**1.1 Introduction**

Le risque est une notion difficile à cerner mais de façon générale, on peut dire que c'est une contingence indésirable, appréhendée, relativement anodine et peu probable. Par appréhendée, on entend par là que le risque est connu au préalable. L'exposition au risque résulte donc souvent d'une démarche consciente, appelée prise de risque. En ce sens, le risque distingue par exemple de l'aléa ou de l'incident, qui surviennent en général de façon imprévue. Un risque est une contingence peu probable, ce qui constitue une autre différence par rapport au danger. On parle en effet de danger lorsque la probabilité d'occurrence et les conséquences sont importantes, tandis que le risque existe dès lors que sa probabilité d'occurrence n'est pas nulle. Le choix de la méthode ou des méthodes nécessaires pour réaliser l’analyse des risques est primordial. Il n’existe pas une méthode unique miraculeuse qui permettrait à toutes les entreprises de toutes tailles et de tous secteurs d’analyser leurs risques afin de déterminer les mesures de prévention. Il existe donc des méthodes avec des objectifs différents, selon le besoin de l’entreprise dans la mise en place de son système dynamique de gestion des risques.

**1.2. Définition de risque industriel**

Le risque industriel est défini comme un évènement accidentel se produisant sur un site Industriel mettant en jeu des produits et/ou des procédés dangereux et entraînant des conséquences immédiates graves pour le personnel, les riverains, les biens et l'environnement **[4]**.

**1.3. Les facteurs de risque industriel**

**1.3.1. Danger:** Un danger est une propriété ou une capacité d’un objet, d’une personne, d’un processus, pouvant entraîner des conséquences néfastes, aussi appelés dommages. Un danger est donc une source possible d’accident **[5]**.

**1.3.2. Risque:** Le risque est la probabilité que les conséquences néfastes, les dommages, se matérialisent effectivement. Un danger ne devient un risque que lorsqu’il y a exposition et donc, possibilité de conséquences néfastes **[5]**.

**1.3.3. Exposition:** Dans le présent contexte, quand on parle d’exposition, il s’agit du contact entre le danger et une personne, pouvant dès lors entraîner un dommage. Sans exposition, pas de possibilité de dommage. Le risque est donc la probabilité que quelqu’un soit atteint par un danger **[5]**.

**1.3.4. Facteur des risques:** Les facteurs de risques sont des éléments qui peuvent augmenter ou diminuer la probabilité de survenance d’un accident ou la gravité d’un événement Les facteurs de risques complètent l’équation:

**RISQUE = DANGER X EXPOSITION [5]**

**1. .4Typologie des risques industriels**

Les différentes catégories de risques**:**

**1.4.1 Incendie/explosion[4]**

Risque d’accident suite à un incendie ou à une explosion.



**Figure 1.1**: incendie /explosion

**1.4.1.1 Identification du risque d’incendie/explosion**

* Présence de matériaux ou produits combustibles (stockage de produits facilement
* Inflammables ou explosifs, stockage de papier, etc.)
* Présence d’équipement ou d’installation pouvant générer de la chaleur (soudage, etc.)
* Présence d’un comburant (oxygène, produits chimiques dégageant de l’oxygène, etc.)
* Stockage de produits incompatibles

**1.4.1.2 Modalités d’exposition**

* Toute situation de travail où se trouvent simultanément des
* Produits/matériaux combustibles, une source de chaleur et un comburant (air,…)

**1.4.1.2 Modalités d’exposition**

* Toute situation de travail où se trouvent simultanément des
* Produits/matériaux combustibles, une source de chaleur et un comburant (air,…)
* Utilisation de substances facilement inflammables
* Création d’une atmosphère explosive (gaz, vapeurs, poussières, etc.)
* Mélange de produits incompatibles

**1.4.1.3 Moyens de prévention**

* Formation, information et instruction du personnel
* Remplacement par des produits non dangereux et, si cela n’est possible, par des produits moins dangereux
* Organisation du stockage
* Organisation de l’alerte et de l’intervention des secours
* Contrôle des équipements et installations
* Signalisation et étiquetage appropriés.

**1.4.2 Risques biologiques[4]**

Risques d’infection, d’allergies ou d’intoxications résultant de la présence de microorganismes.

**1.4.2.1 Identification du risque biologique**

Dangers liés :

* Au degré de pathogénicité des agents biologiques
* Aux objets coupants, tranchants et piquants
* à la libération de produits biologiques allergisants ou toxiques
* à l’incertitude face à la pathogénicité de différents agents
* Aux produits dangereux pour l’environnement

**1.4.2.2 Modalités d’exposition**

* Toute situation de travail où existe la possibilité de contamination par différentes voies
* (Inhalation, ingestion, contact, pénétration suite à une lésion).
* Toute situation pouvant entraîner une propagation accidentelle dans l’environnement
* Travail de laboratoire sur microorganismes
* Travail en contact avec des animaux
* Soins aux personnes en milieu hospitalier
* Travail en contact avec des produits agroalimentaires

**1.4.2.3 Moyens de prévention**

* Information, formation et instruction des salariés
* Ventilation correcte des locaux
* Bonne gestion des déchets
* Utilisation des moyens de protection individuelle (faire porter des protections respiratoires, lunettes, gants, écran facial, etc.)
* Réduction des temps d’exposition et limiter le personnel exposé
* Procédures de décontamination
* Vaccinations et surveillance médicale des salariés concernés.

**1.4.3 Risques chimiques[4]**

Risques d’infections, d’allergies, d’intoxications ou de brûlures.



**Figure 1.2** : Produit chimique.

**1.4.3.1 Identification du risque chimique**

Dangers liés :

* Aux propriétés physico-chimiques (produits corrosifs, comburants, explosifs ou
* Inflammables)
* Aux propriétés toxicologiques (produits irritants, nocifs toxiques, cancérogènes, mutagènes, Etc.)
* Aux propriétés éco-toxicologiques
* à l’incertitude scientifique sur les dangers des produits synthétisés

**1.4.3.2. Modalités d’exposition**

* Toute situation de travail où existe la possibilité de contamination par différentes voies

(Inhalation, ingestion, contact, pénétration suite à une lésion)

Toute situation où les produits sont susceptibles de déclencher ou de propager un incendie

**1.4.3.3 Moyens de prévention**

* Information, formation et instruction du personnel
* Remplacer par des produits non dangereux et, si cela n’est pas possible, par des moins dangereux
* Réduction des quantités
* Limitation du nombre de salariés exposés et du temps d’exposition
* Vérification et entretien périodique des systèmes de captage à la source
* Organisation et conditions de stockage adaptées
* Port d’équipements de protection individuelle
* Surveillance médicale du personnel concerné.

**1.4.4 Risques physiques[4]**

Risques liés au bruit, aux vibrations et aux rayonnements.



