III.1. La gestion des risques

La gestion des risques est une discipline en développement rapide. De nombreuses définitions et différents points de vue existent sur ce qu'elle représente ou implique ainsi que sur la manière de la conduire. Une forme de cadre de référence est donc nécessaire pour préciser :

- La terminologie ;
- Le processus de déploiement de la gestion des risques ;
- L'organisation de la gestion des risques ;
- L'objectif de la gestion des risques.

Elle a pour but d'atteindre ou de dépasser les objectifs d'une organisation grâce à l'approche réfléchie des opportunités et des risques. Ils évaluent les événements, les actions et les développements qui peuvent empêcher une entreprise d'atteindre ses objectifs et de mener à bien sa stratégie. **[7]**

III.1.1. Définition

Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. La gestion du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque

La gestion du risque relève de la direction de l'entreprise et contribue à l'amélioration des performances et de l'efficacité d'une organisation. Elle permet de mettre en œuvre les exigences de sécurité et de garantir la réalisation des objectifs des organisations et des systèmes.

Le risque comprend les opportunités et le potentiel de dommages. Le scénario est évalué selon sa probabilité et ses conséquences. Le risque ne comprend pas seulement des sinistres soudains, mais également les dysfonctionnements insidieux inattendus. **[7]**

III.1.2. Les avantages de la gestion du risque

On peut limiter les avantages de la gestion des risques aux points suivants :

- Amélioration de la marge de manœuvre de l'entreprise ;
- Identification et gestion des risques et des opportunités à l'échelle de toute l'entreprise ;

- Détection précoce (système d'alarme précoce), minimisation et maîtrise des dangers et des risques ;
- Prévention des impondérables en entreprise et minimisation des pertes ;
- Assurer l'avenir à long terme ;
- Survie de l'organisation ;
- Optimiser la mise de capital et assurer la capacité de rendement à long terme ;
- Identifier et saisir les opportunités pour l'entreprise ;
- Contrôle du risque pour mieux profité des opportunités ;
- Améliorer la communication ainsi que la gestion des risques et des opportunités. **[7]**

III.1.3. Le système de gestion du risque

La politique de risque découle de la politique de l'organisation; elle est planifiée, mise en œuvre, contrôlée et constamment améliorée par la direction générale. La gestion du risque relève de la direction. Les systèmes de management basés sur le modèle ISO 9000 s'y prêtent parfaitement.

Le système de management de la famille ISO 9000, mis en œuvre par plus de 800 000 organismes dans le monde, est devenu une référence internationale. C'est pourquoi il est important que la gestion du risque puisse être intégrée le plus facilement possible et donc à moindre coût dans le système de management. Le modèle d'entreprise, qui se situe dans le champ de tension entre les besoins et la satisfaction de la clientèle d'une part et les exigences des parties intéressées, en est le point de départ. Le processus de management comprend également la gestion du risque. **[7]**

III.1.4. Processus de gestion des risques

Le schéma ci-dessus présente les six phases de gestion des risques retenues dans ce site pour représenter le processus de gestion des risques. Pour chacune des six phases, vous retrouverez: une présentation synthétique une présentation détaillée (Détail de la phase), des témoignages, des gabarits, des conseils et des exemples.

En résumé, les six phases de la gestion des risques s'effectuent tour à tour tout au long d'un projet. Elles se lisent dans le sens des aiguilles d'une montre.

Ainsi, la phase d'**IDENTIFICATION** est généralement celle qui initie la gestion des risques; elle est suivie par l'**ANALYSE**, la **PLANIFICATION**, le **SUIVI** et le **CONTRÔLE**.

La phase de **COMMUNICATION** est une exception car elle ne suit pas d'ordre chronologique et s'applique à l'ensemble des phases de gestion des risques. **[7]**

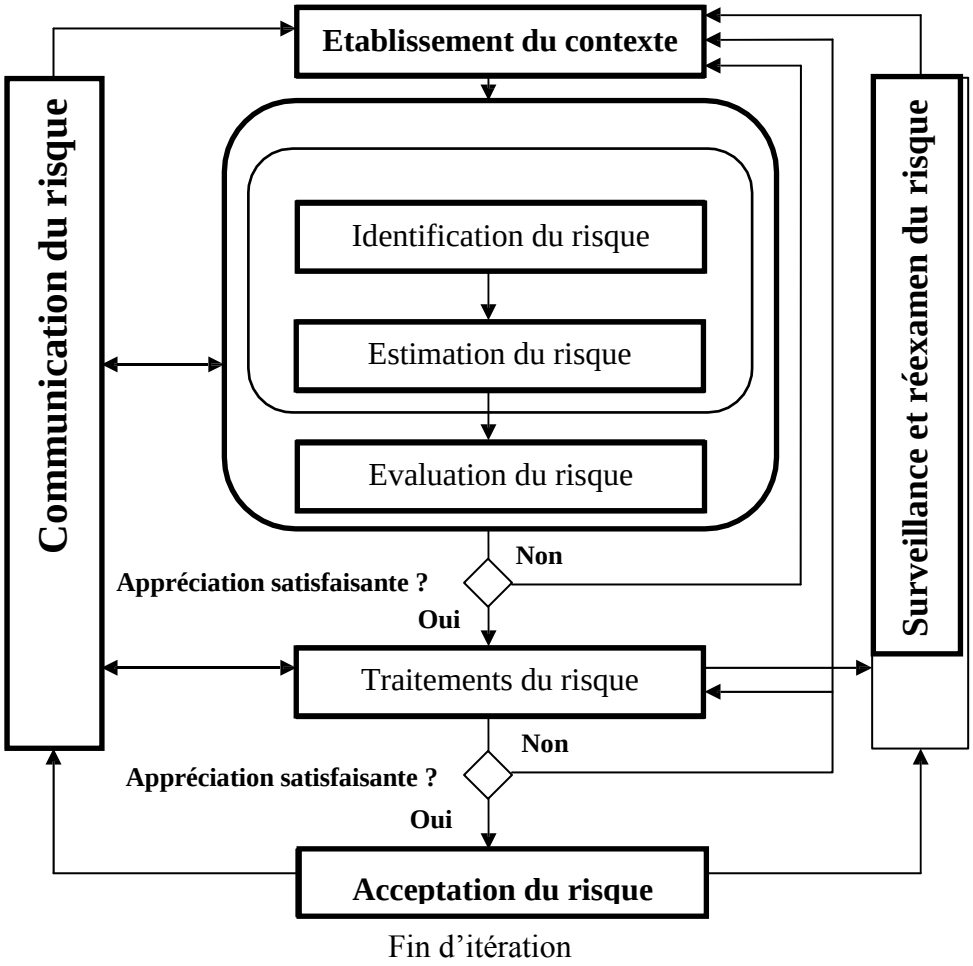

Figure III.1. Processus de gestion des risques.

