Chapitre 3 – Formalismes de certaines méthodes quantitatives d'analyse des risques

Les méthodes des arbres permettent de représenter le fonctionnement et l'évolution d'un système en forme d'arbre.

Il existe plusieurs méthodes, nous allons étudier dans un premier temps l'arbre des causes, des défaillances puis nous finirons par l'étude de l'arbre des événements.

3.1 / Méthode Arbre des Causes (AdC)

Analyse à posteriori d'un accident: arbre des causes.

Objectif : Réaliser un arbre des causes et proposer des mesures de prévention.

L'arbre des causes est la représentation graphique de l'enchaînement logique des faits qui ont provoqué un accident.

L'arbre des causes est une méthode d'analyse permettant de :

• reconstituer d'une façon logique et chronologique l'accident en cherchant les causes.

• mettre en œuvre une prévention afin d'éviter la survenue d'un accident identique.

3.1.1 / Recueil des faits.

C'est la première étape de cette méthode d'analyse.

• Se rendre sur le lieu de l'accident le plus tôt. Relever tous les faits dans le désordre, sans les relier. Le faire de préférence en équipe.

• Identifier le fait ultime (le dommage en général).

Exemple	Fait	Opinion
Utilise une perceuse	**x**	
Geste dangereux	**x**	**x**
Travail les mains nues		
Chute de l'échafaudage	**x**	

Un fait est concis, précis, vu, lu ou entendu et est non contestable.

Ne pas confondre : fait, interprétation, jugement et opinion.

3.1.2/ Construction de l'arbre des causes

Il se construit de la droite vers la gauche **en partant du fait ultime** et en se posant pour chaque fait, ces questions : **Qu'a-t-il fallu pour que ce fait apparaisse ? Est-ce nécessaire? Est-ce suffisant? A-t-il fallu autre chose?**

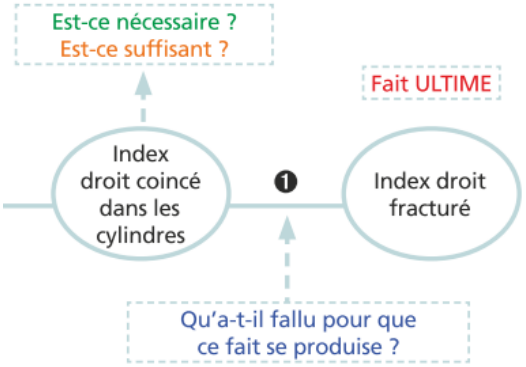


Figure 3 : construction de l'Arbre des Causes (Source Delagrave PSE)

Les faits peuvent être reliés par trois types de liaisons :

a/ Enchainement :
Un **fait** est lié à un **antécédent** Couteau dérape → Se coupe

b/ Conjonction :
Un **fait** lié à plusieurs ***antécédents*** *Escalier raide}* → Chute
Pas de lumière}

c/ Disjonction :
Plusieurs **faits** liés à un **antécédent** Pas de courant ← {Pas de lumière
{Pas de chauffage

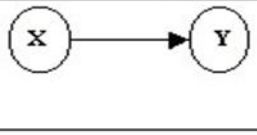
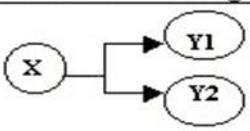
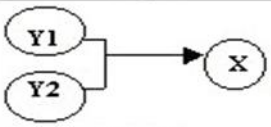
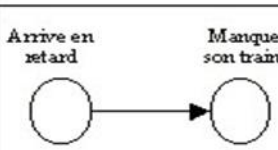
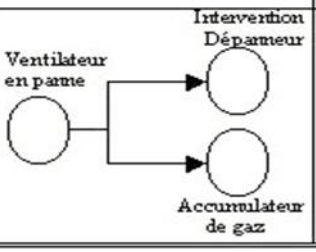
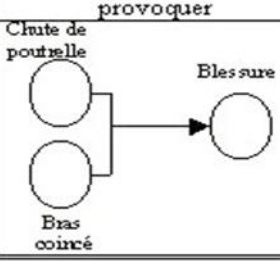
	Enchaînement	Disjonction	Conjonction
Définition	Un antécédent **Y** a une seule origine **X**	Deux (ou plus) antécédents **Y1, Y2** ont une seule et même origine	Un antécédent **X** a plusieurs origines directes **Y1, Y2**
Représentation			
Propriété	**X** est nécessaire et suffisant pour que **Y** se produise	**X** est nécessaire et suffisant pour que **Y1** et **Y2** se produisent	Chaque **Y1, Y2** est nécessaire pour que **X** se produise, mais aucun d'eux ne peut à lui seul le provoquer
Exemple			