**Figure 1.3 :** Les risques physiques au travail sont en hausse

**1.4.4.1 Identification Risques biologiques physique**

* Différents moyens de transport, installations, machines (bruit et vibrations)
* Présence de sources de rayonnements ionisants
* Présence de sources de rayonnements électromagnétiques
* Présence de sources de rayonnements infrarouge ou ultraviolet

**1.4.4.2 Modalités d’exposition**

* Bruit émis de façon continue par des machines, compresseurs, outils, moteurs, etc.
* Bruit d’impulsion des machines et outils travaillant par chocs
* Exposition à une amplitude sonore trop importante
* Vibrations émises par des moyens de transport, machines et outils
* Utilisation d’appareils générant des rayonnements ionisants
* Utilisation d’appareils générant des rayonnements optiques
* Utilisation d’appareils générant des rayonnements électromagnétiques
* Utilisation de matières émettant des rayonnements ionisants (matières radioactives)
* Toute situation où il y a possibilité de contamination, d’exposition externe/interne à des rayonnements
* Toute situation où des personnes peuvent s’exposé à une source de rayonnement.

**1.4.4.3 Moyens de prévention**

* Informer, former et instruire le personnel
* Essayer de supprimer les sources de bruit ou de vibrations
* Limiter le temps d’exposition du personnel
* Disposer les installations bruyantes dans des locaux séparés
* Installer des protections sonores
* Installer des isolations contre les vibrations
* Entretenir régulièrement les machines, outils et moyens de transport
* Utiliser les moyens de protection individuelle adaptés
* Disposer de lunettes adaptées aux rayonnements
* Respecter les valeurs limites
* Classer les locaux en zones surveillées ou contrôlées
* Adapter le stockage des sources rayonnantes et déchets rayonnants
* Assurer un suivi médical du personnel exposé.

**1.4.5 Risques liés à l’électricité[4]**

Risques d’accident résultant du contact avec des installations électriques.



**Figure 1.4 :** Accident d’origine électrique

**1.4.5.1 Identification du risque lie à l’électricité**

* Contact direct avec des éléments sous tension
* Contact indirect (arc électrique)

**1.4.5.2 Modalités d’exposition**

* Toute situation où il y a possibilité d’électrocution ou électrisation
* Conducteurs nus accessibles aux travailleurs
* Matériel défectueux, âgé ou usé
* Non-consignation d’une installation électrique lors d’une intervention

**1.4.5.3 Moyens de prévention**

* Information, formation et instruction du personnel
* Remplacement des équipements dangereux par des équipements non dangereux, et/ou, si cela n’est pas possible, par des équipements moins dangereux
* Contrôle et maintenance des installations
* Signalisation adaptée
* Protection ou éloignement des pièces nues sous tension
* Mise en place de consignes en cas d’intervention
* Dispositifs de coupure d’urgence
* Matériel à double isolation
* Equipements de protection individuelle adaptés
* Contrôles périodiques
* Respect des cinq règles de sécurité.

**1.4.6 Chutes[4]**

Risque d’accident résultant du contact brutal d’une personne avec le sol ou avec une autre surface suffisamment large et solide.

**1.4.6.1 Identification du risque lié aux chutes**

* Travail en hauteur
* Déplacements à pied



**Figure 1.5** : Chutes de hauteur / Chutes de plain-pied

**1.4.6.2 Modalités d’exposition**

* Déplacement sur un sol glissant et/ou encombré, déformé
* Déplacement sur un sol en dénivelé
* Travail en arête de chute (bordures de vide, quais de chargement, toits, terrasses, fenêtres, etc).
* Accès à des parties hautes (rayonnages, plafonds, armoires,…).
* Utilisation d’échelles, d’échafaudages, d’escaliers, d’escabeaux…

**1.4.6.3 Moyens de prévention**

* Formation, information et instruction du personnel
* Signalisation des arêtes de chute
* Signalisation des sols glissants
* Signalisation des sols déformés
* Réparation des chemins de circulation en mauvais état
* Montage des échafaudages par des personnes compétentes et selon les indications de fabricant
* Vérification de la conformité des matériels (échafaudages et échelles conformes et
* Maintenus en bon état)
* Eclairage correct
* Equipements de protection collective (garde-corps, etc.)
* Equipements de protection individuelle (chaussures de sécurité antidérapantes, harnais antichute, etc.)

**1.4.7 Chutes d’objets[4]**

Risques d’accident résultant de la chute d’objets lors du transport ou du stockage (p.ex.: d’un étage supérieur ou de l’effondrement de matériau) et lors de travaux en hauteur. Risques d’accident résultant de la chute d’objets lors du transport ou du stockage (p.ex.: d’un étage supérieur ou de l’effondrement de matériau) et lors de travaux en hauteur.



**Figure 1.6** : Chutes d’objets

**1.4.7.1 Identification Risques lié à la chute des objets**

* Lieux de travail superposés
* Objets stockés en hauteur
* Objets empilés sur une grande hauteur
* Travaux effectués à des hauteurs ou étages différents
* Travaux effectués dans des tranchées, des puits, des galeries, etc.
* Transports avec un appareil de levage (grues, ponts roulants, grues mobiles, etc).

**1.4.7.2 Modalités d’exposition**

* Travaux avec des objets pouvant tomber d’un niveau supérieur (matériel, outils, etc.)
* Objets empilés sans être sécurisés
* Stockage sur étagères multiples
* Travaux en dénivelé, en profondeur
* Utilisation d’échelles, d’échafaudages, grues, etc.

**1.4.7.3 Moyens de prévention**

* Formation, information et instruction du personnel
* Organisation du stockage: emplacements réservés, largeur des allées, stockage selon taille des objets, etc.
* Limiter la hauteur de stockage selon les caractéristiques des objets
* Installation de protections évitant la chute d’objets pendant des travaux sur échafaudages ou à différents niveaux
* Respect des indications de taille et de poids pour le stockage sur étagères
* Port des équipements de protection individuelle
* Protéger la charge contre la chute lors du transport avec grues
* Ne pas déplacer des charges au-dessus de personnes.

**1.4.8. Circulation[4]**

**1.4.8.1. Circulation dans l’entreprise (interne)**

Risques d’accident résultant du heurt d’une personne par un véhicule ou d’une collision entre véhicules ou entre un véhicule et un obstacle…



**Figure 1.7 :** Plan de circulation en milieu de travail.

**1.4.8.2 Circulation routière (externe)**

Risque d’accident de la circulation lié au déplacement d’un salarié réalisant une mission pour le compte de l’entreprise.



**Figure 1.8 :** Circulation externe.

**1.4.8.3 Identification du risque lié à la circulation :**

Déplacement en voiture ou par un autre véhicule motorisé (chariot élévateur) au sein de l’entreprise ou à l’extérieur pour le compte de l’entreprise.

**1.4.8.4 Modalités d’exposition**

* Utilisation de véhicules sur voie publique ou privée
* Zones de circulation communes pour piétons et véhicules
* Zones de manœuvre
* Etat des véhicules, équipements des véhicules
* Conduite inappropriée
* Utilisation de moyens de communication pendant la conduite (GSM, GPS, etc.).

**1.4.8.5. Moyens de prévention**

* Information, formation et instruction des salariés concernés
* Respect du code de la route
* Signalisation appropriée sur le site de l’entreprise
* Séparation des voies de circulation pour véhicules et piétons
* Eclairage et entretien des voies de circulation
* Entretien préventif des véhicules
* Réparation immédiate des dégâts
* Limiter les déplacements.

