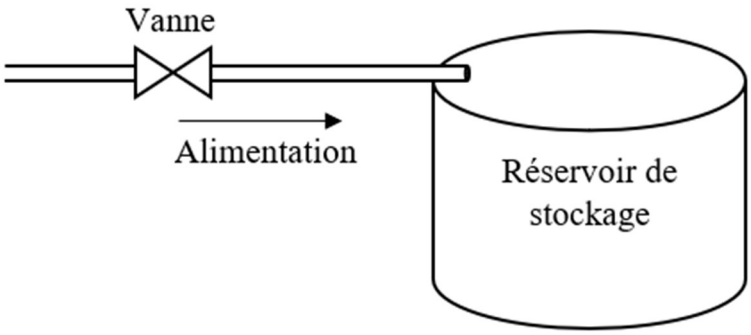


Figure 15 : Système de stockage de produit liquide

Le débordement est dû à deux causes :

- L'alimentation en produit liquide n'arrête pas (vanne bloquée ouverte)

- L'absence des dommages (défaillances) au niveau du réservoir comme une fuite…, qui est le bon état de réservoir

La deuxième cause n'apparaitre pas dans les ADD cohérent parce que c'est la négation de défaillance (mode de fonctionnement).

L'apparaitre de cet événement aide le concepteur à concentrer non seulement sur l'arrêt d'alimentation, mais sur le réservoir aussi comme ajouter un point de décharge pour limiter la perte de produit en connectant le point de décharge à un autre moyen de stockage si le produit est cher, ou pour contrôler le sens de perte de produit pour les produits dangereux ou salissants…

3. Fuite d'huile : [34]

La fourniture du système par l'huile est faite par une canalisation (tuyaux) connectée au réseau d'alimentation (stockage) de cette huile :

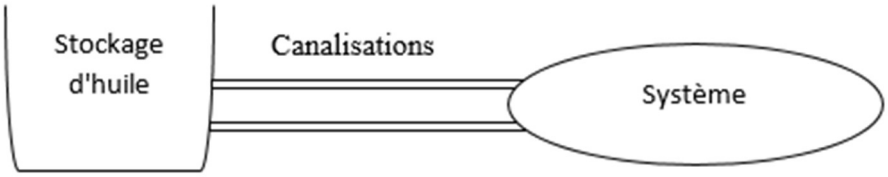


Figure 16 : Schéma de système d'huile

L'analyse d'une fuite liée à un tuyau endommagé est comme suit :

- Une fuite d'huile est due à un tuyau endommagé, cette simplification est une représentation cohérente du système.

- Lorsque la représentation non cohérente est une fuite d'huile est due à un tuyau endommagé et la négation de défaut de fournir d'huile ou la négation d'arrêt d'alimentation (fournir d'huile).

La représentation cohérente impose le concepteur la réparation du tuyau comme une solution unique pour arrêter la fuite puisque c'est la seule cause de la fuite.

La représentation non cohérente aide le concepteur à empêcher la fuite d'huile en coupant l'alimentation en huile lorsque le tuyau est endommagé et maintenir le stock d'huile, et à améliorer le système en ajoutant un outil pour couper l'alimentation en huile dans de telles situations.

4. Le système de feux tricolores : [33]

Considérez que les voitures A, B et C approchent une intersection :

A et B approchent l'intersection avec le feu rouge et doivent s'arrêter, et la voiture C a la priorité de continuer.

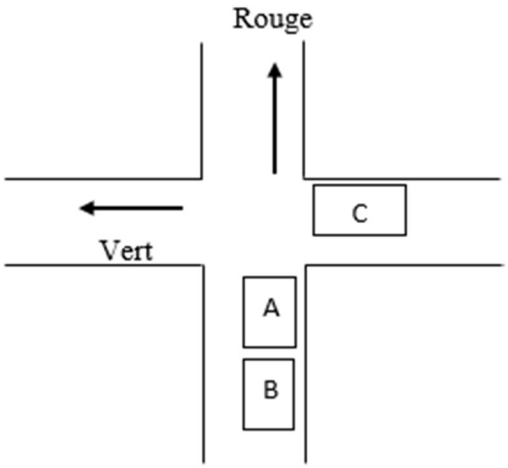


Figure 17 : Schéma de système de feux tricolores

L'événement redouté (ER) est noté : la collision

La collision peut se produire de manières suivantes :

1- Collision entre A et C :

Si la voiture A ne parvient pas à s'arrêter ET la voiture C ne parvient pas à continuer.

2- Collision entre A et B :

Si la voiture A s'arrête (la négation de A) ET la voiture B ne parvient pas à s'arrêter.

3- Collision entre A et B ou A et C :

Si la voiture B ne parvient pas à s'arrêter ET la voiture C ne parvient pas à continuer.

Dans cette situation l'état de A (fonctionnement/défaillance) n'a pas d'importance, il y aura une collision (événement redouté), soit :

A fonctionne : Collision entre A et B

A défaillant : Collision entre A et C

Et même en négligeant la situation 3, la combinaison des situations 1 et 2 dans un ADD lui permettent de contenir les deux états de A (fonctionnement/défaillance).

L'ADD :

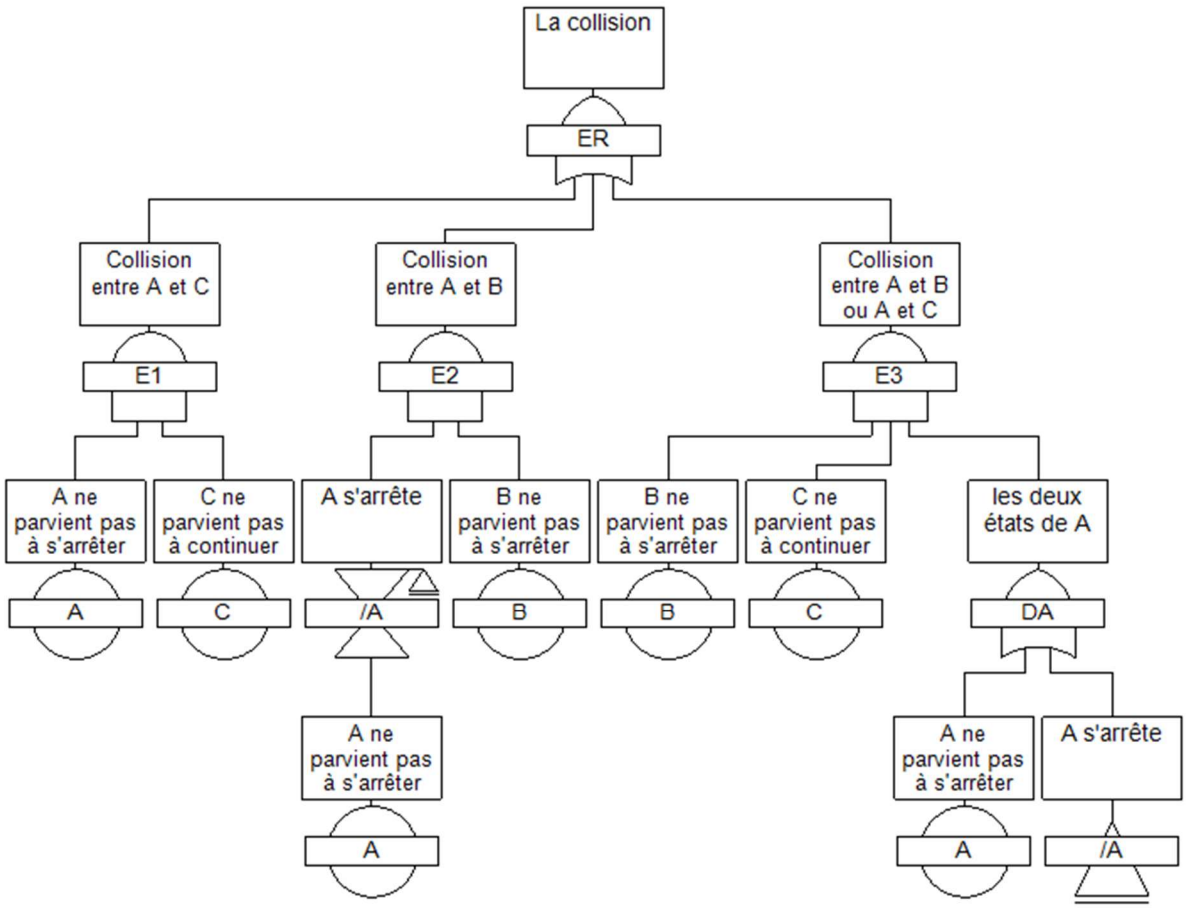


Figure 18 : Schéma de l'ADD-La collision

5. système de mélange des produits :

Considérez le système suivant :

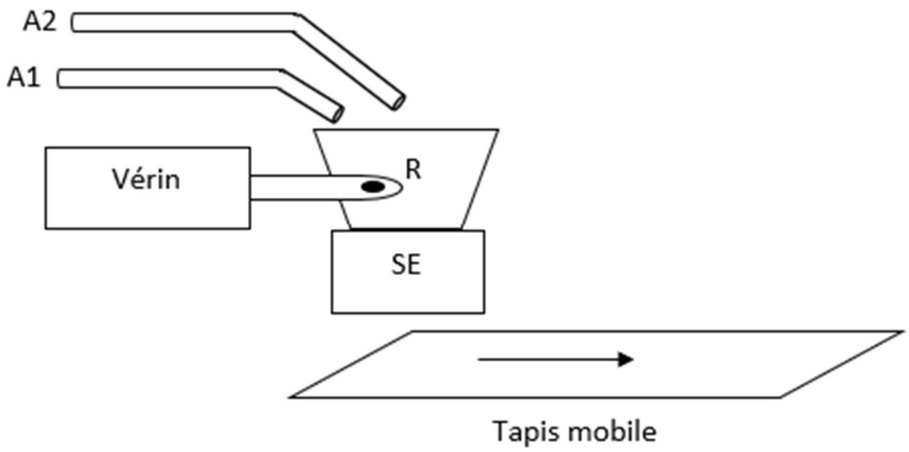


Figure 19 : Système de mélange des produits

Le produit final est au débit un mélange de deux produits alimentés à travers la canalisation A1, et A2.

A1 et A2 fonctionne alternativement : A1 fonctionne lorsque A2 est arrêté pour remplir le récipient R jusqu'à un poids prédéfini mesuré par la solde électronique SE, et arrêtez.

Puis, A2 remplit le récipient R jusqu'à un poids maximal prédéfini mesuré par la solde électronique SE, et arrêtez.

Le vérin (V) tourner le récipient pour vider sur le tapis mobile (T) qui transporte le mélange pour d'autres manipulations.

Une situation de défaillance :

Une erreur sur le produit peut apparaitre lorsque A1 et A2 fonctionne ou arrête dans le même temps, avec le fonctionnement de tous les autres composants :

L'arrête de A1 et A2 dans le même temps mené à un manque de produit, et le fonctionnement aux mauvaises mesures de mélange.

Dans cette situation, le fonctionnement de tous les autres composants n'a aucun effet sur le fonctionnement du système.

La connexion entre A1 et A2 est démontrée par la porte X-NOR (3.3. Connecteurs logiques).