III.2. Méthodes d'analyse des risques

Afin de prévenir les risques associés à un procédé, un certain nombre de méthodologies ont été développées pour procéder à une analyse systématique des risques et de leurs conséquences.

Ces méthodologies servent à mettre en évidence toutes les sources de dangers, à identifier les risques posés par les éléments du système et leurs interactions, à anticiper des dérives et mettre en place des mesures de sécurité (ou barrières dans le cas d'accidents majeurs), pour d'une part éviter que ces déviations apparaissent et d'autre part en limiter les conséquences dans les cas où cette déviation ne pourrait être corrigée.

L'application de méthodes d'analyse de risques permet donc de regrouper un certain nombre de données dans le but de maintenir à tout instant l'installation en sécurité que ce soit en fonctionnement normal ou en marche dégradée. **[8]**

III.2.1. Classification des méthodes d'analyse de risque

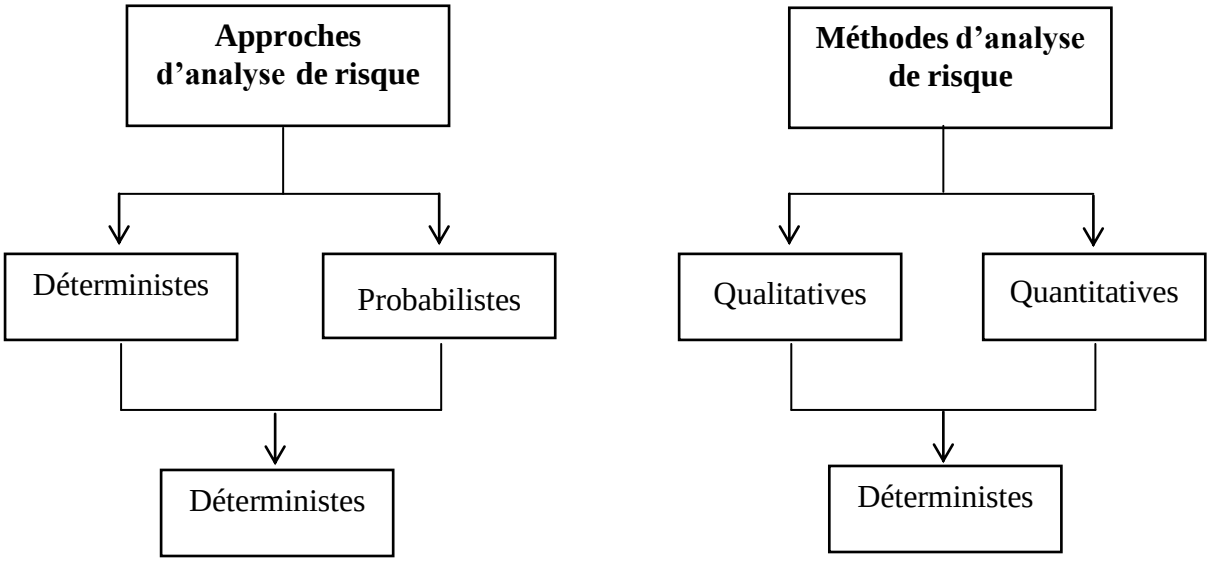

Figure III.2. Typologies et Approches des méthodes d'analyse de risque.

1. Méthodes quantitatives et qualitatives

a) Méthodes quantitatives : Les analyses quantitatives sont supportées par des outils mathématiques ayant pour but d'évaluer la sûreté de fonctionnement et entre autres la sécurité. Cette évaluation peut se faire par des calculs de probabilités (par exemple lors de l'estimation quantitative de la probabilité d'occurrence d'un événement redouté) tels que les Arbres de défaillances ou bien par recours aux modèles différentiels probabilistes tels que les Chaines de Markov, les Réseaux de Pétri, les automates d'états finis, etc.

b) Méthodes qualitatives : L'APR, HAZOP restent des méthodes qualitatives même si certaines mènent parfois aux estimations de fréquences d'occurrence avant la classification des risques. La plupart des méthodes revêtent un caractère inductif dans une optique de recherche allant des causes aux conséquences éventuelles. En contre partie, il existe quelques méthodes déductives qui ont pour but de chercher les combinaisons de causes conduisant à des évènements redoutés

2. Approche déterministe et Approche probabiliste

a) Approche déterministe : L'approche déterministe a généralement été adoptée dans les domaines à haut risque tels que nucléaire, militaire, transports guidés, où le moindre risque significatifs est traqué et réduit à la source. Elle consiste à recenser les événements pouvant conduire à un scénario d'accident en recherchant le pire cas possible et en affectant une gravité extrême à ses conséquences potentielles. Par conséquent, les sous- systèmes critiques (systèmes de sauvegarde, de protection et de prévention) sont dimensionnés pour éviter toute défaillance dangereuse et organisés rigoureusement selon une stratégie de défense en profondeur.

b) Approche probabiliste : L'approche probabiliste fait intervenir le calcul de probabilités relatives à l'occurrence d'événements faisant partie du processus de matérialisation d'un scénario d'accident donné. Il s'agit d'une approche complémentaire qui permet d'analyser le dispositif de défense en profondeur décidé à l'issue d'une approche purement déterministe, ceci a été le cas dans le domaine nucléaire ou les techniques probabilistes viennent appuyer l'approche déterministe.