**1.5. Le concept d'analyse de risque**

Le concept d'analyse de risque pour un projet repose sur la démarche en 5 étapes, il s'agit d'un modèle de référence structurant les points suivants :

* Identification et classification des risques.
* Les conséquences du risque (financier, juridique, humain, ...).
* La gestion du risque (prévention, protection, évitement de risque, transfert).
* Maîtrise interne ou transfert vers un tiers (externalisation, assurance). **[5]**

**1.6. Les méthodes d’analyses les risques [7]**

Le choix de la méthode ou des méthodes nécessaires pour réaliser l’analyse des risques est primordial. Il n’existe pas une méthode unique miraculeuse qui permettrait à toutes les entreprises de toutes tailles et de tous secteurs d’analyser leurs risques afin de déterminer les mesures de prévention. Il existe donc des méthodes avec des objectifs différents, selon le besoin de l’entreprise dans la mise en place de son système dynamique de gestion des risques.

Les principales méthodes d’analyse les risques :

* L’analyse préliminaire des risques (APR).
* L’analyse des modes de défaillance de leur effet et de leur criticité (AMDEC).
* L’analyse des risques sur schémas type HAZOP.
* L’analyse par arbres des défaillances (AdD).
* L’analyse par arbres d’évènements (AdE).
* L’analyse par NoeudPapillon.
* L’analyse par la méthode HIRA

**1.6.1 Analyse préliminaire des risques (APR) :**

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 **[7]**

**1.6.1.1 Les principes**

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. L’APR peut être mise en œuvre sans ou avec l’aide de liste de risques types ou en appliquant les mots guides Hazop. 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.

A partir de ces éléments dangereux, l’APR vise à identifier, pour un élément dangereux, une ou plusieurs situations de danger. Dans le cadre de ce document, une situation de danger est définie comme une situation qui, si elle n’est pas maîtrisée, peut conduire à l’exposition d’enjeux à un ou plusieurs phénomènes dangereux.

Le groupe de travail doit alors déterminer les causes et les conséquences de chacune des situations de danger identifiées 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’amélioration doivent alors être envisagées **[7]**.

**1.6.1.2 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 termes 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 tels que 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 **[7]**.

**1.6.2 La méthode HAZOP**

La méthode HAZOP s’intègre dans une démarche d’amélioration de la sécurité et des procédés pour une installation existante ou en projet, avec ses avantages :

* Réalisation de l’étude au sein d’un groupe de travail rassemblant différents métiers : sécurité, ingénierie, exploitation, maintenance…
* Méthode d’analyse systématique liée aux installations avec circuits fluides
* Contribution au respect des normes en matière de sécurité **[9]**.

**1.6.2.1 Description de la méthode:**

* Définition du système à étudier
* Prise de connaissance du système
* Eléments spécifiques à la méthode
* Présentation du tableau HAZOP
* Analyse des dysfonctionnements et mise en place de recommandations
* Quand utiliser HAZOP ?
* Application de la méthode sur un cas d’école **[9]**

**1.6.2.2 Les avantages et les limites**

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 ne permet pas dans sa version classique 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.

Enfin, L’HAZOP traitant de tous types de risques, elle peut être particulièrement longue à mettre en œuvre et conduire à une production abondante d’information ne concernant pas des scénarios d’accidents majeurs **[7]**.

**1.6.3 La méthode arbre d’événement**

L’arbre d’événements illustre graphiquement les conséquences potentielles d’un accident qui résulte d’un événement initiateur (une défaillance spécifique d’un équipement ou une erreur humaine). Une analyse par arbre d’événements (AAE) prend en compte la réaction des systèmes de sécurité et des opérateurs à l’événement initiateur lors de l’évaluation des conséquences potentielles de l’accident. Les résultats de l’AAE sont des séquences accidentelles; c’est-à-dire un ensemble de défaillance ou d’erreurs qui conduisent à l’accident. Ces résultats décrivent les conséquences potentielles en termes de séquence d’événements (succès ou défaillance des fonctions de sécurité) qui font suite à un événement initiateur. Une analyse par arbre d’événements est bien adaptée pour étudier des procédés complexes qui ont plusieurs barrières de protection ou procédures d’urgence en place pour réagir à un événement initiateur spécifique **[11]**.

**1.6.3.1 Principe de l’arbre d’événements**

L’ADE évalue le potentiel d’accident résultant d’une défaillance d’un équipement ou d’un dérangement de procédé (événement initiateur). À la différence de l’analyse par arbre de panne (une approche déductive) l’AAE est un raisonnement inductif où l’analyste commence par un événement initiateur et développe la séquence probable d’événements qui conduisent aux accidents potentiels, en tenant compte tant du succès que de la défaillance des barrières de sécurité au fur et à mesure que l’accident progresse. Les arbres d’événements fournissent une façon systématique d’enregistrer les séquences d’accidents et de définir la relation entre les événements initiateurs et la séquence d’événements qui peut résulter en accidents.

Les arbres d’événements sont bien indiqués pour analyser les événements initiateurs qui pourraient conduire à une variété de conséquences. Un arbre d’événements met en évidence la cause initiale d’accidents potentiels et fonctionne à partir de l’événement initiateur jusqu’aux effets finaux. Chaque branche d’un arbre d’événements représente une séquence séparée d’accident qui est, pour un événement initiateur donné, un ensemble de relations entre les barrières de sécurité **[11]**.

**1.6.3.2 Les avantages et les limites**

L’analyse par arbre d’évènements est une méthode qui permet d’examiner, à partir d’un événement initiateur, l’enchaînement des évènements pouvant conduire ou non à un accident potentiel. Elle trouve ainsi une utilité toute particulière pour l’étude de l’architecture des moyens de sécurité (prévention, protection, intervention) existants ou pouvant être envisagés sur un site. A ce titre, elle peut être utilisée pour l’analyse d’accidents a posteriori. Cette méthode peut s’avérer lourde à mettre en œuvre. En conséquence, il faut définir avec discernement l’événement initiateur qui fera l’objet de cette analyse **[7]**.

**1.6.4 La méthode NoeudPapillon**

Le noeudpapillon utilisé dans de nombreux secteurs industriels a été développé par la compagnie Shell. L’approche est de type dit arborescente ce qui permet de visualiser en un coup d’œil les causes possibles d’un accident, ses conséquences et les barrières mises en place. L’accident non désiré (au centre) peut être le résultat de plusieurs causes possibles telles que la perte de confinement d’une substance toxique, une explosion, une rupture de canalisation, un emballement de réaction, une brèche dans un réservoir, une décomposition d’une substance, etc. Cet outil permet d’illustrer le résultat d’une analyse de risque détaillée (de type AMDEC, HAZOP ou What-if par exemple) donc plus complexe qu’une analyse préliminaire de risques **[12]**.



**Figure 1.9 :** Exemple de la méthode Nœud de Papillon

La partie gauche du nœud représente l’identification des dangers, des causes possibles d’accident et des divers enchaînements ou combinaisons (flèches noires) pouvant engendrer l’accident non désiré. Entre ces causes possibles et l’accident, des barrières dites de prévention (rectangles orange) doivent être installées.