L'ADD :

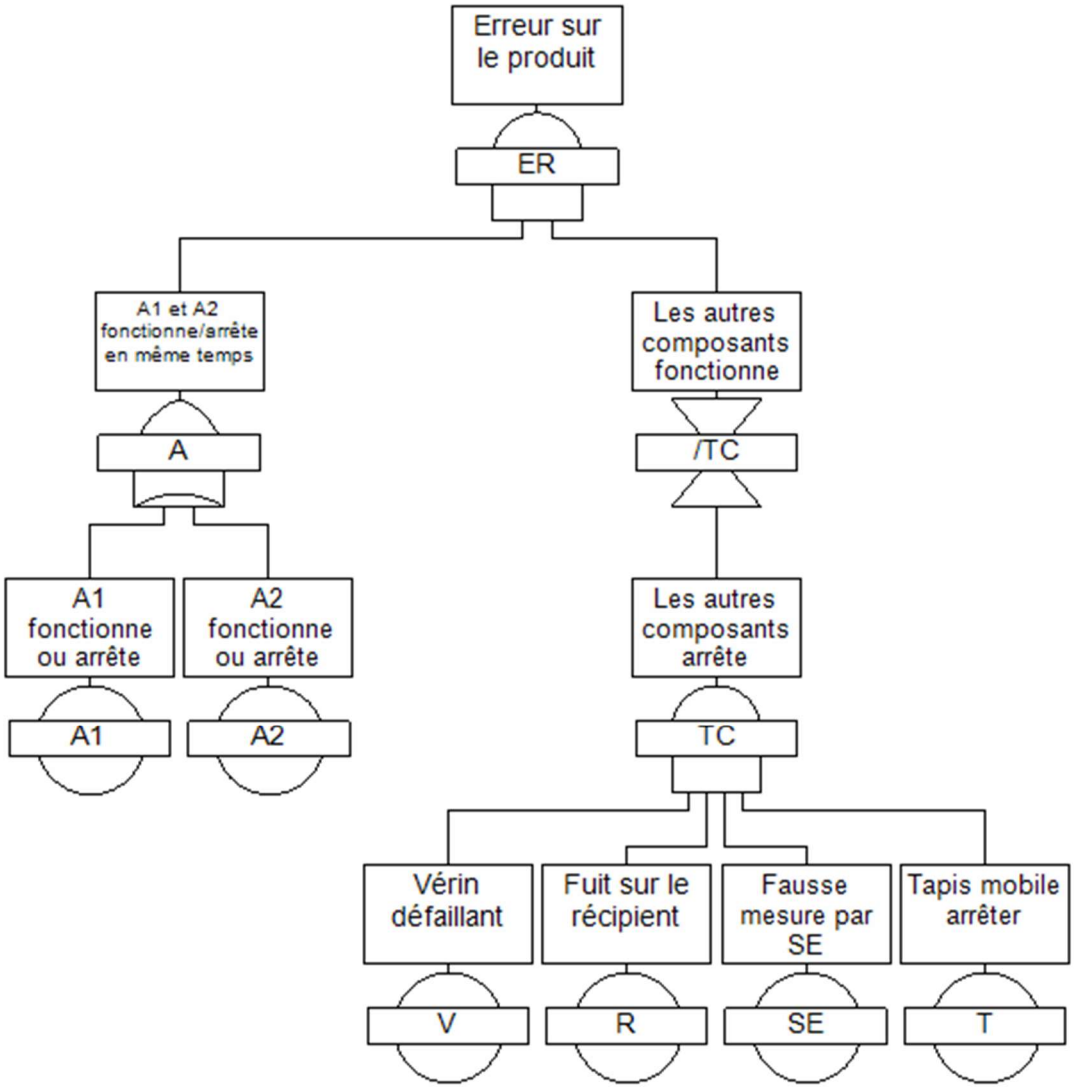


Figure 20 : Schéma de l'ADD-Système de mélange des produits

7. Analyse qualitative :

7.1. Description :

Étant donné que l'ADD lui-même est une évaluation qualitative, sa construction qui est la même que la version cohérente avec la déférence d'inclure la logique NOT signifie que toutes les causes possibles de panne du système sont identifiées.

Parce que l'ADD non cohérent contient les deux états de défaillance et de fonctionnement comme des causes de panne du système, toutes les causes sont référencées comme des ensembles des impliquants premiers.

7.2. Les impliquants premiers :

Une combinaison de défaillance des composants qui conduisent à une défaillance du système est appelée un ensemble des coupes minimales pour les ADD cohérents. Pour les ADD non cohérents, une défaillance du système est possible à la fois par l'état de défaillance et l'état de fonctionnement du composant, chaque cause possible de défaillance du système est appelée un ensemble des impliquants premiers (prime implicant set).

7.3. L'obtention des impliquants premiers :

Pour les systèmes industriels qui contiennent un grand nombre des impliquants premiers le traitement est fait par un logiciel pour la détermination des ensembles des impliquants premiers.

Pour les systèmes petits où le traitement est fait manuellement (sans logiciel), l'identification des ensembles des impliquants premiers nécessite la conversion de la structure de l'ADD en version cohérente en éliminant la logique NOT, en tant que suppression de la logique NOT, des méthodes telles que l'approche descendante pour un ADD cohérent sont appliquées pour déterminer les ensembles des impliquants premiers.

L'obtention des impliquants premiers est possible par plusieurs procédures.

7.3.1. La substitution de la porte NOT :

Toutes les portes NOT doivent être éliminées [32]. Pour identifier les impliquant premiers, il est d'abord nécessaire de s'assurer que la structure de l'arbre de défaillance ne contient que des portes ET et OU.

1- La porte NOT est poussé vers le bas de l'arbre jusqu'aux événements de base, en substituant la porte dans les entrées qui se trouvent directement en dessous en utilisant les lois de De-Morgan : $\overline{A + B} = \overline{A}.\overline{B}$; $\overline{A.B} = \overline{A} + \overline{B}$

Un exemple d'élimination de la porte NOT :

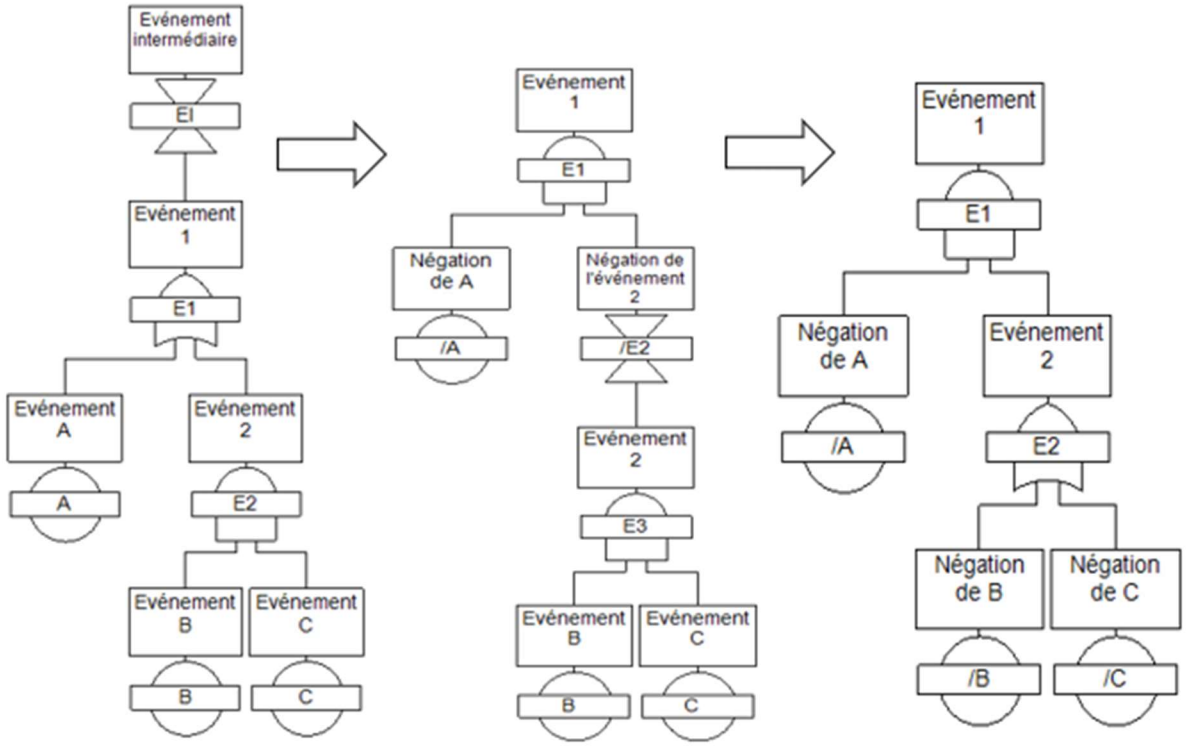


Figure 21 : Elimination de la porte NOT

2- Une fois la porte NOT est éliminée, l'approche descendante est appliquée. Cependant, il ne produira pas une liste complète des impliquants premiers. Le reste des impliquants premiers peut être identifié en appliquant la loi de consensus : $\overline{A}X + AY = \overline{A}X + AY + XY$

Un exemple d'utilisation de la loi de consensus :

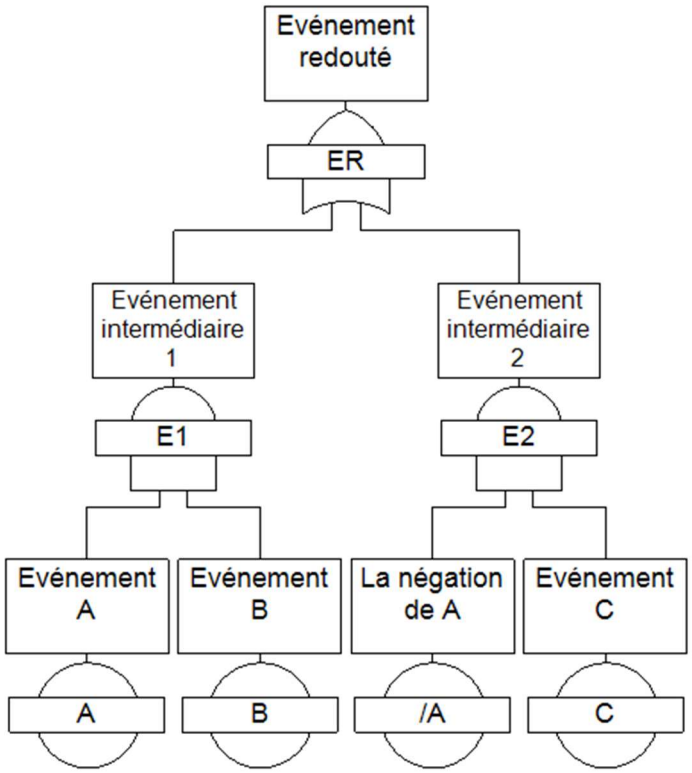


Figure 22 : utilisation de la loi de consensus

L'équation de l'événement redouté :

ER = E1 + E2

ER = A*B + $\overline{A}$*C

En applique la loi de consensus :

ER = A*B + $\overline{A}$*C + B*C

Les impliquants premiers sont identifiés.

Cette technique est pour les ADD simple comme celle-ci où l'on peut faire le calcul manuellement, mais il peut ne pas identifier exactement les impliquants premiers pour les arbres les plus grands et complexes.

Dans de tels cas, une approximation cohérente peut être obtenue en utilisant l'approche descendante en identifiant uniquement les parties positives des impliquants premiers connues sous le nom de coupes P minimales, et toutes les parties négatives sont ignorées en les supprimant de l'expression d'événement sommet.

L'obtention des coupes P minimales pour l'exemple précédent (Figure 11) :

E1 = A*B

E2 = $\overline{A}$*C ; $\overline{A}$ est ignorée => E2 = C

ER = E1 + E2

ER = A*B + C

8. Analyse quantitative :

La quantification des ADD non cohérents ne tient pas les mêmes méthodes utilisées dans les ADD cohérent, car elles ne prendront pas en compte les cas entraînant une défaillance du système.

8.1. Calcul de la probabilité de l'événement sommet :

La méthode d'expansion inclusion-exclusion utilisé pour calculer la probabilité de l'événement sommet dans les arbres de Défaillance cohérent, elle a été modifiée par Inagaki et Henley pour devenir approprié de calculer la probabilité d'occurrence de l'événement indésirable. Inagaki et Henley ont proposé l'équation suivante pour faire le calcul : [32]

$$Q_{sys}(t) = \sum_{i=2}^{n} \sum_{j=1}^{i-1} P(\varepsilon_i \cap \varepsilon_j) + \ldots + (-1)^{n-1} P(\varepsilon_1 \cap \varepsilon_2 \cap \varepsilon_n)$$

Où, $P(\varepsilon_i)$ représente la probabilité que l'impliquant premier i existe en instant t, avec :

$$P(\varepsilon_i) = \prod_{j=1}^{np} q^{\alpha_j}(t)$$

np désigne le nombre d'événements de base dans un impliquant premier donné :

q^{aj} = qj(t) si α = 1 c'est à dire j apparaît.