3. Démarche inductive et démarche déductive

a) Démarche inductive : Le principe de ces méthodes consiste à partir d'une cause d'anomalie (défaillance, erreur humaine, agression externe, etc.) et à déterminer les scénarios d'évènements qui en résultent et/ou l'ensemble de ses conséquences possibles.

b) Démarche déductive : Les méthodes d'analyse déductive ont pour finalité la recherche des combinaisons des causes possibles d'un événement redouté

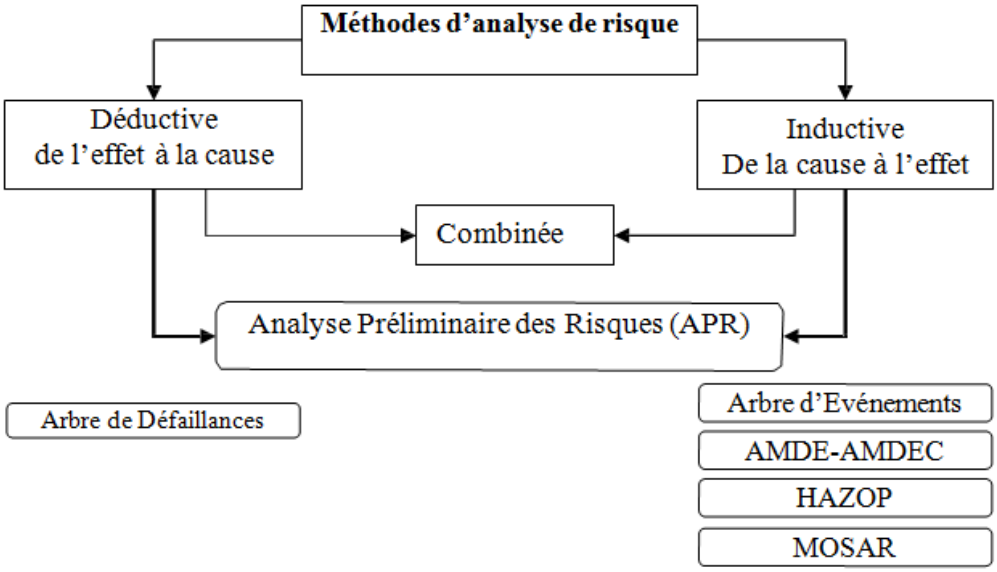

Figure III.3. Classification des principales méthodes d'analyse de risque.

III.2.2. Critères de choix d'une méthode d'analyse de risque

On est retenu l'essentiel des critères pesant dans la mise en œuvre d'une méthode plutôt qu'une autre dans l'étude d'un système donné, ces critères sont :

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

Toutefois, l'utilisation séparée d'une seule méthode d'analyse de risque peut ne pas apporter une démonstration définitive de la réalisation des objectifs de sécurité. En effet, il est nécessaire de combiner plusieurs méthodes pour une meilleure complétude et une bonne cohérence en termes de résultats. **[8]**

III.3. Les principaux outils d'analyse des risques

Les principales méthodes d'analyse des risques sont : **[8]**

III.3.1. Analyse préliminaire des risque / dangers

a) **Historique et domaine d'application :** L'analyse Préliminaires des Risques (Dangers) a été développée au début des années 1960 dans les domaines aéronautiques et militaires. Utilisée depuis dans de nombreuses autres industries, l'Union des Industries Chimiques (UIC) recommande son utilisation en France depuis le début des années 1980. L'analyse Préliminaire des Risques (APR) est une méthode d'usage très général couramment utilisée pour l'identification des risques au stade préliminaire de la conception d'une installation ou d'un projet. En conséquence, cette méthode ne nécessite généralement pas une connaissance approfondie et détaillée de l'installation étudiée. En ce sens, elle est particulièrement utile dans les situations suivantes :

- **Au stade de la conception d'une installation,** lorsque la définition précise du procédé n'a pas encore été effectuée. Elle fournit une première analyse de sécurité se traduisant par des éléments constituant une ébauche des futures consignes d'exploitation et de sécurité. Elle permet également de choisir les équipements les mieux adaptés.

- **Dans le cas d'une installation complexe existante,** au niveau d'une démarche d'analyse des risques. Comme l'indique son nom, l'APR constitue une étape préliminaire, permettant de mettre en lumière des éléments ou des situations nécessitant une attention plus particulière et en conséquence l'emploi de méthodes d'analyses de risques plus détaillées. Elle peut ainsi être complétée par une méthode de type AMDEC ou arbre des défaillances par exemple.

- **Dans le cas d'une installation dont le niveau de complexité ne nécessite pas d'analyses plus poussées,** au regard des objectifs fixés au départ de l'analyse des risques

b) **Principe :**

- L'analyse Préliminaire des Risques nécessite dans un premier temps d'identifier les éléments dangereux de l'installation. Ces éléments

dangereux désignent le plus souvent : Des substances ou préparations dangereuses, que ce soit sous forme de matières premières, de produits finis, d'utilités... ;

- des équipements dangereux comme par exemple des stockages, zones de réception expédition, réacteurs, fournitures d'utilités (chaudière...) ;
- Des opérations dangereuses associées au procédé.

L'identification de ces éléments dangereux est fonction du type d'installation étudiée. Il est également à noter que l'identification de ces éléments se fonde sur la description fonctionnelle réalisée avant la mise en œuvre de la méthode. À partir de ces éléments dangereux, l'APR vise à identifier, pour un élément dangereux, une ou plusieurs **situations de dangers**. Dans le cadre de ce document, une situation de dangers est définie comme une situation qui, si elle n'est pas maîtrisée, peut conduire à l'exposition de cibles à un ou plusieurs phénomènes dangereux. Le groupe de travail doit alors en déterminer les causes et les conséquences de chacune des situations de dangers identifiés puis identifier les sécurités existantes sur le système étudié. Si ces dernières sont jugées insuffisantes vis-à-vis du niveau de risque identifié dans la grille de criticité, des propositions d'améliorations doivent alors être envisagées

c) Limites et avantages : Le principal avantage de l'Analyse Préliminaire des Risques est de permettre un examen relativement rapide des situations dangereuses sur des installations. Par rapport aux autres méthodes présentées ci-après, elle apparaît comme relativement économique en terme de temps passé et ne nécessite pas un niveau de description du système étudié très détaillé. Cet avantage est bien entendu à relier au fait qu'elle est généralement mise en œuvre au stade de la conception des installations.