La partie droite du nœud représente les conséquences possibles de l’accident. Par exemple, lors de la rupture d’une canalisation ou d’une brèche dans un réservoir, il peut en résulter la formation d’une flaque ou d’un nuage. Entre cet accident et les récepteurs, des barrières de protection doivent être installées pour réduire les effets sur ces récepteurs.

Donc, le nœud papillon reflète les scénarios d’accident qui peuvent survenir et les mesures prises pour les prévenir ou en réduire la probabilité ainsi que celles prises pour en réduire les conséquences. On parle de barrières de prévention et de barrières de protection. Les barrières de protection abaissent le niveau de gravité des conséquences et celles de prévention abaissent la probabilité. À l’aide d’une matrice (du type utilisé dans une analyse préliminaire des risques)où on établit notre zone d’acceptabilité, l’effet des barrières est visible et peut rendre tolérable une situation qui était au départ inacceptable **[12]**.

**1.6.4.2 Les avantages et les limites**

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 éléments vulnérables identifiés. 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 **[7]**.

**1.6.5 La méthode HIRA**

**HIRA** : En anglais c’est l’acronyme : ***Hazard Identification Risk Assessment***.

En français : identification des dangers et évaluation des risques **[13]**.

**1.6.5.1 Techniques utilisées pour faire l’analyse des risques**

Sur terrain, la commission doit observer les tâches des postes à analyser, impliquer les travailleurs par des interviews, prendre en compte les retours d’expérience au cours de la rédaction de l’analyse des risques. Après la finalisation de l’HIRA principale (Analyse des risques des postes de travail) le retour de l’information aux travailleurs des postes concernés est obligatoire moyennant les fiches des en sibilisation aux risques des postes de travail. Chaque responsable hiérarchique doit communiquer et expliquer aux personnels sous sa responsabilité les résultats de l’analyse des risques [13].

**1.6.6 L’analyse des modes de défaillance de leur effet et de leur criticité (AMDEC)**

**1.6.61. 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 tels que l’industrie chimique, pétrolière ou le nucléaire.

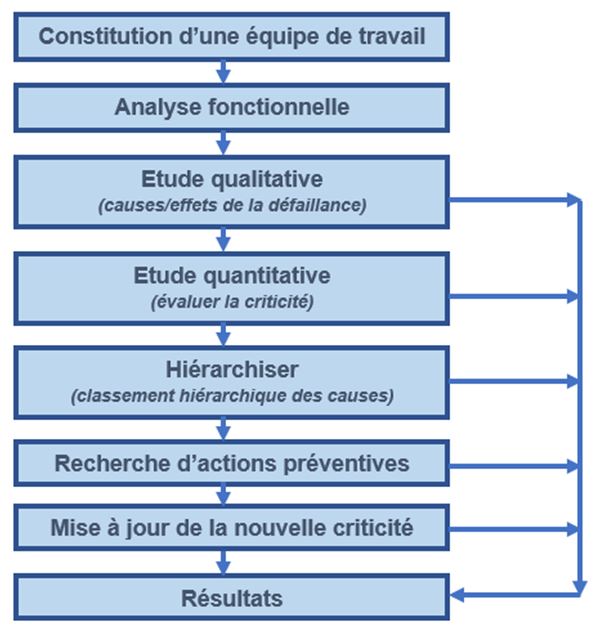
De fait, elle est essentiellement adaptée à l’étude des défaillances de matériaux et d’équipements et peut s’appliquer aussi bien à des systèmes de technologies différentes (systèmes électriques, mécaniques, hydrauliques…) qu’à des systèmes alliant plusieurs techniques **[7]**.

**1.6.6.2 Principe de L’AMDEC**

Recenser les risques potentiels d’erreur (ou les modes de défaillance) et en évaluer les effets puis en analyser les causes**.** L’AMDEC est d’identifier et de hiérarchiser les modes potentiels de défaillance susceptibles de se produire sur un équipement, d’en rechercher les effets sur les fonctions principales des équipements et d’en identifier les causes. Pour la détermination de la criticité des modes de défaillance, l’AMDEC requiert pour chaque mode de défaillance la recherche de la gravité de ses effets, la fréquence de son apparition et la probabilité de sa détectabilité. Quand toutes ces informations sont disponibles, différentes méthodes existent pour déduire une valeur de la criticité du mode de défaillance. Si la criticité est jugée non acceptable, il est alors impératif de définir des actions correctives pour pouvoir corriger la gravité nouvelle du mode de défaillance (si cela est effectivement possible), de modifier sa fréquence d’apparition et d’améliorer éventuellement sa détectabilité **[8]**.

**1.6.6.3 Les étapes de la méthode AMDEC**

La méthode s’inscrit dans une démarche en huit étapes :



**Figure 1.10** : La démarche de la méthode AMDEC.

**1.6.6.4 Les avantages et les limites**

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 majeurs constituent par exemple, en règle générale, 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 complétée, 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 **[7]**.

**1.6.7 Arbre de défaillances «AdD» (FaultTree « FT » en anglais)[13]**

**1.6.7.1 Définition**

Un arbre de défaillances (aussi appelé arbre de pannes ou arbre de fautes) est une technique d’Ingénierie très utilisée dans les études de sécurité et de fiabilité des systèmes statique **[13]**

**1.6.7.2 Formalisme**

Cette méthode consiste à représenter graphiquement les combinaisons possibles d’évènements qui permettent la réalisation d’un évènement indésirable prédéfini (appelé communément évènement redouté « ER »). La représentation graphique met donc en évidence les relations causes à effet **[13]**

**1.6.7.3 Modélisation**

Cette technique est complétée par un traitement mathématique qui permet la combinaison des défaillances simples ainsi que de leur probabilité d’apparition. Elle est basée sur l’algèbre de Boole relative à la théorie des ensembles. Elle permet ainsi de quantifier la probabilité d’occurrence d’un évènement indésirable. Egalement appelé « évènement redouté » **[13]**

**1.6.7.4 Méthodologie**

L’arbre de défaillance est formé de niveaux successifs d’évènements qui s’articulent par l’intermédiaire des portes (initialement logique). En adoptant cette représentation et la logique déductive (allant des effets vers les causes) et booléenne, il est possible de remonter d’effets en causes de l’évènement indésirable à des évènements de base indépendants entre eux et probabilistes **[13]**.

**1.6.7.5 Généralités et description de l’arbre de défaillance**

**1.6.7.5.1 Introduction**

Lorsqu’il s’agit d’étudier les défaillances d’un système, l’arbre de défaillance s’appuie sur une analyse dysfonctionnelle d’un système à réaliser préalablement : une analyse des modes de défaillances et de leurs effets (AMDE). Cette méthode inductive allant des causes aux effets apparaît donc comme préalable à la construction d’un arbre de défaillance puisque l’identification des composants et de leurs modes de défaillance est généralement utilisée au dernier niveau d’un arbre.

L’analyse par arbre de défaillance et le diagramme de fiabilité sont des méthodes pratiques à condition que les évènements de base soit faiblement dépendant. Dans le cas contraire, ces techniques deviennent caduques et il est nécessaire d’employer une technique plus appropriée reposant sur un modèle dynamique comme un processus de MARKOV **[13]**.