= 1- qj(t) si a = 0 c'est à dire j/ apparaît.

Notons que : $A.\overline{A} = 0$

8.2. L'extension des facteurs d'importance probabilistes aux ADD non cohérents :

Lorsqu'il s'agit d'un système cohérent, une défaillance du système ne peut être provoquée que par une défaillance des composants. Par conséquent, un composant dans un système cohérent ne peut être critique que des défaillances. Cependant, lorsqu'il s'agissait d'un système non cohérent, une défaillance du système peut être provoquée non seulement par défaillance de composants appelée événement i, mais également par réparation de composants appelée événement i/, Ainsi, un composant dans un système non cohérent peut être critique s'il est défaillant ou réparer. Ces deux critiques doivent être considérées séparément car le composant i peut exister dans un seul état à tout moment. [32]

Dans ce cas le facteur d'importance marginale peut être calculé comme suit :

Bi(t) = BiF(t) + BiR(t)

$$Bi(t) = \frac{\delta Q(t)}{\delta qi(t)} + \frac{\delta Q(t)}{\delta(1-qi(t))}$$

Avec :

BiF(t) : est la probabilité que le composant i est défaillant critique.

BiR(t) : est la probabilité que le composant i est réparé critique.

1- Le facteur d'importance critique :

Lors de l'analyse d'un arbre de défaillance non cohérent, la défaillance des composants et la réparation des composants peuvent entraîner une défaillance du système.

Parce que CIF est défini sur la base de facteur de Birnabaum, la criticité de défaillance et la criticité de la réparation peuvent être écriées séparément comme suit : [33]

$$Ci(t) = CiD(t) + CiR(t)$$

$$Ci(t) = BiD(t)\frac{qi(t)}{Q(t)} + BiR(t)\frac{1-qi(t)}{Q(t)}$$

Avec :

CiD(t) : la probabilité que le composant i est défaillant critique pour le système et est dans un état de dysfonctionnement pondéré par l'indisponibilité du système.

CiR(t) : la probabilité que le composant i est le succès (réparation) essentielle au système et est dans un état de fonctionnement pondéré par l'indisponibilité du système.

2- Le facteur d'importance diagnostique pour les composants :

Dans les arbres de défaillance non cohérent le facteur d'importance diagnostique est défini comme suit : [32]

L'importance de la défaillance de Fussel-Vesely est la probabilité que la défaillance de composant i contribue à la défaillance du système :

$$VFi(t) = \frac{qi(t)}{Q(t)}$$

Avec :

q(t) : l'indisponibilité de composant i à l'instant t.

Q(t) : l'indisponibilité de système à l'instant t.

Et l'importance de la réparation de Fussel-Vesely est la probabilité que la réparation (état de fonctionnement) de composant i contribue à la défaillance de système :

$$VFi(t) = \frac{1-q\ (t)}{Q(t)}$$

Avec :

q(t) : l'indisponibilité de composant i à l'instant t.

Q(t) : l'indisponibilité de système à l'instant t.

3- Facteur d'importance diagnostique pour les impliquants premiers :

C'est la probabilité que l'impliquant premier ε ait provoqué la défaillance du système. [32]

$$VFi(t) = \frac{Q\varepsilon(t)}{Q(t)}$$

Avec :

Qε(t) est la probabilité d'occurrence d'impliquant premier ε.

9. Autres procédures de non cohérence :

Des procédures permettant d'examiner les ADD non cohérents et d'obtenir les ensembles d'impliquants premiers, et que certaines n'ont pas besoin d'ensembles des impliquants premiers et conduisent directement au calcul de la probabilité des défaillances.

9.1. Combinaison logique des sous arbres monotones :

Une méthode simple pour un arbre de défaillance non cohérent [30], l'événement sommet d'un ADD peut être représentée comme une combinaison logique de ET ou OU porte des sous arbres monotones (monotonic sub-trees), ou simplement des sous arbres cohérents.

Monotone signifie que le sous arbre :

- contient uniquement des portes logiques ET et OU.

- n'a pas les deux représentations positive et négative pour un événement de base, un événement de base peut apparaitre avec l'état de fonctionnement dans un sous arbre et comme défaillant dans un autre.

De cette signification la négation d'un sous arbre monotone est monotone.

Certaines transformations sont nécessaires dans les étapes intermédiaires en fonction de certaines propriétés.

9.1.1. Combinaison logique de ET porte des sous arbres monotones :

Chaque sous arbre contient seulement le mode de fonctionnement ou le mode de défaillance des composants, cela signifie que chaque sous arbre sous l'événement sommet est monotone et que l'arbre de défaillance est non monotone.

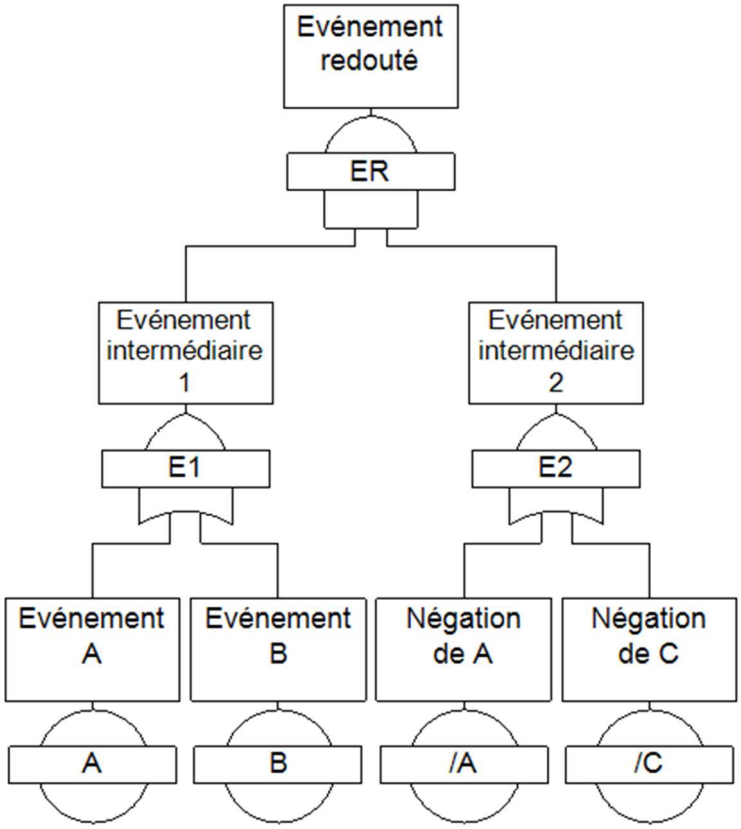


Figure 23 : Combinaison logique de ET porte des sous arbres monotones

Les ensembles des coupes minimales de chaque sous arbre peuvent être obtenus en utilisant des méthodes conventionnelles pour les ADD cohérents. Puis, les coupes minimales pour l'événement redouté (l'ADD entier) sont représentées comme un ET combinaison des coupes minimale des sous arbres, avec une condition que chaque sous arbre doit contenir au moins une coupe minimale pour satisfaire le terme de conjonction (opération logique de ET porte).

Les coupes minimales sont obtenues sans l'utilisation des lois des consensus :

Les coupes minimales de chaque sous arbre monotone :

E1= A+B

E2 = $\overline{A}$+$\overline{C}$

Les ensembles des coupes minimales pour l'ADD entier :

ER = E1*E2

ER = (A+B)*($\overline{A}$+$\overline{C}$)

ER = A*$\overline{A}$ + A*$\overline{C}$ + B*$\overline{A}$ + B*$\overline{C}$

ER = A*$\overline{C}$ + B*$\overline{A}$ + B*$\overline{C}$

Les coupes minimales : {A ; $\overline{C}$}, {B ; $\overline{A}$} , {B ; $\overline{C}$}

9.1.2. Combinaison logique de OU porte des sous arbres monotones :

Une combinaison logique de OU porte des sous arbres monotones :

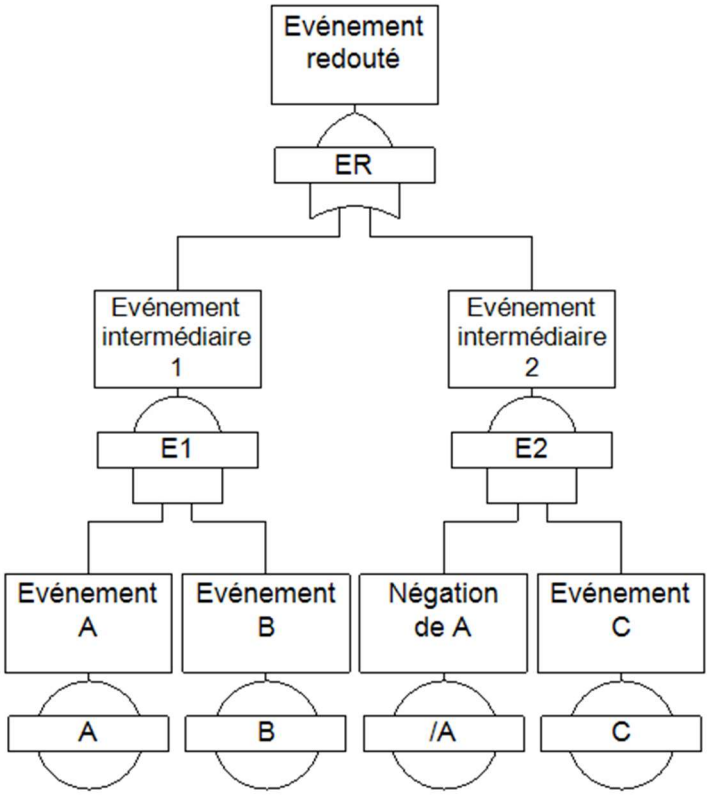


Figure 24 : Combinaison logique de OU porte des sous arbres monotones

Combinaison logique de OU porte des sous arbres monotones :

ER = E1 + E2

ER = A*B + $\overline{A}$*C

- L'obtention de la négation d'une combinaison logique de OU porte des sous arbres monotones qui est une Combinaison logique de ET porte des sous arbres monotones :

$\overline{ER} = \overline{E1}*\overline{E2}$

$\overline{ER} = (\overline{A} + \overline{B})*(A + \overline{C})$

- L’obtention des coupes minimales de cette négation :

$\overline{ER} = \overline{A}*A + \overline{A}*\overline{C} + \overline{B}*A + \overline{B}*\overline{C}$

$\overline{ER} = \overline{A}*\overline{C} + \overline{B}*A + \overline{B}*\overline{C}$

- L’obtention de la négation des coupes minimales :

$ER = \overline{\overline{ER}} = (A + C)*(B + \overline{A})*(B + C)$

- L’obtention des coupes minimales lorsque la négation d’un sous arbre monotone est monotone :

$ER = (B + \overline{A})*(A*B + C)$ (Lois de distributivité)

$ER = A*B + B*C + \overline{A}*C$

Les coupes minimales : {A ; B}, {B ; C} , {$\overline{A}$; C}

9.2. Diagramme de décision binaire (BDD) :

Le BDD (Binary Decision Diagram) est une méthode efficace qui est utilisée pour le pronostic des systèmes, pour prédire les défaillances et le succès du système qui sont utiles dans le processus de prise de décision.

L’ADD est converti en BDD pour surmonter certaines difficultés conventionnelles dans l'analyse qualitative et quantitative des ADD cohérents et non cohérents, le BDD ajoute également un autre degré d'efficacité si l’ADD est simplifié à la forme minimale avant la conversion en BDD.

Le processus de conversion des ADD en BDD représente la fonction de structure (structure function en anglais) du système ou un SFBDD, et ne nésite pas l’obtention des ensembles des impliquants premiers.