En revanche, l'APR ne permet pas de caractériser finement l'enchaînement des évènements susceptibles de conduire à un accident majeur pour des systèmes complexes. Comme son nom l'indique, il s'agit à la base d'une méthode préliminaire d'analyse qui permet d'identifier des points critiques devant faire l'objet d'études plus détaillées. Elle permet ainsi de mettre en lumière les équipements ou installations qui peuvent nécessiter une étude plus fine menée grâce à des outils comme l'AMDEC, l'HAZOP ou l'analyse par arbre des défaillances.

Toutefois, son utilisation seule peut être jugée suffisante dans le cas d'installations simples ou lorsque le groupe de travail possède une expérience significative de ce type d'approches.

III.3.2. AMDE ET ADMEC

a) **Historique et domaine d'application :** L'analyse des Modes de Défaillance et de leurs Effets (AMDE) a été employée pour la première fois dans le domaine de l'industrie aéronautique durant les années 1960. Son utilisation s'est depuis largement répandue à d'autres secteurs d'activités telles que l'industrie chimique, pétrolière ou le nucléaire. De fait, elle est essentiellement adaptée à l'étude des défaillances de matériaux et d'équipements et peut s'appliquer aussi bien à des systèmes de technologies différentes (systèmes électriques, mécaniques, hydrauliques...) qu'à des systèmes alliant plusieurs techniques

b) **Principe :** L'analyse des Modes de Défaillance et de leurs Effets repose notamment sur les concepts de :

- **Défaillance** : soit la cessation de l'aptitude d'un élément ou d'un système à accomplir une fonction requise ;
- **Mode de défaillance** : soit l'effet par lequel une défaillance est observée sur un élément du système ;
- **Cause de défaillance** : soit les évènements qui conduisent aux modes de défaillances ;
- **Effet d'un mode de défaillance** : soit les conséquences associées à la perte de l'aptitude d'un élément à remplir une fonction requise.

En pratique, il est souvent difficile de bien distinguer ces différentes notions. La maîtrise de ce vocabulaire est néanmoins primordiale pour une bonne utilisation de cet outil. Pour illustrer ces différents concepts, prenons l'exemple d'une pompe. Dans des conditions normales d'exploitation, la fonction de cette pompe est sera définie comme son aptitude à fournir un débit donné à sa sortie. Si le débit en sortie de pompe est nul, nettement inférieur ou supérieur à ce débit défini, la pompe sera dite « défaillante ». Si, en cours d'exploitation, la pompe s'arrête de façon non désirée, on assistera bien à une défaillance de la pompe. Le fait que la pompe s'arrête constitue donc un effet par lequel une défaillance est observée ; il s'agit d'un mode de défaillance. La coupure de courant qui a entraîné l'arrêt de la

pompe sera alors définie comme une des causes de ce mode de défaillance. L'arrêt de l'approvisionnement du réacteur alimenté par cette pompe suivie d'une dégradation du produit de synthèse constituera des conséquences de cette défaillance.

L'AMDE est une méthode inductive d'analyse qui permet :

- d'évaluer les effets et la séquence d'évènements provoqués par chaque mode de défaillance des composants d'un système sur les diverses fonctions de ce système ;
- Déterminer l'importance de chaque mode de défaillance sur le fonctionnement normal du système et en évaluer l'impact sur la fiabilité, la sécurité du système considéré ;
- Hiérarchiser les modes de défaillances connus suivant la facilité que l'on a à les détecter et les traiter.

Lorsqu'il est nécessaire d'évaluer la criticité d'une défaillance (probabilité et gravité), l'Analyse des Modes de Défaillance de leurs Effets et de leur Criticité (AMDEC) apparaît comme une suite logique à l'AMDE. L'AMDEC reprend en effet les principales étapes de l'AMDE et y ajoute une évaluation semi quantitative de la criticité.

c) **Limites et avantages :** L'AMDEC s'avère très efficace lorsqu'elle est mise en œuvre pour l'analyse de défaillances simples d'éléments conduisant à la défaillance globale du système. De par son caractère systématique et sa maille d'étude généralement fine, elle constitue un outil précieux pour l'identification de défaillances potentielles et les moyens d'en limiter les effets ou d'en prévenir l'occurrence. Comme elle consiste à examiner chaque mode de défaillance, ses causes et ses effets pour les différents états de fonctionnement du système, l'AMDEC permet d'identifier les modes communs de défaillances pouvant affecter le système étudié. Les modes communs de défaillances correspondent à des événements qui de par leur nature ou la dépendance de certains composants provoquent simultanément des états de panne sur plusieurs composants du système. Les pertes d'utilités ou des agressions externes majeures constituent généralement des modes communs de défaillance. Dans le cas de systèmes particulièrement complexes comptant un grand nombre de

composants, l'AMDEC peut être très difficile à mener et particulièrement fastidieuse compte tenu du volume important d'informations à traiter. Cette difficulté est décuplée lorsque le système considéré comporte de nombreux états de fonctionnement. Par ailleurs, l'AMDEC considère des défaillances simples et peut être utilement complété, selon les besoins de l'analyse, par des méthodes dédiées à l'étude de défaillances multiples comme l'analyse par arbre des défaillances par exemple. **(voir annexe G)**