Tableau 1 : Construction AdC

Exemple : Amar, 22 ans travaille dans un environnement bruyant 90 dB. Un incendie se déclenche et il n'entend pas l'alarme. Il est **intoxiqué**.
La présence d'essence et de flammes sont à l'origine de cet incendie.
Faits: 1 Bruit **/ 2** n'entend pas l'alarme **/ 3** incendie **/ 4** Intoxiqué (fait ultime)
/ 5 présence d'essence **/ 6** flammes

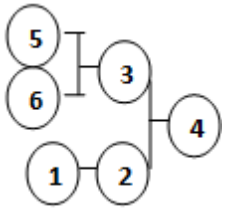


Figure 4 : Type de construction d'un AdC

3.1.3/ Proposer des mesures de prévention

La démarche de prévention des risques professionnels est sous la responsabilité de l'employeur qui met en œuvre les **9 principes généraux de prévention** (Art **L.4121-1** Code du travail).

1/ éviter ou éliminer les risques.

2/ évaluer les risques qui ne peuvent être évités.

3/ combattre les risques à la source.

4/ adapter le travail à l'homme.

5/ tenir compte de l'état d'évaluation de la technique.

6/ remplacer ce qui est dangereux par ce qui ne l'est pas ou ce qui l'est moins.

7/ planifier la prévention en y intégrant, dans un ensemble cohérent :

La technique, l'organisation du travail, les conditions de travail, les relations Sociales et influences des facteurs humains.

8/ prendre des mesures de protection collective en leur donnant la priorité sur les mesures de protection individuelle.

9/ donner les instructions appropriées aux travailleurs.

3.1.4/ Les facteurs potentiels d'accident

Un facteur potentiel d'accident (**FPA**) est une famille de risques à laquelle peut être rattaché un facteur particulier d'un accident qui s'est déjà produit.

La notion de **FPA** permet d'utiliser dans des analyses a priori des informations issues des analyses a posteriori.

En effet, ces dernières apportant des connaissances sur les risques, elles ont, dans ce sens, un caractère prospectif.

3.2/ Méthode Arbre des Défaillances (AdD)

L'arbre des défaillances est la seule méthode qui utilise une démarche déductive, c'est-à-dire partir des effets vers les causes.

L'objectif de l'arbre de défaillance est de déterminer les enchainements ou combinaisons possibles d'événement unique et redouté.

Le but de cette analyse est d'accéder aux multiples causes d'un événement final unique.

L'arbre des défaillances est composé de plusieurs niveaux d'événements, le niveau inférieur d'un événement génère un nouvel événement. Un événement est une défaillance liée aux erreurs humaine, défaut technique…

Un arbre des défaillances est constitué d'un événement sommet, d'un événement base, des événements intermédiaires, des événements conditionnels.

Chaque événement est représenté par un symbole. Les événements sont reliés par des portes logiques (ET/OU).

Des principes d'élaborations ont été mis en place :

- recherche des causes immédiates, nécessaires et suffisantes
- classement des événements intermédiaires
- recherche des causes immédiates, nécessaires et suffisantes des événements intermédiaires jusqu'à obtention des événements de base
- itération : revenir sur les caractéristiques de l'arbre en cours de construction

Pour construire l'arbre des défaillances, trois étapes doivent être respectées :

- définition de l'événement final indésirable
- analyse du système concerné
- construction effective de l'arbre des défaillances

Après la construction de l'arbre, l'exploitation des résultats peut être faite de plusieurs façons, soit au niveau système, soit qualitativement soit semi qualitativement.

Le principal avantage de l'analyse par arbre des défaillances c'est qu'elle permet de considérer des combinaisons d'évènements pouvant conduire à un événement redouté.

Elle permet de hiérarchiser les scenarii en fonction de leur priorité et de leur probabilité de survenir.

Il est conseillé de mettre en œuvre au préalable des méthodes inductives d'analyse des risques, par d'autres méthodes pour identifier les évènements les plus graves qui pourront faire l'objet d'une analyse par arbre des défaillances et pour faciliter la détermination des causes immédiates, nécessaires et suffisantes au niveau de l'élaboration de l'arbre.