Le BDD est peut ensuite être utilisé pour quantifier les paramètres de défaillance du système, mais ne convient pas pour produire une liste complète des impliquants premiers.

Considérer le système de transport de gaz en pression : [35]

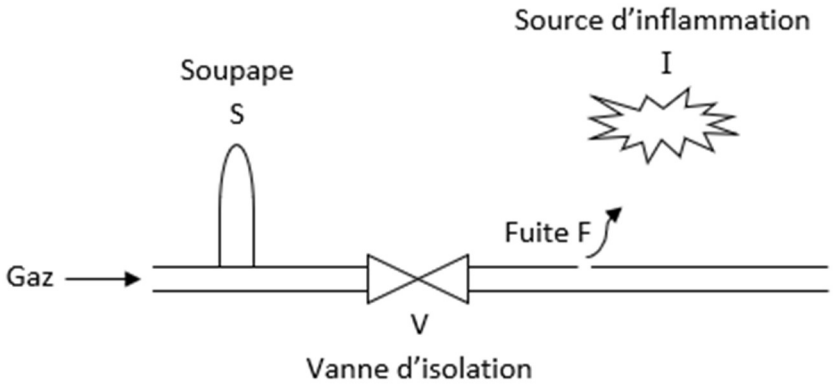


Figure 25 : Système de transport de gaz en pression

En cas de fuite F après la vanne d'isolation V, le système de détection fermer la vanne d'isolation V pour empêcher l'explosion de gaz a causse du contact avec la source d'inflammation I, cela conduite à une augmentation de pression sur la canalisation, l'explosion par cette augmentation de pression est évitée par une soupape S.

L'explosion est possible :

- Avant la vanne d'isolation V : la fuite oblige le système de détection de fermer la vanne d'isolation V (fonctionnement de V), mais la soupape S échoue à démener l'augmentation de pression.

- Après la vanne d'isolation V : le système de détection échoue à fermer la vanne d'isolation V (défaillance de V), et la fuite contact la source d'inflammation I.

L'ADD :

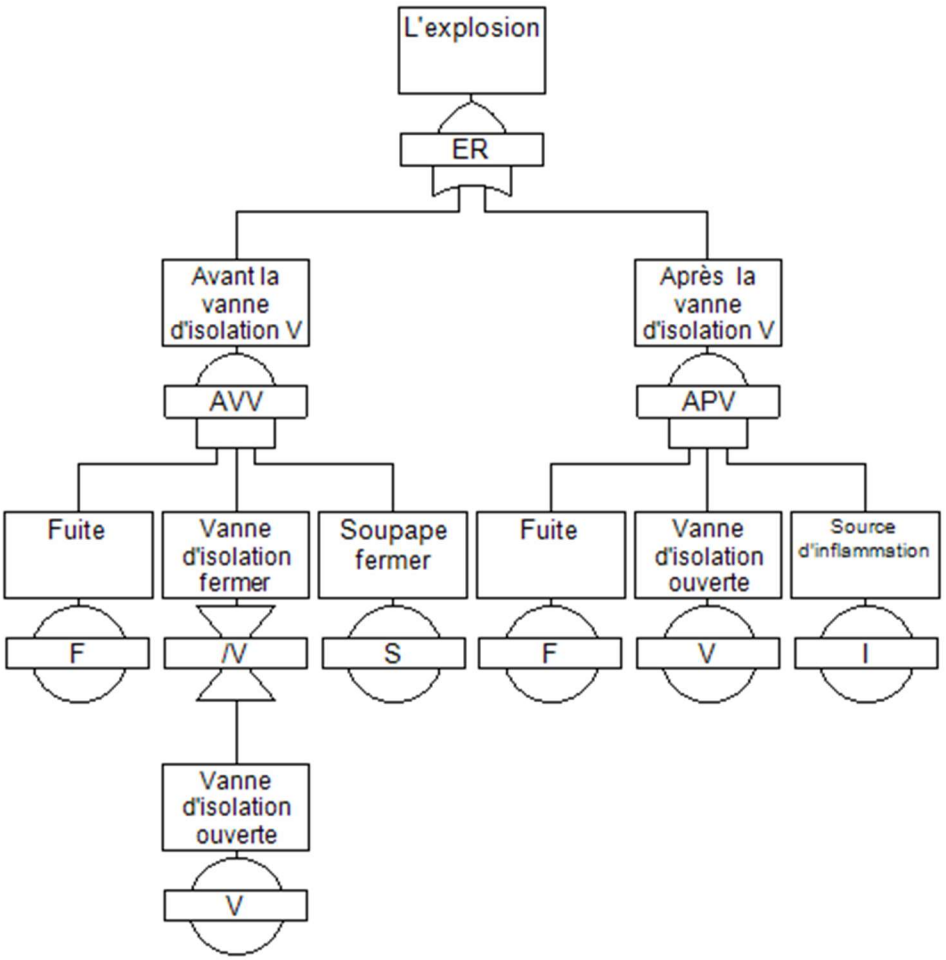


Figure 26 : Schéma de l'ADD-Système de transport de gaz en pression

ER = F. $\bar{V}$.S + F.V.I

En appliquant la loi de consensus $\bar{A}X + AY = \bar{A}X + AY + XY$:

F($\bar{V}$.S + V.I) = F($\bar{V}$.S + V.I + S.I)

ER = F.$\bar{V}$.S + F.V.I + F.S.I

L'évènement F.S.I : en cas de fuite F avec une source d'inflammation I et la soupape S fermé, ça n'a pas d'importance si la vanne d'isolation V fonctionne ou non.

La conversion en BDD :

- Avant la conversion à un BDD, la porte NOT est poussée vers le bas de l'ADD en utilisant les lois de De Morgan :

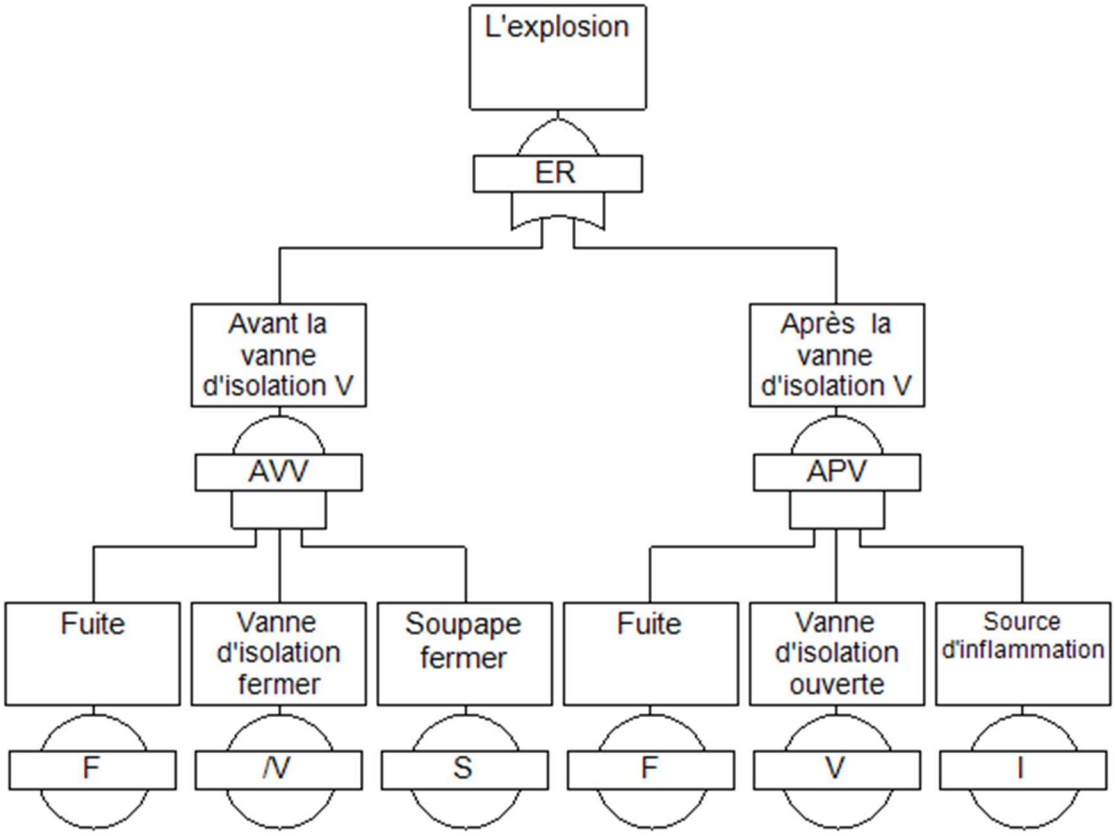


Figure 27 : Schéma de l'ADD-Système de transport de gaz en pression sans porte NOT

La construction du SFBDD à partir d'un ADD se déplace dans l'ADD de manière ascendante :

1- La construction du SFBDD nécessite initialement que les événements de base reçoivent un ordre :

Considérez l'ordre des variables : F < V < S < I

Pour les petits ADD l'ordre des variables est en grande partie pas pertinent.

2- Chaque événement de base se voit attribuer une structure ite ou sas :

Les composants ou les événements de bases sont représentés par des nœuds dans la SFBDD, chaque nœud d'une SFBDD a deux branches 1 et 0, la branche 1 correspond à la défaillance du composant, et la branche 0 correspond au fonctionnement du composant.

De plus, chaque nœud a une structure ite(if, then, else) en anglais ou sas(si, alors, sinon).

Considérez la structure sas d'un composant x : sas(x, f1, f0), ce qui signifie que si le composant x est défaillant alors considérez la fonction f1, sinon (le composant x fonctionne) considérez la fonction f0.

La fonction f1 se trouve sur la branche 1, et f0 se trouve sur la branche 0.

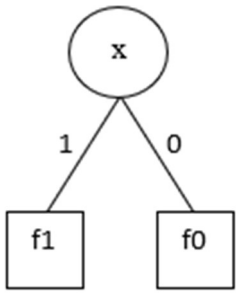


Figure 28 : Structure ite

Par exemple, considérez la structure sas de l'évènement de fuite F : sas(F, f1, f0), ce qui signifie que si la fuite F apparaitre alors considérez la fonction f1, sinon (la fuite F n'apparait pas) considérez la fonction f0.

F = sas(F, 1, 0)

V = sas(V, 1, 0)

$\bar{V}$ = sas(V, 0, 1)

I = sas(I, 1, 0)

S = sas(S, 1, 0)

3- Traitement des entrées de porte :

Si J = sas(x, f1 , f0), et H = sas(y, g1, g0) représentent deux entrées dans une porte de type logique $\oplus$ alors :

J$\oplus$H =

- sas(x, f1$\oplus$H, f0$\oplus$H) si x < y dans l'ordre

- sas(x, f1$\oplus$g1, f0$\oplus$g0) si x = y dans l'ordre

La SFBDD :

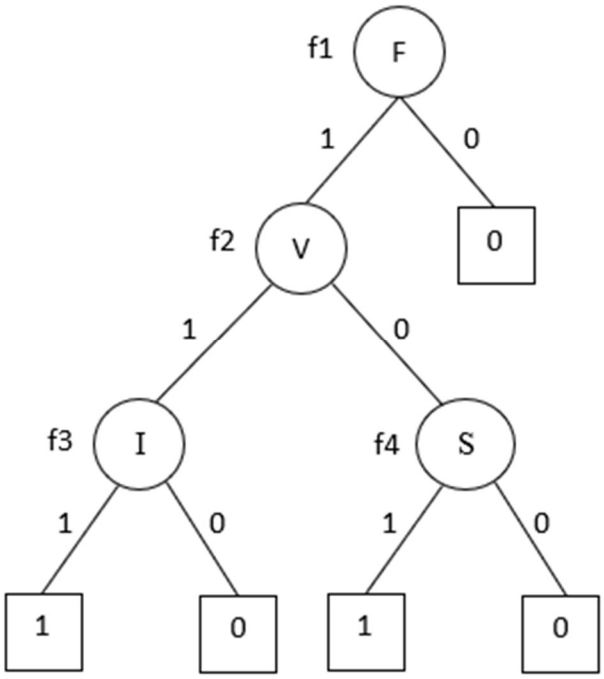


Figure 29 : Schéma de SFBDD

La SFBDD ne peut pas être utilisé directement pour fournir toutes les informations sur l'analyse qualitative pour produire une liste complète des impliquants premiers d'un ADD non cohérent.