**1.6.7.5.2 Utilités des arbres de défaillances**

Les arbres de défaillances sont utilisés dans l’ingénierie de sûreté des industries « à risque » et peuvent être utilisés comme un outil d’évaluation de la conception, ils permettent d’identifier les scénarios conduisant à des accidents dans les phases amont du cycle de vie d’un système et peuvent éviter des changements de conception autant plus coûteux qu’ils sont tardifs. Ils peuvent aussi être utilisés comme un outil de diagnostic, prévoyant la ou les défaillances des composants la ou les plus probables lors de la défaillance d’un système **[13]**

**1.6.7.5.3 Représentation de la méthode de l’arbre de défaillances**

* La ligne la plus haute ne comporte que l’évènement dont on cherche à décrire comment il peut se produire.
* Chaque ligne détaille la ligne supérieure en présentant les combinaisons susceptibles de produire l’évènement de la ligne supérieure auquel elles sont rattachées.
* Les relations sont représentées par des liens logiques, dont la plupart sont des « portes OU » et des « portes ET » **[13]**.

**1.6.7.5.4 Méthodologie de la méthode arbre de défaillances**

***Démarche:*** L’arbre de défaillance est une méthode déductive, qui fournit une démarche systématique pour identifier les causes d’un évènement unique intitulé évènement redouté. Le point de départ de la construction de l’arbre est l’évènement redouté lui-même (également appelé évènement du sommet). Il est essentiel qu’il soit unique et bien identifier. A partir de là, le principe est de définir des niveaux successifs d’évènements tels que chacun est une conséquence d’un ou plusieurs évènements du niveau inférieur.

La démarche est la suivante :

* Pour chaque évènement d’un niveau donné, le but est d’identifier l’ensemble des évènements immédiats nécessaires et suffisants à sa réalisation. Des opérateurs logiques (portes) permettent de définir précisément les liens entre les évènements des différents niveaux.
* Le processus déductif est poursuivi niveau par niveau jusqu’à ce que les spécialistes concernés ne jugent pas nécessaire de décomposer des évènements en combinaison d’évènements de niveaux inférieurs, notamment parce qu’ils disposent d’une valeur de probabilité d’occurrence de l’évènement analysé.

Ces évènements non décomposés de l’arbre sont appelés évènements élémentaires (ou évènements de bases). Notons que :

a) Il est nécessaire que les évènements soient indépendants entre eux.

b) Leurs probabilité d’occurrence doit pouvoir être quantifiée (condition nécessaire seulement dans le cas où l’arbre est destiné à une analyse quantitative).

c) Contrairement à l’approche inductive de l’AMDEC (analyse des modes de défaillance, de leurs effets et de leur criticité) qui ne cible pas les conséquences des défaillances élémentaires, l’approche déductive de l’arbre de défaillance permet de focaliser exclusivement sur les défaillances contribuant à l’évènement redouté.

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 qui sera réalisée par la suite **[13]**.

**1*.*6.7.5.5 Analyse qualitative :**

L’arbre de défaillance étant construit, deux types d’exploitation qualitative peuvent être réalisés :

1. L’identification des scénarios critiques susceptibles de conduire à l’évènement redouté. Par l’analyse des différentes combinaisons de défaillances menant à l’évènement sommet, l’objectif est ici d’identifier les combinaisons les plus courtes appelées coupes minimales.

2. La mise en œuvre d’une procédure d’allocation de barrières. Ce deuxième type d’exploitation qualitatif permet d’allouer un certain nombre de barrières de sécurité (technique ou d’utilisation) en fonction de la gravité de l’évènement redouté et des contraintes normatives éventuelles **[13]**

**1.6.7.5.6 Analyse quantitative**

Une étude probabiliste peut avoir deux objectifs :

1. L’évaluation rigoureuse de la probabilité d’occurrence de l’évènement redouté.

2. Le tri de scénarios critiques (en partant des coupes minimales de plus fortes probabilités).

Ces calculs ne peuvent se concevoir que si chaque évènement élémentaire peut être probabilisé à partir d’une loi soigneusement paramétrée et de la connaissance du temps de mission associé à l’évènement redouté et/ou à l’aide de données issues du retour d’expérience.

**1.6.7.5.7 Identification de l’évènement :**

L’identification de l’évènement redouté est absolument essentielle à l’efficacité et à la pertinence de la méthode. Il correspond le plus souvent à un évènement catastrophique en termes humain, environnemental ou économique. Il peut s’avérer nécessaire parfois de caractériser l’évènement redouté pour chacune des missions du système étudié. Il existe plusieurs méthodes permettant de procéder à l’identification des évènements redoutés. L’analyse préliminaire des risques (APR), est utilisée dans la plupart des industries.

**1.6.7.5.8 Examen du système**

Lors d’une analyse fiabiliste d’un système, il est toujours difficile de délimiter précisément les contours de l’étude. L’analyste doit pour cela se poser certain nombre de questions incontournable du type :

1. Quelles sont les intentions de l’analyse ?

2. Quelles sont les limites ?

3. S’agit-il de maîtriser une prise de risque relative à la sécurité des personnes ou de comparer différents dispositifs ?

4. L’objectif est-il de démonter la conformité à des normes officielles et/ou à des spécifications imposées par le client ?

Avant d’entamer la construction de l’arbre de défaillance proprement dite, les analystes chargés de l’étude doivent acquérir au préalable une très bonne connaissance de l’ensemble du système et de sa fonction. Ils doivent s’appuyer pour cela sur l’expérience des ingénieurs et techniciens chargés des opérations sur le terrain.

Il est également nécessaire de délimiter précisément l’étude à différents niveaux :

5. Natures des évènements pris en compte ;

6. équipements impliqués ou non dans la fonction du système ;

7. Importance de l’environnement, etc.

Afin d’être complet et rigoureux, l’examen du système doit couvrir obligatoirement chacun des thèmes suivants :

1. La description du système (éléments et sous-systèmes inclus dans l’étude et éléments exclus).

2. La définition de la mission (spécification du système, phase de diverses missions, procédure de maintenance et de réparation, reconfiguration possible…)

3. L’analyse de l’environnement ;

4. L’identification des évènements à prendre en compte: étendue donnée à l’étude (prise en compte des résultats des erreurs humaines, des problèmes de transport de pièces/ personnel,..).

**1.6.7.5.9 Construction de L’arbre**

Cette construction est détaillée dans plusieurs normes industrielles dont la norme **CEI 61025 [13]**.

**1. Evènement sommet (évènement indésirable) :**

La première étape réside dans la définition de l’évènement à étudier d’une façon explicite et précise, cet évènement est appelé sommet, ou encore évènement redouté. Cette étape est cruciale quant à la valeur des conclusions qui seront tirées de l’analyse. L’arbre de défaillance se veut être une représentation synthétique ; le libellé de l’évènement devra être bref, mais aussi évocateur que possible dans la boite qui le représente dans l’arbre, on lui associant un texte complémentaire apportant toutes les précisions utiles sur la définition de l’évènement. Cette remarque est aussi valable pour tous les éléments qui vont figurer dans l’arbre [10].