III.3.3. Arbre des défaillances

a) **Historique et domaine d'application :** L'analyse par arbre des défaillances fut historiquement la première méthode mise au point en vue de procéder à un examen systématique des risques. Elle a été élaborée au début des années 1960 par la compagnie américaine Bell Téléphone et fut expérimentée pour l'évaluation de la sécurité des systèmes de tir de missiles. Visant à déterminer l'enchaînement et les combinaisons d'évènements pouvant conduire à un événement redouté pris comme référence, l'analyse par arbre des défaillances est maintenant appliquée dans de nombreux domaines tels que l'aéronautique, le nucléaire, l'industrie chimique... Elle est aussi utilisée pour analyser a posteriori les causes d'accidents qui se sont produits. Dans ces cas, l'événement redouté final est généralement connu car observé. On parle alors d'analyse par arbre des causes, l'objectif principal étant de déterminer les causes réelles qui ont conduit à l'accident.

b) **Principe :** L'analyse par arbre de défaillances est une méthode de type déductif. En effet, il s'agit, à partir d'un événement redouté défini a priori, de déterminer les enchaînements d'évènements ou combinaisons d'évènements pouvant finalement conduire à cet événement. Cette analyse permet de remonter de causes en causes jusqu'aux évènements de base susceptibles d'être à l'origine de l'événement redouté. Les évènements de base correspondent généralement à des :

- Évènements élémentaires qui sont suffisamment connus et décrits par ailleurs pour qu'il ne soit pas utile d'en rechercher les causes. Ainsi, leur probabilité d'occurrence est également connue ;
- Évènements ne pouvant être considérés comme élémentaires mais dont les causes ne seront pas développées faute d'intérêt ;

- Évènements dont les causes seront développées ultérieurement au gré d'une nouvelle analyse par exemple ;
- Évènements survenant normalement et de manière récurrente dans le fonctionnement du procédé ou de l'installation ;
- Quelle que soit la nature des éléments de base identifiés, l'analyse par arbre des défaillances est fondée sur les principes suivants :
  - ✓ Ces évènements sont indépendants ;
  - ✓ Ils ne seront pas décomposés en éléments plus simples faute de renseignements, d'intérêt ou bien parce que cela est impossible ;
  - ✓ Leur fréquence ou leur probabilité d'occurrence peut être évaluée.

Ainsi, l'analyse par arbre des défaillances permet d'identifier les successions et les combinaisons d'évènements qui conduisent des évènements de base jusqu'à l'événement indésirable retenu. Les liens entre les différents évènements identifiés sont réalisés grâce à des portes logiques (de type « ET » et « OU » par exemple). Cette méthode utilise une symbolique graphique particulière qui permet de présenter les résultats dans une structure arborescente. Les conventions de présentation sont proposées dans la norme CEI 61025 :1990 « Analyse par Arbre de Panne (APP) ». A l'aide de règles mathématiques et statistiques, il est alors théoriquement possible d'évaluer la probabilité d'occurrence de l'événement final à partir des probabilités des évènements de base identifiés. L'analyse par arbre des défaillances d'un événement redouté peut se décomposer en trois étapes successives :

- ✓ Définition de l'événement redouté étudié ;
- ✓ laboration de l'arbre ;
- ✓ Exploitation de l'arbre.

Il convient d'ajouter à ces étapes, une étape préliminaire de connaissance du système. Nous verrons que cette dernière est primordiale pour mener l'analyse et qu'elle nécessite le plus souvent une connaissance préalable des risques.

c) **Limites et avantages :** Le principal avantage de l'analyse par arbre des défaillances est qu'elle permet de considérer des combinaisons d'évènements pouvant conduire in fine à un événement redouté. Cette possibilité permet une bonne adéquation avec l'analyse d'accidents passés qui montre que les accidents majeurs observés résultent le plus souvent de la conjonction de plusieurs évènements qui seuls n'auraient pu entraîner de tels sinistres. Par ailleurs, en visant à l'estimation des probabilités d'occurrence des évènements conduisant à l'événement final, elle permet de disposer de critères pour déterminer les priorités pour la prévention d'accidents potentiels. L'analyse par arbre des défaillances porte sur un événement particulier et son application à tout un système peut s'avérer fastidieuse. En ce sens, il est conseillé de mettre en œuvre au préalable des méthodes inductives d'analyse des risques. Ces outils permettent d'une part d'identifier les évènements les plus graves qui pourront faire l'objet d'une analyse par arbre des défaillances et d'autre part, de faciliter la détermination des causes immédiates, nécessaires et suffisantes au niveau de l'élaboration de l'arbre. Depuis une dizaine d'années, des logiciels informatiques sont commercialisés afin de rendre plus aisée l'application de l'arbre des défaillances. Ces outils se montrent très utiles pour la recherche des coupes minimales, la détermination des probabilités ainsi que pour la présentation graphique des résultats sous forme arborescente.

III.3.4. Arbre des évènements

a) **Historique et domaine d'application :** L'analyse par arbre d'évènements a été développée au début des années 1970 pour l'évaluation du risque lié aux centrales nucléaires à eau légère. Particulièrement utilisée dans le domaine du nucléaire, son utilisation s'est étendue à d'autres secteurs d'activité. De par sa complexité proche de celle de l'analyse par arbre des défaillances, cette méthode s'applique préférentiellement sur des sous-systèmes bien déterminés. Elle apporte une aide précieuse pour traiter des systèmes comportant de nombreux dispositifs de sécurité et de leurs interactions. À l'instar de l'analyse par arbre des défaillances dont elle s'inspire, elle permet d'estimer les probabilités d'occurrence de séquences accidentelles. Cette méthode est particulièrement utilisée dans le domaine de l'analyse après accidents en vue d'expliquer les conséquences observées résultant d'une défaillance du système.

b) Principe : L'analyse par arbre des défaillances, comme nous l'avons vu précédemment, vise à déterminer, dans une démarche déductive, les causes d'un événement indésirable ou redouté retenu a priori. À l'inverse, l'analyse par arbre d'évènements suppose la défaillance d'un composant ou d'une partie du système et s'attache à déterminer les évènements qui en découlent. À partir d'un événement initiateur ou d'une défaillance d'origine, l'analyse par arbre d'évènements permet donc d'estimer la dérive du système en envisageant de manière systématique le fonctionnement ou la défaillance des dispositifs de détection, d'alarme, de prévention, de protection ou d'intervention... Ces dispositifs peuvent concerner aussi bien des moyens automatiques qu'humains (intervention des opérateurs) ou organisationnels (application de procédures).