Depuis la connaissance des ensembles d'impliquants premiers peut s'avérer précieuse pour mieux comprendre le système, et pour calculer les probabilités ou la fréquence de défaillance, et parce que l'évaluation qualitative et quantitative est requise pour la prise de décision, d'autres méthodes dérivées d'un BDD sont présentées :

9.2.1. Méthodes dérivées d'un BDD :

Méthodes efficaces de conversion d'un ADD permettant des analyses qualitatives et quantitatives [35], telles que la méthode BDD de méta-produits (meta-products BDD), la BDD supprimée par zéro (zero-suppressed BDD ou ZBDD), la BDD étiquetée (labelled BDD ou L-BDD) et le diagramme de décision ternaire (ternary decision diagram ou TDD) :

1- Un diagramme de décision ternaire (TDD) qui a trois branches pour chaque nœud 1, 0 et C, la branche 1 correspond à pertinence de la défaillance du composant, la branche 0 correspond à pertinence de la réparation du composant, et la branche C correspond à non-pertinence du composant.

La branche C représente l'intersection des branche 1 et 0, il n'est pas obtenu pour tous les composants (reste vide) où le composant est seulement défaillance ou réparation pertinente et pas les deux.

Chaque nœud d'un TDD a une structure ifre(if, failure relevant, repair relevant, else) en anglais ou sdrs(si, défaillance pertinente, réparation pertinente, sinon). Considérez la structure sdrs d'un composant x : sdrs(x, f1, f0, f2), ce qui signifie que si le composant x est défaillance pertinente alors considérez la fonction f1, sinon x est réparation pertinente alors considérez la fonction f0, sinon considérez la fonction f2.

La fonction f1 se trouve sur la branche 1, et f0 se trouve sur la branche 0, et f2 se trouve sur la branche C.

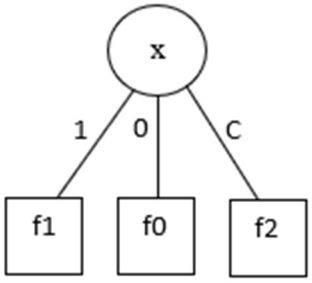


Figure 30 : Structure ifre

Dans les cas où la branche C n'est pas requise (reste vide) f2 = NIL.

L’ordre des variables est le même : F < V < S < I

Traitement des entrées de porte :

Si J = sdrs(x, f1, f0, f2), et H = sdrs(y, g1, g0, g2) alors :

J⊕H =

- sdrs(x, f1⊕H, f0⊕H, f1⊕H×f0⊕H) si x < y dans l’ordre

- sdrs(x, f1⊕g1, f0⊕g0, f1⊕g1×f0⊕g0) si x = y dans l’ordre

Le TDD :

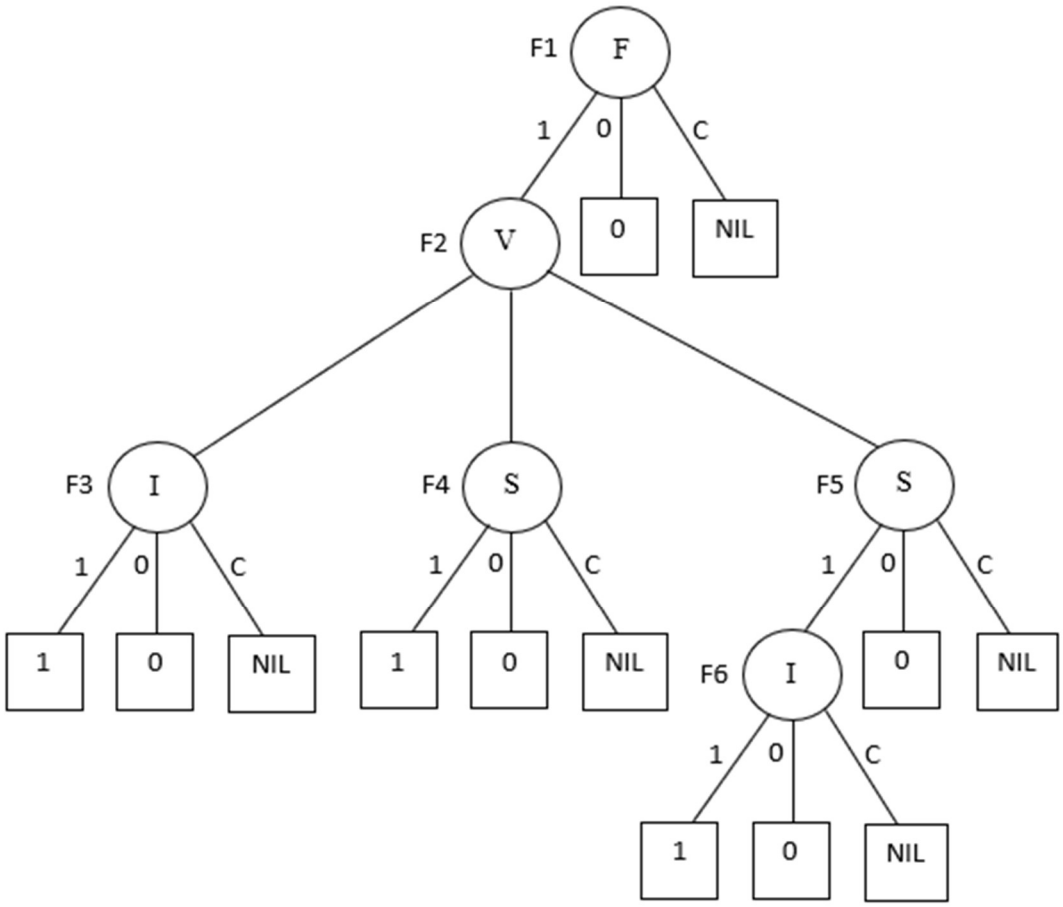


Figure 31 : Schéma de TDD

Les impliquants premiers :

La branche 1 d'un nœud représente l'état de défaillance, La branche 0 d'un nœud représente l'état de fonctionnement, La branche C d'un nœud n'est pas incluse.

F1 F2 F3 => {F, V, I}

F1 F2 4 => {F, $\bar{V}$, S}

F1 F2 F5 F6 => {F, S, I}

2- Une méthode BDD à zéro supprimé (ZBDD) nécessite d'étiqueter les nœuds avec des états de défaillance et / ou de fonctionnement des événements de base et aboutit à tous les ensembles des impliquants premiers obtenus.

3- Une méthode de BDD étiqueté (L-BDD), où chaque événement de base est étiqueté en fonction de son type (positif, négatif, et les deux) [36]. Cette information supplémentaire sur l'occurrence des événements de base permet l'application d'un algorithme d'analyse approprié résultant de la détermination d'ensemble des impliquants premiers.

4- Une approche BDD de méta-produits donne tous les ensembles des impliquants premiers. Chaque événement de base est représenté par deux variables, la première représente la pertinence du composant (pertinent ou non pertinent) et la deuxième représente le type de pertinence (pertinent pour la panne ou pertinent pour la réparation).

9.3. HiP-HOPS (Etudes Hiérarchisées d'Origin et de Propagation des dangers) :

HiP-HOPS (Hierarchically Performed Hazard Origin and Propagation Studies) [34] [37] est une méthode d'analyse de sécurité pour la modélisation non cohérente, qui peut donner un aperçu plus précis et correct du comportement de défaillance par un processus d'analyse de défaillance fonctionnelle FFA (functional failure analysis), et fournir une image complète des façons que le système peut tomber en panne.

HiP-HOPS introduit un degré d'automatisation pour résoudre les problèmes, et créer un diagramme de flux hiérarchique des opérations du système et de ses sous-systèmes pour identifier les fonctions et leurs dépendances, avec une notation supplémentaire pour décrire les niveaux du modèle qui permet de concevoir des systèmes complexes comme un diagramme de bloc fonctionnel.

Ces spécifications de niveau de défaillance produisent un ensemble des arbres des défaillances et une analyse des modes de défaillance et de leurs effets FMEA (Failure Modes and Effects Analysis) pour le système, qui est utilisé afin d'identifier des combinaisons plausibles de plusieurs défaillances fonctionnelles et d'évaluer leurs effets et leur criticité.

Ce modèle examine chaque fonction pour les modes de défaillance possibles avec des classes associées (fonction, dysfonctionnements, perte de fonction) pour éliminer les dépendances évitables telles que les causes communes de défaillances de et déterminer les effets, la criticité de ces défaillances, la récupération, et le potentiel de détection, où un composant ne génère pas seulement des événements de défaillance, mais a la possibilité de détecter et de répondre aux événements de défaillance d'autres composants.

La technique est prise en charge par plusieurs logiciels de modélisation.

9.4. Autres techniques :

D'autres algorithmes [38] qui sont théoriquement corrects peuvent être une méthode alternative pour l'analyse des ADD non cohérentes, ils sont considérés comme une approche descendante pour obtenir les ensembles des impliquants premiers.

10. Notion :

Une idée fausse commune [34] selon laquelle la porte d’inhibition (INHIBIT) peut être utilisée comme substitut de la porte NOT. La porte d’inhibition est désignée avec une condition qui peut être efficace lorsque la condition représente la défaillance du composant pouvant entraîner une défaillance du système, mais lors de la représentation de l'état de fonctionnement du composant, le système nécessite toujours une modélisation non cohérente.

11. Pour et contre les ADD non cohérents :

Arguments pour et contre les arbres de défaillances non cohérents : [34]

Pour :

- Bénéfique pour identifier les mesures préventives potentielles.

- Important dans la modélisation des défaillances des systèmes multitâches.

- La nécessité d'indiquer que la coexistence de deux pannes est interdite par les frontières du système (porte XOR).

- système avec une séquence d'opérations nécessitant la négation de défaillance pour se produisent.

Contre :

- La négation des défaillances des composants peut provoquer une défaillance du système et le contraire.

- Les probabilités trompeuses d'une négation des défaillances des événements dans l'analyse quantitative.

12. Conclusion :

Les arbres de défaillances sont classés selon leur fonction logique (portes). L'ADD qui contient des portes ET et OU uniquement est un arbre de défaillance cohérent, et non cohérente lorsque la porte NOT est utilisée ou directement impliquée (portes OU exclusif, XOR…).

L'utilisation de la porte NOT est généralement déconseillée, lorsque la porte NOT signifie que lorsque le composant fonctionne le système est dans l'état défaillant, et lorsque le composant tombe en panne le système est restauré à l'état non défaillant. La logique NOT complique la compréhension du système et rend les analyses qualitative et quantitative plus difficiles.

Puisque la réparation d'un composant défaillant peut conduire à une défaillance du système, et la défaillance d'un composant à une performance réussit du système, et aussi si l'ADD contient les deux états (fonctionnement/défaillance) d'un élément, crée une incohérence. L'ADD peut devenir cohérent si la logique NOT est éliminée de la structure.

Mais il a été soutenu que la logique NOT est bénéfique dans certains cas et l'incohérence facilite la compréhension afin de représenter certains systèmes avec plus de précision.

La structure d'un ADD non cohérent est différente d'une structure cohérente, lorsque l'état de système se change de façon différente en fonction de changement d'état des composants. Cette structure d'ADD non cohérent est due à des causses de compréhension des fautes...

Les causes possibles de panne du système dans l'ADD non cohérent contiennent les deux états de défaillance et de fonctionnement des composants, pour cela les causes sont référencées comme des ensembles des impliquants premiers.