**2. Evènement intermédiaires**

L’évènement sommet étant défini, il convient de décrire la combinaison d’évènements pouvant conduire à cet évènement sommet. Les évènements intermédiaires sont des évènements moins globaux. Une fois un évènement définis, ils seront liés à l’évènement sommet via un connecteur. Ces évènements intermédiaires peuvent être, à leur tour, redéfinis par d’autres évènements intermédiaires plus détaillés **[13]**.

**3. Evènements de base, transfert et conditions**

Il est possible de prendre en compte des évènements sur lesquels les informations sont insuffisantes pour les décomposer davantage ou encore qu’il n’est pas utile de développer plus, ces évènements sont appelés évènements non développés. Lors de la construction de gros arbres de défaillances, il est pratique d’utiliser des portes de transfert, permettant ainsi de rendre la lecture et la validation de l’arbre plus aisée. Ces portes signalent que la suite de l’arbre est développée sur une autre page. Les évènements de bases sont les évènements les plus fins de l’arbre, il ne sera pas possible de les détailler davantage ; ils concernent la défaillance (électrique, mécanique, logiciel…) d’un élément du système.

L’apparition de certains évènements (de base ou autres) peut avoir une conséquence à certaines conditions. Nous sommes donc conduits à introduire dans l’arbre des conditions dont la réalisation conditionne l’enchainement. Ces conditions interviennent dans la construction de l’arbre comme des évènements intermédiaires, à l’exception que ces conditions ne sont plus décomposées donc « de base » **[13]**.

**4. Connecteurs logiques**

Les connecteurs (portes) logiques sont les liaisons entre les différents branches et/ou évènements. Les plus classiques sont **ET** et **OU.** Les connecteurs fonctionnent comme suit :

* **OU** : l’évènement en sortie/supérieur survient si, au moins, un des évènements en entrée/inférieur survient/est présent ;
* **ET** : l’évènement en sortie/supérieur survient seulement si tous les évènements en entrée/inférieur surviennent/sont présents ;
* K/N : c’est un vote majoritaire : l’évènement en sortie/supérieur survient si au moins **K** (c’est un entier qui sert à paramétrer le comportement de la porte) parmi les **N** évènements en entrée/inférieur surviennent/sont présents. Cette porte généralise les deux précédentes : une porte OU est une porte 1/N et une porte ET est une porte N/N.

L’utilisation exclusive des trois connecteurs mentionnés ci-dessus permet de rester dans le cadre des arbres de défaillances cohérents, et c’est en pratique ce qui est fait le plus souvent. Dans certaines situations, il est nécessaire d’introduire des non cohérences avec des connecteurs **NON, OU exclusif** (réalisé si une et une seule de ses entrées est réalisée) ...etc. mais cela rend le traitement mathématique plus complexe. Enfin, il peut être pratique à des fins descriptives d’utiliser des connecteurs plus complexes, comme des connecteurs de vote conditionnels… Ces connecteurs permettent de traduire des comportements particuliers qu’il est possible de rencontrer dans certaines architectures. Au même titre, une dimension temporelle peut être nécessaire pour traduire le comportement d’un système, pour cela il existe des connecteurs **ET** séquentiels prenant en compte le séquencèrent des évènements, des connecteurs **SPARE** prenant en compte des lots de rechanges, etc. l’utilisation de ces connecteurs peut conduire à des modèles dont la signification mathématique est ambigue et sont interprétée différemment suivant les outils informatiques dans lesquels ils sont saisis **[13]**.

**1.6.7.5.10 Symbole graphique**

Les symboles de base utilisés dans les arbres de défaillance sont classés en plusieurs types :

* Evènements ;
* Portes ;
* Symboles de transfert.

(Dans les logiciels permettant d’éditer des arbres de défaillances on pourra constater des variations mineures). Les différents symboles utilisés sont regroupés dans les tableaux 1 et 2.

**Tableau 1.1 :** Symboles des évènements dans les arbres de défaillances **[13]**

|  |  |  |
| --- | --- | --- |
| **Symbole** | **Nom** | **Description** |
| C:\Users\Server01\Desktop\symboles\1.PNG | Evènement de base | Evènement du plus bas niveau pour lequel la  probabilité d’apparition ou d’information de fiabilité est disponible |
| C:\Users\Server01\Desktop\symboles\2.PNG | Evènement  Maison | Evènement qui doit se produire avec certitude lors de la production ou de la maintenance. On peut aussi le définir comme un évènement non- probalisé, que l’on doit choisir de mettre 1 ou 0 avant tout traitement de l’arbre. Ce type d’évènement permet d’avoir plusieurs variantes d’un arbre sur un seul dessin, en modifiant la logique de l’arbre selon la valeur choisie par l’utilisateur |
| C:\Users\Server01\Desktop\symboles\3.PNG | Evènement  non développé | Le développement de cet évènement n’est pas terminé, soit parce que ses conséquences sont négligeables, soit par manque d’information. |

**Tableau 1.2 :** Symboles des portes dans les arbres de défaillances [13]

|  |  |  |  |
| --- | --- | --- | --- |
| **Symbole** | **Nom** | **Description** | **Nombre**  **d’entrées** |
| C:\Users\Server01\Desktop\symboles\4.PNG | OU (OR) | L’évènement de sortie apparait si au moins un des évènements d’entrées apparait | ˃1 |
| C:\Users\Server01\Desktop\symboles\5.PNG | ET (AND) | L’évènement de sortie apparait si tous les évènements apparaissent | ˃1 |
| C:\Users\Server01\Desktop\symboles\6.PNG | NON (NOT) | L’évènement de sortie apparait si l’évènement d’entrée n’apparait pas.  L’état logique de la sortie est l’inverse de celui d’entrée. | =1 |
| C:\Users\Server01\Desktop\symboles\7.PNG | OU Exclusif  (XOR) | L’évènement de sortie apparait si un seul évènement d’entrée apparait. | ˃1 |
| C:\Users\Server01\Desktop\symboles\8.PNG | Vote  Majoritaire | L’évènement de sortie apparait si au moins K évènements d’entrées apparaissent (K˂n) | ˃1 |

Les principaux traitements que l’on peut faire à partir de la fonction booléenne sont les suivants :

* L’énumération des coupes minimales
* Le calcul des facteurs d’importance structurelle. Très peu utilisés en pratique, ils visent à donner des indications du même ordre que les facteurs d’importance calculés avec des probabilités, lorsque celles-ci ne sont pas disponibles.

Une grande variété d’algorithmes permettant de faire ces traitements.

**1.6.7.5.11 Résumé des règles importantes de la construction de l’arbre de défaillance :**

1. Partir de l’évènement redouté (sommet de l’arbre),

2. Imaginer les évènements intermédiaires possibles expliquant l’évènement sommet,

3. Considérer chaque évènement intermédiaire comme un nouvel évènement sommet,

4. Imaginer les causes possibles de chaque évènement au niveau considéré,

5. Descendre progressivement dans l’arbre jusqu’aux évènements de base **[13]**

**Il est important de ne pas considérer immédiatement les évènements de bases (panne d’un composant par exemple).**

**1.6.7.5.12 La cohérence d’un arbre de défaillances**

Une propriété très importante du point de vue pratique est ce qui est appelé la cohérence d’un arbre de défaillances.