La démarche généralement retenue pour réaliser une analyse par arbre d'évènements est la suivante :

- Définir l'événement initiateur à considérer ;
- Identifier les fonctions de sécurité prévues pour y faire face ;
- Construire l'arbre ;
- Décrire et exploiter les séquences d'évènements identifiées.

Les paragraphes suivants décrivent ces différentes étapes en suivant un exemple inspiré de l'ouvrage « Guidelines for Hazard Evaluation Procédures », cité en références.

c) Limites et avantages : Le Nœud Papillon offre une visualisation concrète des scénarios d'accidents qui pourraient survenir en partant des causes initiales de l'accident jusqu'aux conséquences au niveau des cibles identifiées. De ce fait, cet outil met clairement en valeur l'action des barrières de sécurité s'opposant à ces scénarios d'accidents et permet d'apporter une démonstration renforcée de la maîtrise des risques. En revanche, il s'agit d'un outil dont la mise en œuvre peut être particulièrement coûteuse en temps. Son utilisation doit donc être décidée pour des cas justifiant effectivement un tel niveau de détail.

III.3.5. Diagramme causes-conséquences

Cette méthode se révèle intéressante pour l'analyse des causes et des conséquences d'un événement initiateur que l'on redoute de voir survenir dans un système. Elle se caractérise par le caractère presque simultané de l'analyse déductive des causes et de l'analyse

inductive des conséquences. Elle est intéressante pour l'analyse des systèmes où l'ordre dans lequel surviennent les défaillances est important ; néanmoins, elle apparaît difficile à utiliser pour l'analyse de systèmes trop complexes.

III.3.6. HAZOP

a) **Historique et domaine d'application :** La méthode HAZOP, pour HAZard OPerability, a été développée par la société Imperial Chemical Industries (ICI) au début des années 1970. Elle a depuis été adaptée dans différents secteurs d'activité. L'Union des Industries Chimiques (UIC) a publié en 1980 une version française de cette méthode dans son cahier de sécurité n°2 intitulé « Etude de sécurité sur schéma de circulation des fluides ». Considérant de manière systématique les dérives des paramètres d'une installation en vue d'en identifier les causes et les conséquences, cette méthode est particulièrement utile pour l'examen de **systèmes thermo-hydrauliques**, pour lesquels des paramètres comme le débit, la température, la pression, le niveau, la concentration... sont particulièrement importants pour la sécurité de l'installation. De par sa nature, cette méthode requiert notamment l'examen de schémas et plans de circulation des fluides ou schémas P&ID (Piping and Instrumentation Diagram)

b) **Principe : La méthode de type HAZOP est dédiée à l'analyse des risques des systèmes thermo-hydrauliques** pour lesquels il est primordial de maîtriser des paramètres comme la pression, la température, le débit... L'HAZOP suit une procédure assez semblable à celle proposée par l'AMDE. L'HAZOP ne considère plus des modes de défaillances mais les dérives potentielles (ou déviations) des principaux paramètres liés à l'exploitation de l'installation. De ce fait, elle est centrée sur l'installation à la différence de l'AMDE qui est centré sur les composants. Pour chaque partie constitutive du système examiné (ligne ou maille), la génération (conceptuelle) des dérives est effectuée de manière systématique par la conjonction :

- de **mots-clé** comme par exemple « Pas de », « Plus de », « Moins de », « Trop de » ;
- des **paramètres** associés au système étudié. Des paramètres couramment rencontrés concernent la température, la pression, le débit, la concentration, mais également le temps ou des opérations à effectuer.

Le groupe de travail doit ainsi s'attacher à déterminer les causes et les conséquences potentielles de chacune de ces dérives et à identifier les moyens existants permettant de détecter cette dérive, d'en prévenir l'occurrence ou d'en limiter les effets. Le cas échéant, le groupe de travail pourra proposer des mesures correctives à engager en vue de tendre vers plus de sécurité. A l'origine, l'HAZOP n'a pas été prévue pour procéder à une estimation de la probabilité d'occurrence des dérives ou de la gravité de leurs conséquences. Cet outil est donc parfois qualifié de qualitatif. Néanmoins, dans le domaine des risques accidentels majeurs, une estimation a priori de la probabilité et de la gravité des conséquences des dérives identifiées s'avère souvent nécessaire. Dans ce contexte, l'HAZOP doit donc être complété par une analyse de la criticité des risques sur les bases d'une technique quantitative simplifiée.

c) **Limites et avantages :** L'HAZOP est un outil particulièrement efficace pour les systèmes thermo-hydrauliques. Cette méthode présente tout comme l'AMDE un caractère systématique et méthodique. Considérant, de plus, simplement les dérives de paramètres de fonctionnement du système, elle évite entre autres de considérer, à l'instar de l'AMDE, tous les modes de défaillances possibles pour chacun des composants du système. En revanche, l'HAZOP permet difficilement d'analyser les évènements résultant de la combinaison simultanée de plusieurs défaillances. Par ailleurs, il est parfois difficile d'affecter un mot clé à une portion bien délimitée du système à étudier. Cela complique singulièrement l'identification exhaustive des causes potentielles d'une dérive. En effet, les systèmes étudiés sont souvent composés de parties interconnectées si bien qu'une dérive survenant dans une ligne ou maille peut avoir des conséquences ou à l'inverse des causes dans une maille voisine et inversement. Bien entendu, il est possible a priori de reporter les implications d'une dérive d'une partie à une autre du système. Toutefois, cette tâche peut rapidement s'avérer complexe.