L'obtention des impliquants premiers est faite par un logiciel pour les grands systèmes de l'industrie, et manuellement (sans logiciel) pour les systèmes petits qui nécessitent l'élimination de la logique NOT pour converser la structure de l'ADD en la version cohérente. Ceci est possible par plusieurs procédures comme la substitution de la porte NOT, Combinaison logique

de ET/OU porte des sous arbres monotones. Il existe d'autres procédures de non cohérence comme la BDD et ces dérivées, HiP-HOPS et d'autres algorithmes aussi.

Les ADD non cohérents a aussi des avantages et des limites.

CHAPITRE 4 :

Application sur les ADD non cohérents

1. Introduction :

Dans cette partie nous allons faire une simulation de certains systèmes qui incluent une situation non cohérente.

La simulation est faite par un logiciel Isograph.

2. système de détection de gaz multitâches :

Considéré le système suivant [32] :

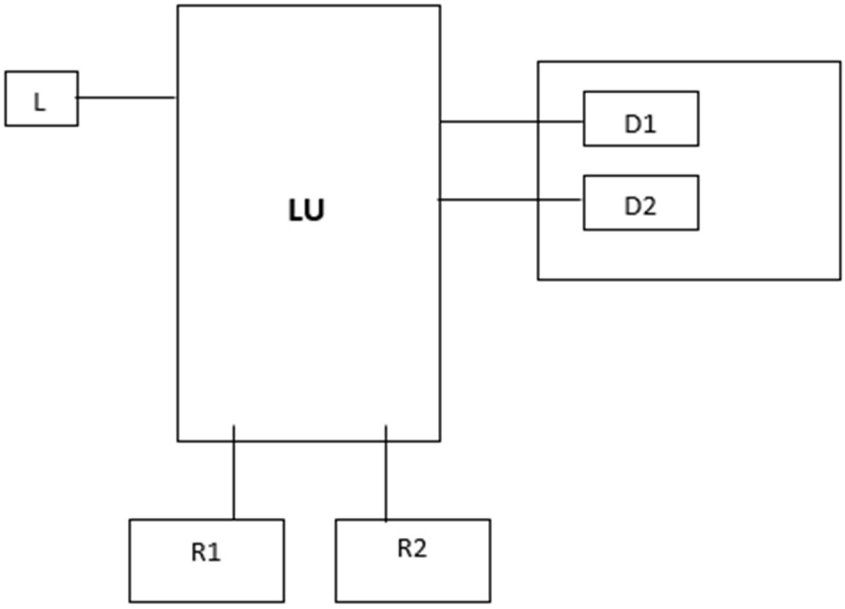


Figure 32 : système de détection de gaz multitâches

D1 et D2 sont deux détecteurs de gaz dans un espace confiné, ils envoient des signaux le long des câbles individuels à l'unité logique (LU). Si l'unité logique reçoit un signal de n'importe quel détecteur, trois taches doivent être effectuées :

- Arrêter le relais R1

- Informer l'opérateur par une lampe et une sirène L

- Arrêter le relais R2

L'évènement indésirable est si le système n'effectue pas une ou plusieurs des trois fonctions fournies une fuite se produit. Il y a sept situations possibles pour que l'évènement indésirable se produise :

Situations	Opérateur non informé	R1 n'arrête pas	R2 n'arrête pas
1	F	F	V
2	F	V	F
3	F	V	V
4	V	F	F
5	V	F	V
6	V	V	F
7	V	V	V

Tableau 17 : Les situations possibles de l'évènement indésirable du système de détection de gaz multitâches

Chaque situation représente une panne du système, mais certaines situations sont plus graves que d'autres. Par exemple, la situation trois depuis que l'opérateur est informé de la détection de gaz comprend ainsi que le système fonctionne correctement (les trois taches sont effectuées).

La représentation logique de la situation 3 :

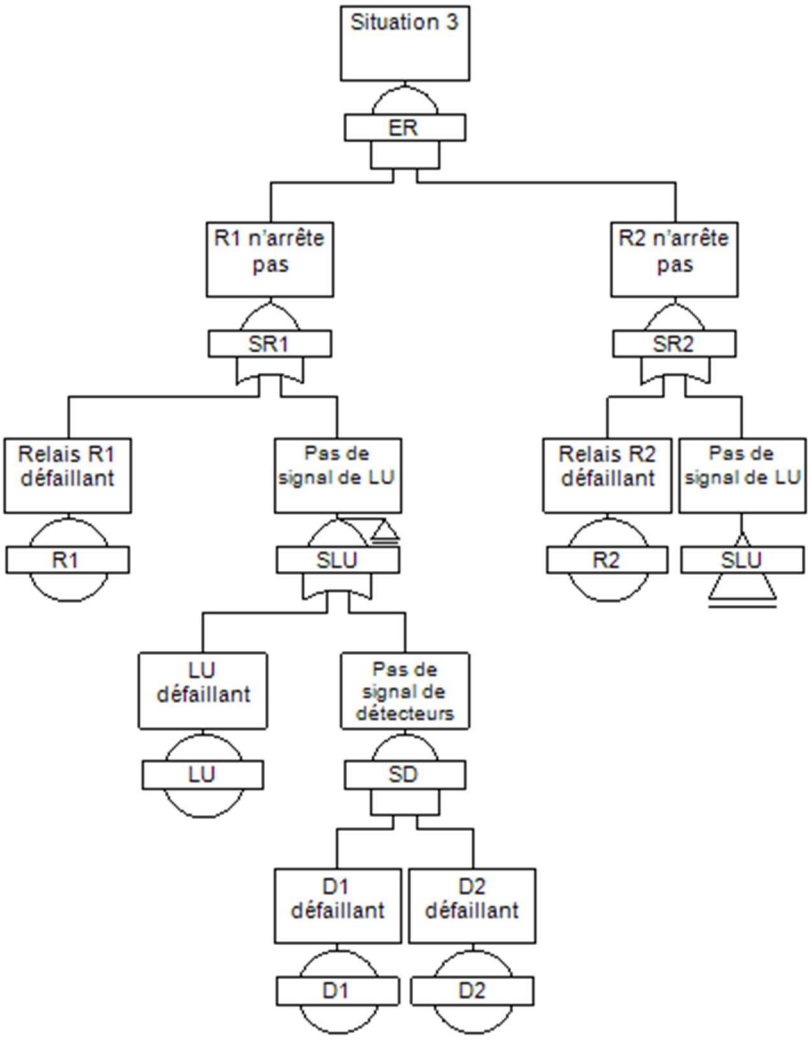


Figure 33 : Schéma de l'ADD-la situation 3

L'équation :

ER = (R1+LU+D1*D2)*(R2+LU+D1*D2)

ER = R1*R2 + LU + D1*D2

Les coupes minimales :

R1*R2 ; LU ; D1*D2

A partir des coupes minimales, nous comprenons que la défaillance de LU ou les deux détecteurs (D1 et D2) conduire à la situation 3. Mais puisque l'opérateur est informé, soit D1 et LU soit D2 et LU doit fonctionner, cela signifie que la défaillance de LU ou les détecteurs seulement ne causerait pas la situation 3. Plus encore la quantification de cet ADD entraine une surestimation importante des probabilités.

Pour une représentation correcte il est essentiel d'utiliser la NOT logique :

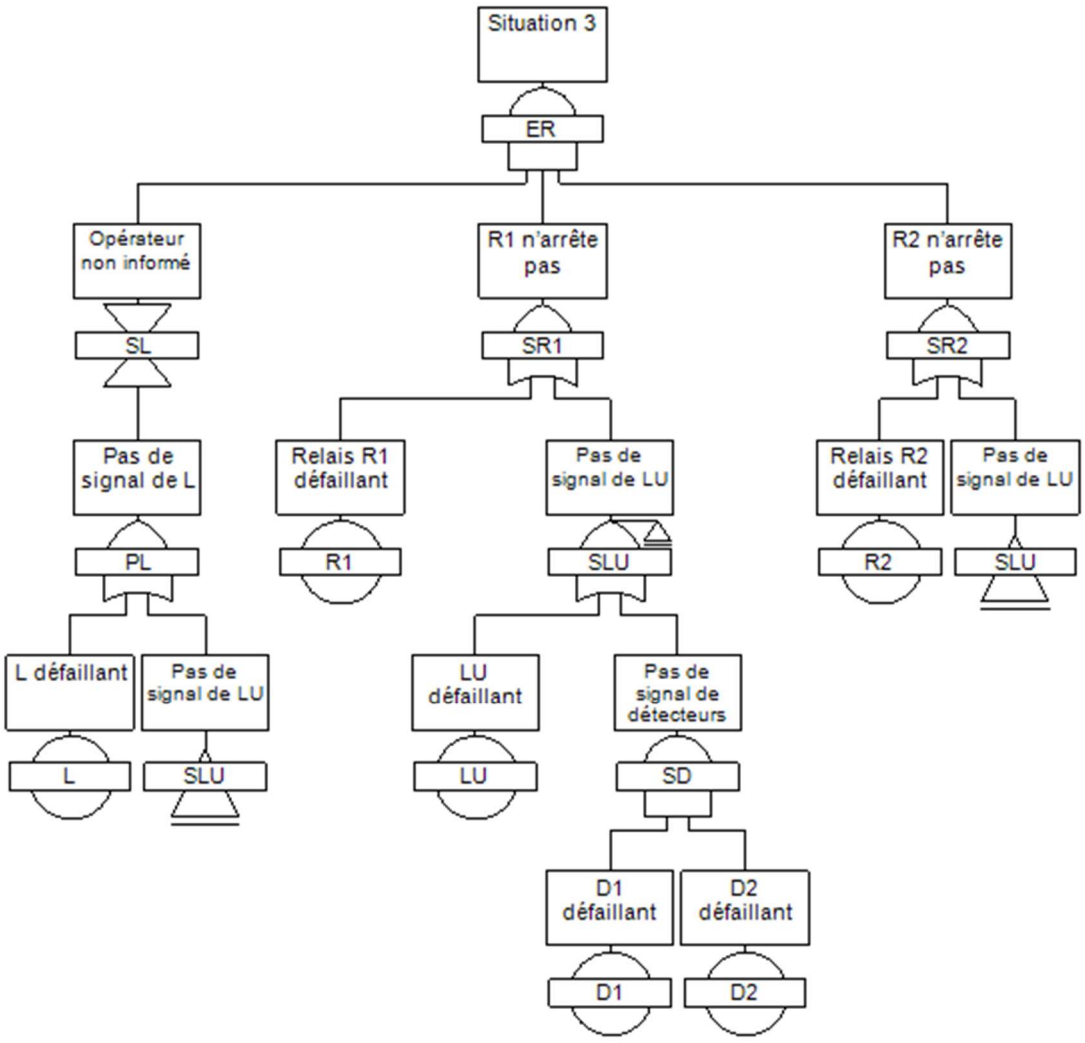


Figure 34 : Schéma de l'ADD-la situation 3 avec la porte NOT

L’obtention des impliquants premiers :

Tout d’abord, l’obtention d’une approximation cohérente à l’aide des lois de De Morgan :