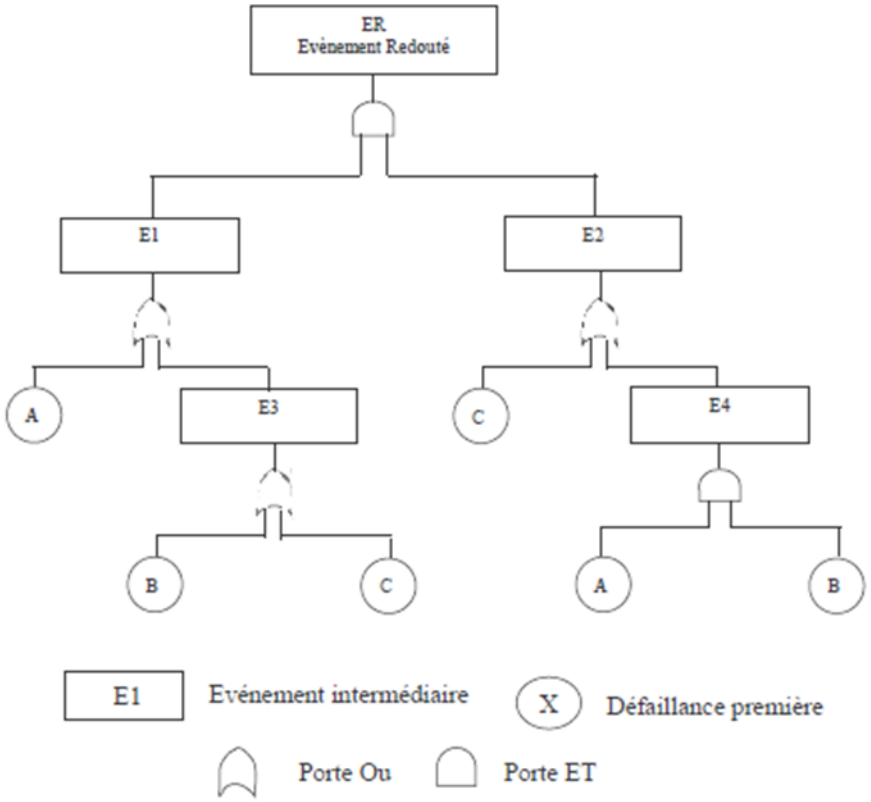


Figure 5 : Exemple d'arbre de défaillance.

3.3/ Arbre des évènements

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 à priori.

À l'inverse, l'analyse par arbre d'évènements a pour objet d'analyser l'évolution d'un système à partir d'un événement initiateur pouvoir décrire les conséquences.

Les arbres d'événements sont utilisés pour identifier les divers accidents qui peuvent se produire dans un système complexe.

À la suite de l'identification des séquences d'accidents individuels, les combinaisons spécifiques de défaillance qui peuvent conduire à des accidents peuvent être déterminées à l'aide de l'arbre d'événements.

Le principe de la méthode de l'arbre consiste :

- définir un événement initiateur comme une défaillance d'un élément, d'un composant… ou comme une perturbation de l'environnement
- identifier les fonctions de sécurité prévues pour y faire face
- construire l'arbre
- décrire et exploiter les séquences d'évènements identifiées

L'arbre d'événements permet :

- de rechercher toutes les causes et les combinaisons de causes conduisant à l'événement de tête
- de déterminer si chacune des caractéristiques de fiabilité du système est conforme à l'objectif prescrit.
- de vérifier les hypothèses faites au cours d'autres analyses à propos de l'indépendance des systèmes et de la non-prise en compte de certaines défaillances.
- d'identifier le(les) facteur(s) qui a(ont) les conséquences les plus néfastes sur une caractéristique de fiabilité ainsi que les modifications nécessaires pour améliorer cette caractéristique.
- d'identifier les événements communs ou les défaillances de cause commune.

L'exploitation des résultats se fait de deux façons soit quantitativement soit qualitativement.

L'analyse par arbre des 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. Cette méthode peut s'avérer rapidement lourde à mettre en œuvre.

Intérêts

- méthode qui permet d'envisager de manière systématique tous les déroulements possibles d'un évènement indésirable
- Le positionnement de barrières de sécurité (de défense) permet de :
- Diminuer la probabilité d'occurrence de l'événement redouté .
- Limiter ses effets .