**1.6.7.5.12.1 Définition**

Un arbre de défaillances est cohérent si :

* Il n’existe aucun état du système, tel qu’à partir de cet état la défaillance d'un composant (formellement, cela correspond au passage de la valeur zéro à la valeur un pour la variable Xi correspondante) peut réparer le système (formellement, cela correspond au passage de la valeur un à la valeur zéro pour la fonction F),
* La fonction F dépend effectivement de toutes les variables X..

Une façon très simple d’assurer par construction la cohérence d’un arbre de défaillance est de **le construire uniquement avec des portes ET, OU, K/N.** C’est ce qui est fait dans la grande majorité des applications pratiques des arbres de défaillances.

Lorsqu’un arbre de défaillances est cohérent, sa fonction F admet une représentation canonique qui s’écrit comme la disjonction logique de ses coupes minimales **[13]**.

**1.6.7.5.13 Coupe minimale**

Une coupe d’un arbre de défaillances cohérent est un ensemble de défaillances de composants tel que lorsque ces défaillances sont simultanément présentes, l’événement sommet de l’arbre est réalisé. Plus généralement, la notion de coupe est définie pour l'ensemble des systèmes statiques **[13]**.

**1.6.7.5.13.1 Définition**

Une « coupe minimale » d’un arbre de défaillances cohérent est une coupe comportant un nombre minimal d'événements défaillants. Autrement dit, dès qu’on enlève une défaillance de la coupe, n’importe laquelle, l’ensemble des défaillances restantes ne suffit plus à provoquer l’événement sommet. Une seconde propriété des coupes minimales est qu'elles ne peuvent contenir aucune autre coupe. La cohérence du système considéré permet alors de garantir que tout ensemble d'événements de base contenant cette coupe minimale est également une coupe.

L'ensemble des coupes minimales est suffisant pour représenter la défaillance du système, le calcul de cet ensemble peut être réalisé par minimisation de la fonction F.

La notion de coupe minimale admet une généralisation appelée **''impliquant premier''** pour les arbres non cohérents. Cette notion étant peu utilisée en pratique, elle n’est pas décrite dans ce chapitre **[13]**.

**1.6.7.5.13.2:Cardinal ou ordre des coupes minimales**

Il est particulièrement intéressant de considérer le cardinal (on dit aussi : ordre) des coupes minimales, autrement dit le nombre minimal d’événements élémentaires nécessaires à produire l’événement sommet de l’arbre.

En particulier pour les systèmes critiques, des règles du type **« il faut la combinaison d’au moins trois événements indépendants pour créer la situation dangereuse »** sont autant, voire plus opérationnelles que des exigences exprimées en probabilités.

Les coupes minimales ayant le plus petit cardinal définissent le nombre minimum d’événements dont l’occurrence simultanée peut provoquer l’événement sommet ; dans un contexte de **« défense en profondeur »,** c’est **le nombre de barrières.**

Les coupes minimales d’ordre un représentent tous les événements de base qui à eux seuls produisent l’événement indésirable **[13]**

**1.6.7.5.14 Quantification avec des probabilités fixes**

Ce qui fait la puissance des arbres de défaillances, et, plus généralement des « méthodes booléennes » en sûreté de fonctionnement est l'hypothèse d'indépendance globale des évènements. Les principaux traitements que l'on peut faire à partir d’un arbre de défaillances muni de probabilités sont les suivants :

* L'énumération des coupes minimales ou impliquant premiers associés à leurs probabilités. La possibilité de les quantifier permet de ne lister que ceux dont la probabilité dépasse un certain seuil, ce qui est une façon efficace de limiter l’explosion combinatoire à laquelle peut conduire ce type de traitement ;
* Le calcul de la probabilité de l'événement redouté F=1(qui s'identifie avec l'espérance mathématique de F).
* Le calcul de divers facteurs d'importance associés aux événements de base.

**1.6.7.5.15 Quantification avec des probabilités fonction du temps[13]**

En donnant à la valeur 1 de la variable la signification “le ième composant est défaillant à l’instant t”, on peut réaliser une série de calculs de la probabilité de l’événement de tête de l’arbre à des instants différents. C’est ainsi que l’on peut calculer l’indisponibilité d’un système en fonction du temps. Par exemple, dans le cas très courant où la durée de vie (aléatoire) d’un composant (le temps avant défaillance) est modélisée par une loi exponentielle de paramètre ʎ , la probabilité que ce composant soit défaillant avant le temps de mission du système (temps pendant lequel l’occurrence de la défaillance peut se produire) est donnée par :

**P= ʎ - e-ʎ t**

**P= ʎ t, (ʎ t)˂ = 0.1 (1)**

Cette formule suppose le composant non réparable. Si au contraire il est réparable, et si on suppose que sa durée de réparation suit une loi exponentielle de paramètre, alors sa probabilité d’être défaillant à l’instant t (son indisponibilité) est donnée par la formule :

**[(ʎ i)/(ʎ i + μi)][1- e- (ʎ i + μi) t]**  **(2)**

En supposant que tous les composants du système sont ainsi modélisés, on voit qu’il est facile de calculer la probabilité de défaillance du système complet à l’instant t. Le calcul des probabilités de tous les événements de base à l’instant t à l’aide des formules (1) ou (2) décrites ci-dessus,

Plus généralement, il existe tout un ensemble de formules analytiques permettant de calculer les probabilités de défaillance des composants en fonction du temps. Ces formules permettent de prendre en compte des hypothèses telles que la possibilité de réparer le composant, de le tester périodiquement, et aussi différents types de lois de probabilité pour les durées de vie des composants. Par exemple, on utilise généralement des lois de Weibull pour modéliser les durées de vie de composants soumis à un phénomène de vieillissement. Il est important de noter que la technique décrite ci-dessus permet de faire seulement des calculs de disponibilité et pas de fiabilité du système. Toutefois, il se trouve que ces deux notions se confondent pour un système cohérent dont aucun composant n’est réparable.

Dans ce cas, que ce soit au niveau d’un composant ou au niveau du système tout entier, toute panne est définitive, et la probabilité d’être en panne à l’instant t (indisponibilité) est égale à la probabilité d’être tombé en panne avant ***t*** (défiabilité). Lorsqu’on a affaire à un système comportant des composants réparables, un calcul de fiabilité reste possible, mais au prix d’une approximation. Le principe de ce calcul consiste à estimer le taux de défaillance du système à différents instants compris entre 0 et t, puis à calculer la fiabilité R(t) à l’instant t par la formule d’intégration du taux de défaillance ci-dessous :

**R(t) = e -ʃ0t ʎ (u) (3)**

L’approximation faite est double : d’une part, dans l’estimation du taux de défaillance, pour lequel il n’existe pas de formule exacte, et d’autre part dans l’intégration numérique de ce taux sur l’intervalle [0, t].