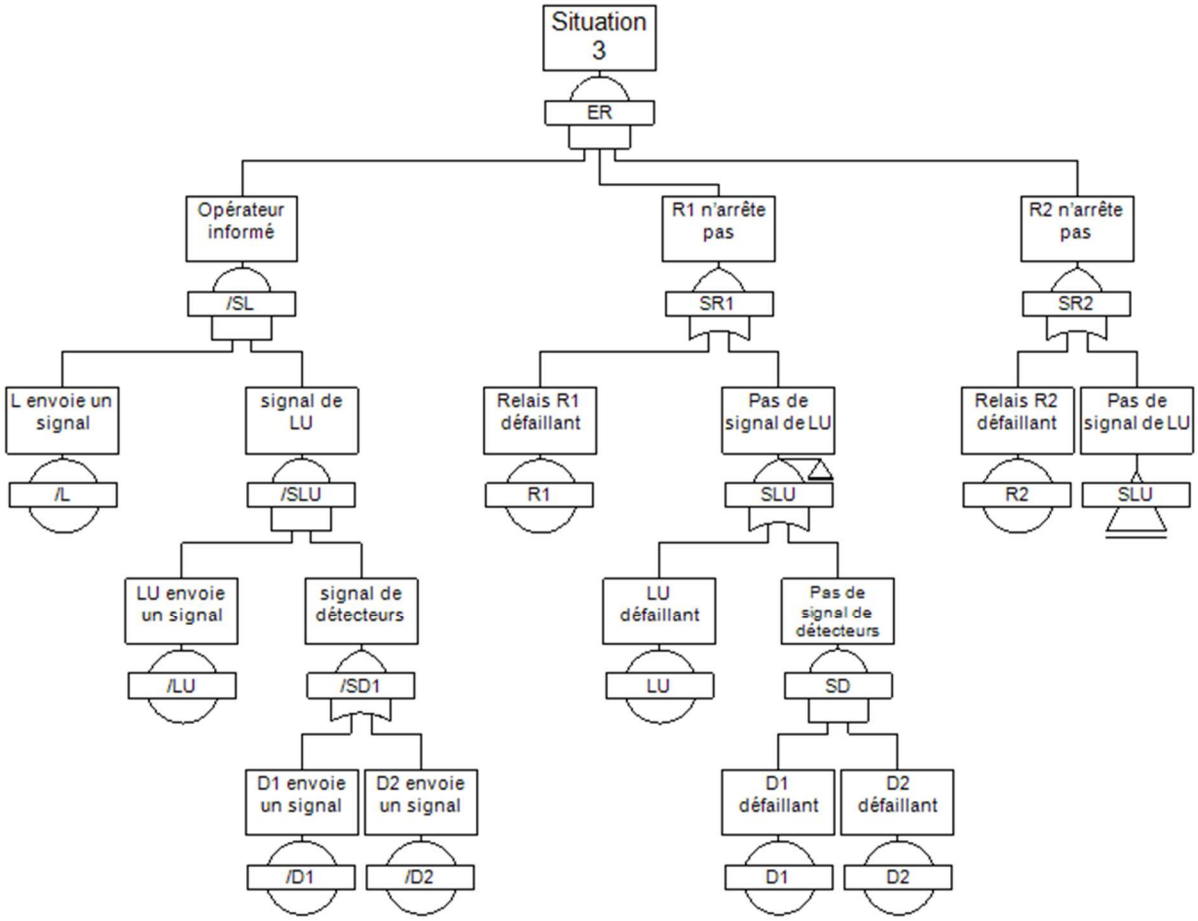


Figure 35 : Schéma de l’ADD-la situation 3 avec la porte NOT éliminé

Equation :

ER = EI1*EI2*EI3

ER = $\overline{L}$*$\overline{LU}$*($\overline{D1}$+$\overline{D2}$)*(R1+LU+D1*D2)*(R2+LU+D1*D2)

ER = $\overline{L}$*$\overline{LU}$*($\overline{D1}$+$\overline{D2}$)*(R1*R2 + LU + D1*D2)

ER = $\overline{L}$*$\overline{LU}$*($\overline{D1}$+$\overline{D2}$)*R1*R2

Analyse par logiciel :

Les probabilités données au logiciel sont le taux de défaillance des composants :

Composant	Taux de défaillance
L	4.68E-5
LU	8.65E-6
D1, D2	1.89E-7
R1	3.7E-7
R2	2.34E-7

Tableau 18 : le taux de défaillance des composants du système de détection de gaz multitâches

Temps de mission : 8760 heures, une analyse de système pour période de temps de 1 an.

Résultats :

Données du système (ER) :

Indisponibilité	4.077E-6
Unfiabilité	8.452E-6
Fréquence	9.648E-10
MTTF	1.76E9
Temps de panne	0.03571
MTTR	
MTBF	
Nombre de défaillances	8.452E-6

Tableau 19 : Résultats du système de détection de gaz multitâches

Les impliquants premiers :

ER = $\overline{SLU}$*$\overline{L}$*R1*R2

Facteurs d'importance :

Evènements	Fussell-Vesely	Bimbaum	Barlow-Proschan	Séquentiel	RRW	RAW
R2	1	0.001991	0.4819	0.5181	1E+300	488.3
R1	1	0.00126	0.4816	0.5184	1E+300	309
SLU	-0.07872	-4.398E-6	0.03655	0.9634	0.927	-9.714E-17
L	-0.5068	-6.143E-6	0	1	0.6637	

Tableau 20 : Résultats des facteurs d'importance du système de détection de gaz multitâches

Ces résultats ne sont pas exacts, car les données des composants de cette analyse ne sont pas les données réelles du système de détection de gaz multitâches.

3. Réacteur nucléaire :

L'accident de Three Mile Island unité 2 (TMI-2) le 28 mars 1979 [39], d'un réacteur nucléaire, l'un des accidents les plus graves de l'histoire de l'exploitation d'une centrale nucléaire avec de faibles rejets radioactifs est une conséquence des événements non cohérente.

Considérons la version simplifiée du système de refroidissement du cœur du réacteur nucléaire et ces événements pour illustrer la non-cohérence :

La figure représente le système utilisé pour refroidir le cœur du réacteur par la circulation d'eau.

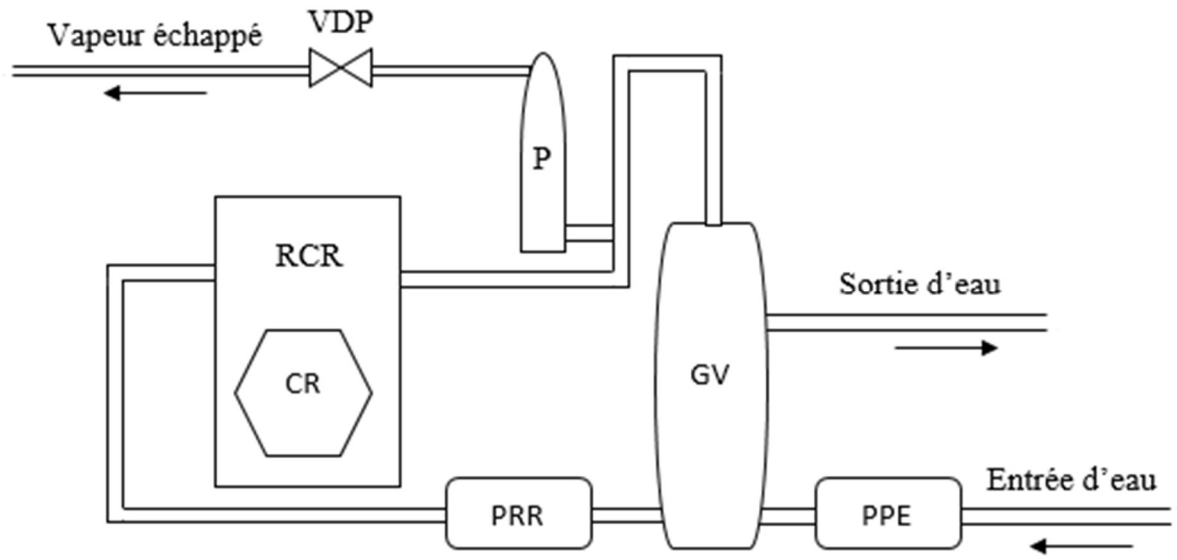


Figure 36 : Système de refroidissement de cœur de réacteur nucléaire simplifié

Le fonctionnement du système :

L'eau de refroidissement du cœur du réacteur est alimentée par les pompes principales d'alimentation en eau PPE, puis le générateur de vapeur GV convertit l'eau sous forme de vapeur qui évacue la chaleur du cœur du réacteur, la circulation d'eau est contrôlée par la pompe de refroidissement du réacteur PRR jusqu'au récipient du cœur du réacteur RCR qui contient le cœur du réacteur CR, un pressuriser P est installé dans la canalisation pour maintenir la pression à un niveau acceptable, au niveau de pressuriser P est située une vanne de décharge pilotée VDP qui ouvert en cas d'augmentation de pression, et enfin la sortie d'eau.

Séquence des événements :

- Les pompes principales d'alimentation en eau PPE n'arrivent pas à envoyer de l'eau au système (entré d'eau) en raison d'une défaillance mécanique ou électrique.

- Le générateur de vapeur GV a continué sa fonction de convertir de l'eau dans la canalisation sous forme de vapeur. La pression dans la tuyauterie nucléaire a commencé à augmenter immédiatement.

- La vanne de décharge pilotée VDP s'est ouverte afin de contrôler cette pression. La vanne aurait dû se fermer lorsque la pression est diminuée à des niveaux appropriés, mais elle est restée bloquée ouverte.

- En conséquence, l'usine subissait un accident de perte de liquide de refroidissement car de l'eau de refroidissement sous forme de vapeur créée par le générateur de vapeur GV s'échappait de la vanne bloquée ouverte.

Le personnel de l'usine n'en était pas conscient car les instruments de la salle de contrôle indiquaient que la vanne était fermée.

- La pompe de refroidissement du réacteur PRR s'est arrêtée car la vanne bloquée ouverte a tellement réduit la pression que la pompe s'est mise à vibrer.

- Le niveau d'eau dans le récipient de cœur du réacteur RCR a chuté et le cœur du réacteur CR a surchauffé sans que la pompe de refroidissement du réacteur ne fasse circuler l'eau et que le système manque d'eau de refroidissement.

Faire face à la situation :

Alors que les alarmes retentissaient en raison du manque d'alimentation en eau et de l'augmentation de la pression, les instruments à disposition du personnel de l'usine fournissaient des informations trompeuses. Ignorant que la vanne de décharge est bloquée ouverte, ce qui entraîne la perte d'eau de refroidissement pour couvrir le cœur du réacteur.

La vanne de décharge bloquée ouverte a fait que le pressuriser s'est rempli d'eau comme l'indiquaient les instruments de la salle de contrôle.

Le personnel de l'usine a supposé que tant que les instruments montraient que le niveau d'eau du pressuriser était suffisamment élevé, le cœur du réacteur était également correctement recouvert d'eau. Parce que pendant les opérations normales, le récipient sous pression qui contenait le cœur du réacteur était toujours rempli d'eau jusqu'en haut, il n'était donc pas nécessaire qu'un instrument de mesure du niveau d'eau indique le niveau d'eau dans le récipient qui recouvrait le cœur, mais ce n'était pas le cas.

La situation non cohérente :

La surchauffe du cœur du réacteur s'est produite à cause de :

Défaut d'alimentation de l'eau :

- Les pompes principales PPE ne fournissent pas d'eau.
- La pompe de refroidissement du réacteur PRR est arrêtée.

Perte d'eau de refroidissement :

- Générateur GV convertit l'eau sous forme de vapeur (mode de fonctionnement).
- La vanne de décharge pilotée VDP est bloquée ouverte.
- Le niveau d'eau du pressuriser P est élevé (mode de fonctionnement).