III.3.7. La méthode « What if »

La méthode dite « What if » est une méthode dérivée de l'HAZOP. Elle suit donc globalement la même procédure et les informations présentées au paragraphe précédent pour l'HAZOP restent donc valables ici. La principale différence concerne la génération des dérives des paramètres de fonctionnement. Ces dérives ne sont plus dans ce cas envisagées en tant que combinaison d'un mot clé et d'un paramètre, mais fondées sur une

succession de questions de type de la forme : « QUE (What) se passe-t-il SI (IF) tel paramètre ou tel comportement est différent de celui normalement attendu ? ». Il apparaît ainsi que l'efficacité de la méthode « What if » repose en grande partie sur l'expérience des personnes réunies au sein du groupe de travail. Cette méthode paraît donc moins fastidieuse à mener que l'HAZOP mais est réservée à une équipe expérimentée

III.3.8. Méthode MOSAR

Cette méthode s'appuie fondamentalement sur une décomposition systémique de l'installation étudiée. L'analyse et l'identification des risques s'y fait d'une façon systématique en s'appuyant sur des grilles typologiques ainsi que sur diverses techniques existantes comme la technique des arbres**. Associée** à MOSAR (Méthode Organisée Systémique d'Analyse des Risques), elle fournit un langage, peut être trop empruntée à la systémique, mais aussi des outils opérationnels pour l'analyse des risques.

III.4. Tableau récapitulatif

Le tableau suivant présente pour chacune des méthodes de sécurité des systèmes décrites, leur positionnement par rapport aux critères de comparaison énoncés antérieurement.

Tableau III.1. Tableau récapitulatif des principales méthodes d'analyse des risques du courant « Sûreté de fonctionnement ».

Critères		Méthodes					
		APR	AMDEC	AdD	AdE	Diag causes-conséquences	MOSAR
Etapes Formalisation	Définition du système	Non	Oui	Non	Non	Non	Oui
	Identification des risques	Oui	Oui	Non	Non	Non	Oui
Etapes Formalisation	Définition du système	Non	Oui	Non	Non	Non	Oui
	Identification des risques	Oui	Oui	Non	Non	Non	Oui
	Identification des mécanismes générateurs de risques	Oui	Oui	Oui	Oui	Oui	Oui
	Evaluation	Non	Oui	Oui	Non	Non	Oui
	Hiérarchisation	Non	Oui	Non	Non	Non	Oui
	Identification des solutions	Oui	Oui	Non	Non	Non	Oui
Victimes prises en compte	Installation	X					X
	Homme au travail	X					X
	Ecosystème	X					X

Types de facteurs de risques envisagés	Technologiques	X	X	X	X	X	X
	Humains	X	Possible	X			X
	Organisationnels	Possibl e	Possible				Possible
Modèle d'accident		Oui	Oui (faible)	Oui (faible)	Non	Implicite	Oui
Sens d'investigation		Inductif	Inductif	Déductif	Induc tif	Inductif et déductif	Inductif et déductif possible

Après cette comparaison des différentes méthodes à utiliser lors d'une analyse des risques, le choix d'une méthode à utiliser pour décrire les risques liés à une installation industrielle doit répondre aux critères suivants :

- Formalisation des étapes de l'analyse des risques ;
- La considération simultanée de l'installation, de l'homme au travail et des écosystèmes comme victimes potentielles du risque ;
- L'utilisation formelle d'un modèle d'accident ;
- La prise en compte des facteurs de risques (technologiques, humains et organisationnels).

Parmi les méthodes les plus utilisées, on peut trouver l'APR, l'AMDEC et MOSAR. Ces deux dernières offrent l'avantage d'avoir une formalisation des étapes de hiérarchisation et d'évaluation du risque.

III.5. Démarche d'analyse des risques par la méthode MADS-MOSAR

III.5.1. Introduction

Nous vivions de plus en plus dangereusement ; l'actualité foisonne de catastrophes humaines, matérielles et financières dues à des événements non souhaités.

La science du danger et particulièrement l'analyse du risque apporte des éléments très importants pour identifier, imaginer des scénarios de risque, prévoir leurs probabilités d'occurrence et leurs coûts induits, définir et dimensionner des barrières préventives afin de les rendre acceptables.

MOSAR (Méthode Organisée et Systémique d'Analyse des Risques) est une méthode d'analyse des risques prenant en compte l'identification exhaustive ou non des risques encourus par le système à étudier, l'évaluation du niveau de danger de ceux-ci, la mise en place de barrières et enfin l'impact de ces barrières sur le niveau du risque.

Les objectifs de cette méthode sont :

- Identifier et évaluer les risques du système à étudier ;
- Négocier les objectifs et l'acceptabilité du risque par les acteurs concernés ;
- Intégrer les réglementations spécifiques ;
- Mettre en œuvre de concepts logiques ;
- Mettre en œuvre de concepts systémiques ;
- Mettre en œuvre d'outils (AMDEC, AdD,…etc.) ;
- Avoir une vision macroscopique et microscopique du système. **[8]**

III.5.2. Structure de la méthode

La méthode s'articule autour de deux visions, d'où les deux modules (A et B) qui la composent.