**1.6.7.5.16 Sensibilité, Facteurs d’importance**

Les composants constitutifs d'un système peuvent avoir une importance plus ou moins grande pour ce système. Un composant correspondant à un point unique de défaillance sera bien entendu plus important qu'un composant de caractéristiques équivalentes mais mis en parallèle avec d’autres composants. Sur un système de très petite taille, l’identification de ces composants importants peut se faire par une simple lecture des coupes. Mais pour un système complexe et sûr dont les coupes sont d'ordre élevé, cette lecture est impossible. C'est pourquoi des facteurs d'importance ont été introduits afin d'établir une hiérarchie des composants. L'importance d'un composant pouvant varier suivant les objectifs recherchés, plusieurs facteurs d'importance ont été créés. Voici cinq facteurs d’importance parmi les plus utilisés :

*a. Birnbaum (aussi appelé facteur d’importance marginal)*

*b. Critique*

*c. Diagnostic*

*d. Facteur d’augmentation de risque*

*e. Facteur de diminution de risque*

Attention, ces différents facteurs d'importance ne vont pas toujours dans le même “sens”, il peut être difficile d'identifier formellement les composants à améliorer (en les rendant plus fiables, mieux maintenus…). C'est pourquoi il est conseillé de ne pas se fier à un seul facteur d'importance. En conclusion nous pouvons citer les avantages et limites de la Méthode ‘’Arbre de Défaillances’’ comme suit :

**1.6.7.5.17 Avantages[10]**

L'analyse par arbre de défaillances est la plus couramment utilisée dans le cadre d'études de fiabilité, de disponibilité ou de sécurité des systèmes. Elle présente en effet un certain nombre d'avantages non négligeables par rapport aux autres méthodes, à savoir :

1. Son aspect graphique tout d'abord, caractéristique particulièrement importante, constitue un moyen efficace de représentation de la logique de combinaison des défaillances. Il participe largement à la facilité de mise en œuvre de la méthode et à la compréhension du modèle. Ainsi, il est un excellent support de dialogue pour des équipes pluridisciplinaires.

2. Le principe de l'arbre est basé sur une méthode déductive permet à l'analyste de se focaliser uniquement sur les événements contribuant à l'apparition de l'événement redouté.

3. Une fois la construction de l'arbre terminée, deux modes d'exploitation sont possibles :

* l'exploitation qualitative servant à l'identification des combinaisons d'événements critiques, la finalité étant de déterminer les points faibles du système;
* l'exploitation quantitative permettant de hiérarchiser ces combinaisons d'événements suivant leur probabilité d'apparition, et estimer la probabilité de l'événement sommet, l'objectif in fine étant de disposer de critères pour déterminer les priorités pour la prévention de l'événement redouté.

4. Par opposition aux méthodes de simulation, l'approche analytique offerte par l'arbre de défaillances a l'avantage de pouvoir réaliser des calculs rapides (avantage tout à fait relatif au vu de l'évolution permanente de l'informatique) et exacts.

5. La méthode permet d'estimer la probabilité non seulement de l'événement redouté, mais aussi celle des portes intermédiaires, à partir de celle des événements de base. Il est également possible de faire de la propagation d'incertitudes sur les données d'entrée, et du calcul de facteurs d'importance.

6. La taille de l'arbre de défaillances est proportionnée à la taille du système étudié, et pas exponentielle en fonction de cette taille.

**1.6.7.5.18 Limites[10]**

L'utilisation de l’arbre de défaillances devient inefficace ou difficilement applicable lorsque les caractéristiques suivantes apparaissent :

**1. Dépendance entre les événements**

Les calculs de probabilité d’occurrence effectués par le biais de l’arbre de défaillances sont basés sur une hypothèse d’indépendance des événements de base entre eux. Par exemple, la probabilité d’apparition d’un événement de base ne peut pas dépendre de l’apparition d’autres événements de base.

**2. Notion d’événements temporisés**

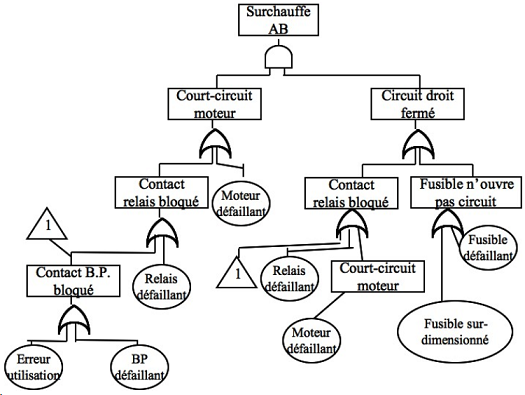
L'arbre de défaillances ne rend pas compte de l'aspect temporel des événements. Il ne peut donc considérer ni les dépendances fonctionnelles, ni les états passés. De plus, il ne permet pas de prendre en compte un ordre imposé dans lequel des événements doivent se produire pour induire une défaillance.

**3. Système dégradé**

L’arbre de défaillances est binaire. Un événement se produit ou ne se produit pas, mais aucune notion de capacité ou d’efficacité ne peut intervenir. Par exemple, une vanne sera considérée comme ouverte ou fermée, mais sans pouvoir déterminer d’état intermédiaire.

**4. Taille de l’arbre**

La taille n’est pas une limite en soi. Néanmoins dès qu'elle augmente de manière significative, l’arbre doit être divisé en sous-arbres, et la lisibilité ainsi que la compréhension du modèle deviennent alors plus difficiles.



**Figure 1.11 :** Exemple de la méthode Arbre de défaillances **[10]**

**1.7. Conclusion**

Dans ce chapitre, plusieurs modèles de classification ont été proposés. Ils ne sont pas exhaustifs, ces classifications intègrent plusieurs types de risques qui n'ont pas été tous détaillés et hiérarchisés (Risque Planning, Risque technologique, Risque humain, Risque accidentel, Risque conjoncturel ....). Il est important de développer l'analyse de risque en se posant les questions suivantes : Pour qui ? Sur quoi ? Quand ?

Le concept d'analyse de risque pour un projet repose sur la démarche en 5 étapes, il s'agit d'un modèle de référence structurant les points suivants :

* Identification et classification des risques.
* Les conséquences du risque (financier, juridique, humain, ...).
* La gestion du risque (prévention, protection, évitement de risque, transfert).
* Maîtrise interne ou transfert vers un tiers (externalisation, assurance).
* Assurabilité d'un risque, calcul financier du transfert à l'assurance.

L'importance de obligations réglementaires, régulièrement modifiées nécessite une veille attentive pour partager la connaissance, capitaliser l'information, fédérer tous les acteurs de la sécurité, et faciliter les mises à jour. Toutefois, légitimement, on peut s'interroger sur l'établissement de classification des risques et des effets sur l'assurance.

Nous avons vu dans ce chapitre les méthodes de management des risques, celles-ci permettent une identification systématique des composantes du risque Les différentes situations dangereuses, évènements redoutés, causes, conséquences, ou accidents potentiels, tous ces éléments sont identifiés d’une manière méthodologique et présentés dans une forme tabulaire à l’image de l’APR et l’AMDEC et HIRA, ou arborescente à l’image de l’Arbre de Défaillances ou d’Evénements.