L’ADD est représenté comme suite :

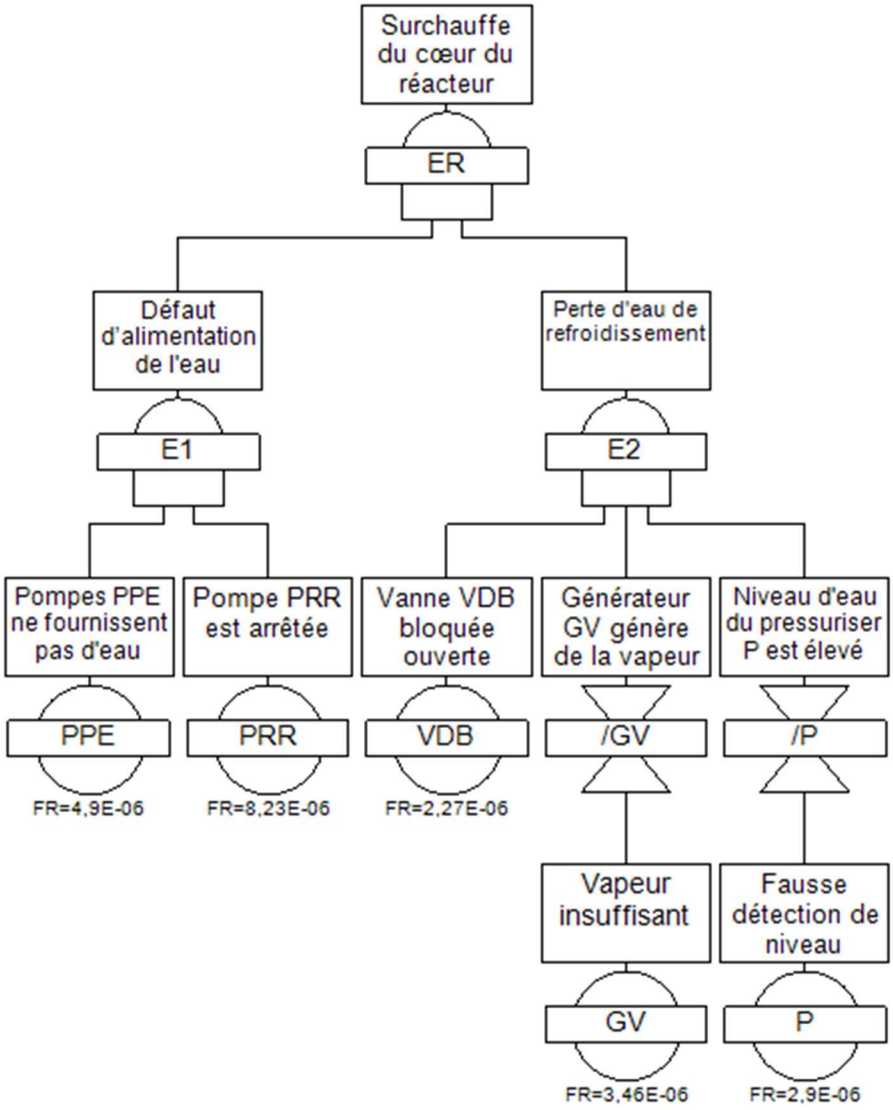


Figure 37 : Schéma de l’ADD-Surchauffe du cœur du réacteur

Analyse par logiciel :

Le taux de défaillance et MTTR des composants [40] :

Composant	Taux de défaillance / h	MTTR / h
PPE	4,9E-6	4
PRR	8,23E-6	6,3
VDP	2,27E-6	2,8
GV	3,46E-6	5
P	2,9E-6	2

Tableau 21 : Le taux de défaillance et MTTR des composants

Temps de mission : 8760 heures, une analyse de système pour période de temps de 1 an.

Résultats :

Données du système (ER) :

Evéenements	ER	E1	E2
Indisponibilité	6,459E-15	1,016E-9	6,356E-6
Unfiabilité	4,333E-11	3,638E-6	1,969E-2
Fréquence	4,946E-15	4,153E-10	2,27E-6
MTTF /h	2,021E+14	2,406E+9	4,404E+5
MTBF/h	2,022E+14	2,408E+9	4,405E+5
MTTR /h	1,306	2,447	2,8
Temps de panne h	5,658E-11	8,902E-6	5,568E-2

Tableau 22 : Résultats du système de réacteur nucléaire

Les impliquants premiers :

ER = E1*E2

ER = $\overline{GV}$*$\overline{P}$*VDP*PPE*PRR

Facteurs d'importance :

Composant	Fussel-Vesely	Birnabaum	Barlow-Proschan	Séquentiel	RRW	RAW
PPE	1	5,185E-5	0,6117	0,3883	1	5,102E-4
PRR	1	1,96E-5	0,3883	0,6117	1	1,929E-4
VDP	1	0.9523	0.9959	1,781E-5	1	1,573E-5
GV	-1,73E-5	-6,356E-6	9,688E-6	1	1	6,497E-17
P	-5,8E-6	-6,356E-6	8,12E-6	1	1	3,412E-17

Tableau 23 : Résultats des facteurs d'importance du système de réacteur nucléaire

Ces résultats ne sont pas exacts, car les données des composants de cette analyse ne sont pas les données réelles du système de réacteur nucléaire.

Conclusion générale :

La sûreté de fonctionnement a une importance et une nécessité dans le processus industriel, en fournissant les concepts et les méthodes d'analyse pour analyser et étudier les systèmes et évaluer le niveau de sécurité.

Le but de l'étude de sûreté de fonctionnement est d'identifier les scénarios des défaillances et les conséquences associées. Elle permet aussi de quantifier la probabilité de la survenue des divers événements indésirables.

Parmi les différentes méthodes d'analyse des risques il y a l'ADD, Un arbre de défaillance (ADD) ou Fault tree analysis FTA (en anglais) est une technique d'ingénierie utilisée dans l'industrie pour l'amélioration des systèmes.

L'ADD consiste à représenter les scénarios possibles des pannes du système et leur enchaînement logique des évènements par une arborescence (schéma graphique en forme d'arbre inversé), cette construction est restreinte à certaines règles. La méthode est suivie par un traitement mathématique pour identifier les points vulnérables du système, les probabilités d'occurrence des défaillances et des pannes.

Les ADD sont classés selon leur fonction logique (portes). L'ADD qui contient des portes ET et OU uniquement est un arbre de défaillance cohérent, et non cohérente lorsque la porte NOT est utilisée ou directement impliquée (portes OU exclusif, XOR…).

La fonction logique NOT est généralement déconseillée en raison de la complexité ajoutée, elle rend la compréhension et les analyses du système plus difficiles. Mais il a été soutenu que la logique NOT est bénéfique dans certains cas et l'incohérence facilite la compréhension afin de représenter certains systèmes avec plus de précision.

Bibliographie

[1] J. C. Laprie, "Dependability : Basic Concepts and Terminology", Springer Vienna, 1992.

[2] B. ZEROUALI, "Analyse du comportement de systèmes industriels par les réseaux bayésiens pour la prévention des scenarios indésirables", Université Badji Mokhtar Annaba, 2018.

[3] G. Afifa, "Évaluation de la fiabilité des systèmes embarqués dès la phase de conception par réseaux de Petri temporels étendus", Université Constantine 2 Abdelhamid MEHRI.

[4] D. A. Belhadj, "Cours de maintenance et sûreté de fonctionnement", Université de Hassiba BENBOUALI DE Chlef, 2020.

[5] «Techno-Science.net,» [En ligne]. Available: https://www.techno-science.net/glossaire-definition/Surete-de-fonctionnement.html.

[6] «CLEMESSY,» [En ligne]. Available: https://www.clemessy.com/surete-de-fonctionnement.

[7] M. Defdaf, "Utilisation des réseaux de files d'attentes pour l'évaluation des performances de la maintenance", Université Badji Mokhtar Annaba, 2018.

[8] B. Hafiza, "Modélisation stochastique pour l'évaluation des indicateurs de la sûreté de fonctionnement d'un système de production Cas de l'entreprise DOMELEC", Batna: Université Hadj Lakhdar, 2010.

[9] L. Grudzien, "Contribution à l'intégration de la sureté de fonctionnement au sein d'une démarche de conception multimétiers", Université de Valenciennes et du Hainaut Cambrésis, 1999.

[10] A. KHAROUATI, "Contribution à l'étude de la sûreté de fonctionnement des systèmes instrumentés intelligents", Annaba: Université BADJI Mokhtar, 2021.

[11] «PRESSBOOKES,» [En ligne]. Available: https://pressbooks.pub/methodes/chapter/surete-de-fonctionnement.

[12] Centre Canadien d'Hygiène et de Sécurité au Travail..

[13] H. BRAHIM, "Etude qualitative et quantitative des scenarios de défaillances de la pompe 2000 d de l'entreprise certaf", Université Aboubekr Belkaid -Tlemcen, 2014.

[14] D. O. a. e. Bennedjai Nouh, "Etude et analyse des risques industriels (Etude de cas)", Annaba: Université BADJI Mokhtar, 2019.

[15] M. Brini, "Safety-Bag pour les systèmes complexes", Université de Technologie de Compiègne (UTC), 2018.

[16] S. Belal, "Modélisation et analyse de sûreté des systèmes par arbre de défaillance", Université Mouloud Mammeri, Tizi-Ouzou, 2011.

[17] H. Kahal, "Réseaux bayésiens dynamiques : application aux réseaux électriques", Oran: Université des Sciences et de la Technologie d'Oran.

[18] M. Sallak, "Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : Application aux Systèmes Instrumentés de Sécurité", Institut national polytechnique de Lorraine, 2007.

[19] A. Imakhlaf, "Application des diagrammes de décision binaires pour l'analyse des arbres de défaillance cohérents et non-cohérents en présence d'incertitudes", Université de Technologie Compiègne (UTC), 2021.

[20] M. Medjoudj, "Contribution à l'analyse des systèmes pilotés par calculateurs : Extraction de scénarios redoutés et vérification de contraintes temporelles", Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS, 2006.

[21] A. Villemeur, "Sûreté de fonctionnement des systèmes industriels", collection de la Direction des Etudes et Recherche d'Electricité de France, 1988.

[22] S. Duval, "Application d'une méthode d'analyse des risques pour optimiser le circuit de l'instrumentation chirurgicale", Université de Strasbourg, 2016.

[23] T. Lombard, "Gestion des risques à priori : application de la méthode AMDEC à la production des médicaments anticancéreux au CHU de Grenoble", Université Joseph FOURIER Grenoble, 2015.

[24] F. B. e. M. W. Babaadoun, "Application de la méthode AMDEC pour le diagnostic et la maintenance duchauffage central à eau chaude de la faculté des sciences et sciences appliquées d'Ain Beida", Université Larbi Ben M'hidi Oum El Bouaghi, 2020.

[25] K. Bachir, "Application de l'arbre de défaillance « Fault-tree » pour le système du ballon à vapeur au niveau de l'unité Production Ammoniac", Algérie: Badji Mokhtar Annaba université, 2017.

[26] «Relyence.com,» [En ligne]. Available: https://relyence.com/2019/12/04/fault-tree-gates-events-explained/.

[27] «Electronics Tutorials,» [En ligne]. Available: https://www.electronics-tutorials.ws/boolean/bool_7.html.

[28] M. Y. Lau, "Development of a Severity Measure for Fault Tree Analysis and an Intuitive Fault Tree Analysis Software Prototype", North Carolina State University, 2019.

[29] «Arbre Analyste,» [En ligne]. Available: https://www.arbre-analyste.fr/doc/lib/exe/detail.php/theorie:importance:mif2.png?id=theorie%3Afacteurs importance.

[30] T. Kohda, "A Simple Method to Derive Minimal Cut Sets for a Non-coherent Fault Tree", International Journal of Automation and Computing, 2006.

[31] M. A. Said, "Calculs d'importance en sureté de fonctionnement Outil d'aide à la décision et au diagnostic de pannes", Université de Tizi Ouzou, 2010.

[32] S. C. Beeson, "Non-coherent Fault Tree Analysis", Loughborough université, 2002.

[33] Y. Tao, "Risk-informed Maintenance for Non-coherent Systems", The Faculty of the Engineering and Applied Science, University of Ontario Institute of Technology, 2010.

[34] Y. P. Septavera Sharvia, "Non-coherent Modelling in Compositional Fault Tree Analysis", Korea: The International Federation of Automatic Control Seoul, 2008.

[35] J. D. A. Rasa Remenyte-Prescott, "An Efficient Real-time Method of Analysis for Non-coherent Fault Trees", UK: Loughborough université.

[36] S. C. V Matuzas, "Dynamic labelling of BDD and ZBDD for efficient non-coherent fault tree analysis", 2015.

[37] J. A. M. Yiannis Papadopoulos, "Hierarchically Performed Hazard Origin and Propagation Studies", 2014.

[38] "Top down algorithmes for obtaining prime implicant sets", World Abstracts on Microelectronics and Reliability.

[39] «U.S.NRC,» [En ligne]. Available: https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html.

[40] OREDA (Offshore Reliability Data).