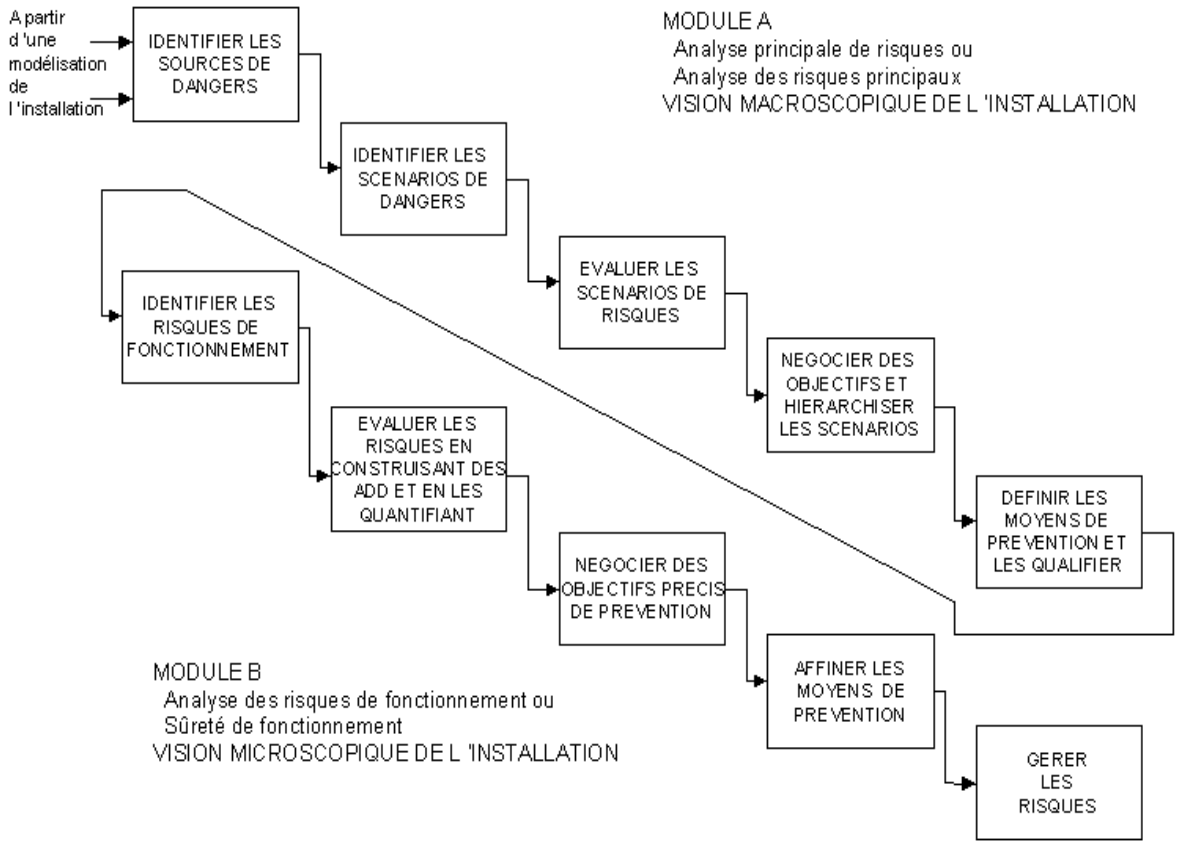

Figure III.4. Structure de la méthode MADS MOSAR.

Une vision **macroscopique** conduisant à un module A qui consiste à faire une analyse des risques de proximité (analyse des risques principaux). Les éléments de l'installation sont modélisés sous forme de systèmes ce qui va permettre d'identifier en quoi ils peuvent être

sources de danger, l'interaction entre eux et avec leur environnement pour générer des scénarios d'accidents.

Une vision **microscopique** conduisant à un module B qui consiste à faire une analyse détaillée et complète des dysfonctionnements techniques et opératoires identifiés dans le module A. c'est en fait une approche de type « sûreté de fonctionnement ». Dans les scénarios établis dans le premier module, on va développer les dysfonctionnements de nature opératoire et ceux de nature technique en mettant en œuvre des outils comme les AMDEC et les arbres logiques. **[8]**

Il s'agit ici de réaliser le modula A pour le système turbopompe.

III.5.3. Les étapes de la méthode

Le déroulement complet de la démarche consiste ainsi à parcourir les étapes suivantes, d'une part pour l'approche macroscopique :

- Identification des sources de danger ;
- Identification des scénarios de risques ;
- Evaluation des scénarios de risques ;
- Négociation des objectifs et hiérarchisation des scénarios ;
- Définition des moyens de prévention et leur qualification.

Puis pour l'approche microscopique :

- Identification des risques de fonctionnement ;
- Evaluation des risques à partir d'arbres ;
- Négociation des objectifs précis de prévention ;
- Affinement des moyens de prévention ;
- Gestion des risques.

III.5.4. Les étapes du module A

- **1ére étape : Identification des sources de danger :** Le premier travail est d'identifier les sources de danger de chaque sous-système ou d'identifier en quoi chaque sous-système peut être source de danger. En faisant cette identification pour tous les sous-systèmes, on obtient une liste des dangers de l'installation (cette liste n'est pas exhaustive, en effet, il est toujours possible de retrouver d'autres sources de danger). Le deuxième travail est l'identification des processus de danger. Ligne

par ligne, on va rechercher les événements qui constituent les processus de danger pour aboutir à un ou plusieurs événements principaux.

- **2éme étape : Identification des scénarios de risques :** La première partie de ce travail consiste à isoler chaque sous-système. En reprenant chaque sous-système et on les représente sous forme de boîtes dont les entrées sont les événements initiateurs d'origine externe ou interne et les sorties sont les événements principaux. Ensuite, il s'agit de s'occuper de la génération des scénarios courts et des scénarios longs.
- **3éme étape : Evaluation des scénarios de risques :** Cette étape permet d'évaluer les risques quantitativement ou qualitativement. On évalue tout d'abord la gravité d'un scénario en jugeant l'impact des conséquences de l'événement final.
- **4éme étape : Négociation des objectifs et hiérarchisation des scénarios**
- **5éme étape : Définition des moyens de prévention et leur quantification**

Cette étape permet d'identifier des barrières de prévention et de protection. Ces barrières vont permettre de neutraliser les scénarios de risque, de les réduire en terme de gravité ou de fréquence ou des deux de manière à les rendre acceptables. Elles sont de deux ordres :

a) **Barrières technologiques (BT) :** Ce sont des éléments ou ensemble technologique faisant partie de l'installation empêchant l'apparition d'événement gênant et indépendant de l'activité humaine.

b) **Barrières opératoires ou d'utilisation (BU) :** Ce sont des actions nécessitant une intervention humaine, reposant sur une consigne précise, activée ou non par un ensemble technologique.

III.5.5. Conclusion

Cette association de méthodes présente alors plusieurs avantages : Elle permet une analyse détaillée et rigoureuse de l'ensemble de l'installation, le retour d'expérience peut être facilement intégré, et elle constitue un document de choix pour les entreprises.

Néanmoins, ces deux méthodes possèdent un inconvénient majeur qu'est leur mise en place. En effet, celle-ci s'avère longue et fastidieuse car elle nécessite une étude minutieuse et détaillée du système.