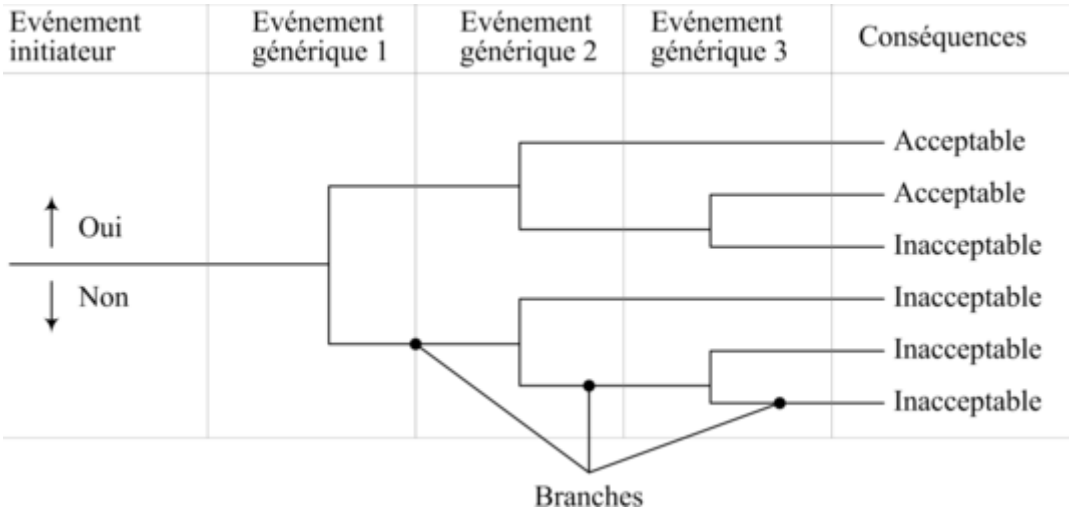


Figure 6 : Exemple d'arbre des évènements.

3.4 / Méthode Nœud de Papillon (NdP)

La représentation nœud papillon existe depuis plusieurs années, mais a suscité un grand intérêt dans les dernières années.
Elle est utilisée dans de nombreux secteurs industriels et a été développée par la compagnie Shell. L'approche est de type dite arborescente ce qui permet de visualiser en un coup d'œil les causes possibles d'un accident, ses conséquences et les barrières de sécurité mises en place. L'événement non désiré (au centre) peut être le résultat de plusieurs causes possibles (identifiées par une analyse de panne ou de défaillance).
À son tour, si celui-ci se matérialise, divers phénomènes dangereux peuvent engendrer des effets sur des éléments sensibles du milieu dans lequel on se trouve (identifiées par une analyse d'événements ou de conséquences) (figure 4).

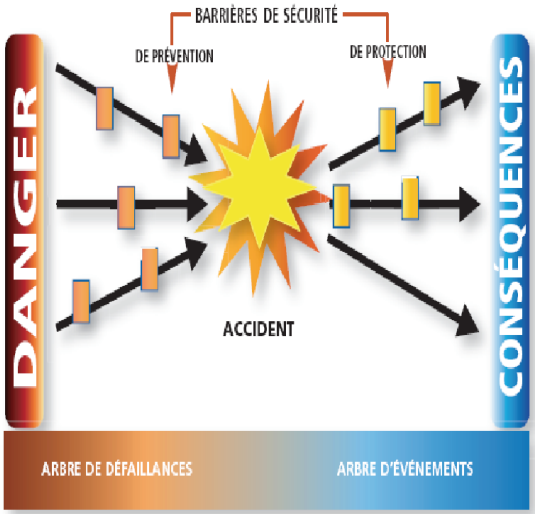


Figure 7 : Représentation générique d'un scénario d'accident par l'approche nœud papillon

3.4.1/ Objectif de l'approche nœud papillon

Cet outil permet d'illustrer le résultat d'une analyse de risque simple ou détaillée (de type APR, AMDEC, HAZOP, What-if ou autres) et d'y superposer les barrières de sécurité (prévention et protection).

Ainsi, c'est un outil grandement efficace pour communiquer les résultats d'une analyse des risques à diverses parties prenantes incluant le grand public et la haute direction des organisations; deux groupes d'intervenants avec lesquels il est crucial de synthétiser et de vulgariser l'information à communiquer.

3.4.2/ Principes de l'approche nœud papillon

Si on se place au centre du schéma (figures 5 et 6), la partie gauche du nœud représente l'identification des dangers, des causes possibles d'accident et des divers enchaînements ou combinaisons (flèches noires) d'événements pouvant engendrer l'accident non désiré (au centre).

Par exemple, l'événement central peut être une 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.

Entre ces causes possibles et l'accident, des barrières dites de prévention (rectangles) doivent être installées.

La partie droite du nœud représente les conséquences possibles de l'accident si l'événement central survient.

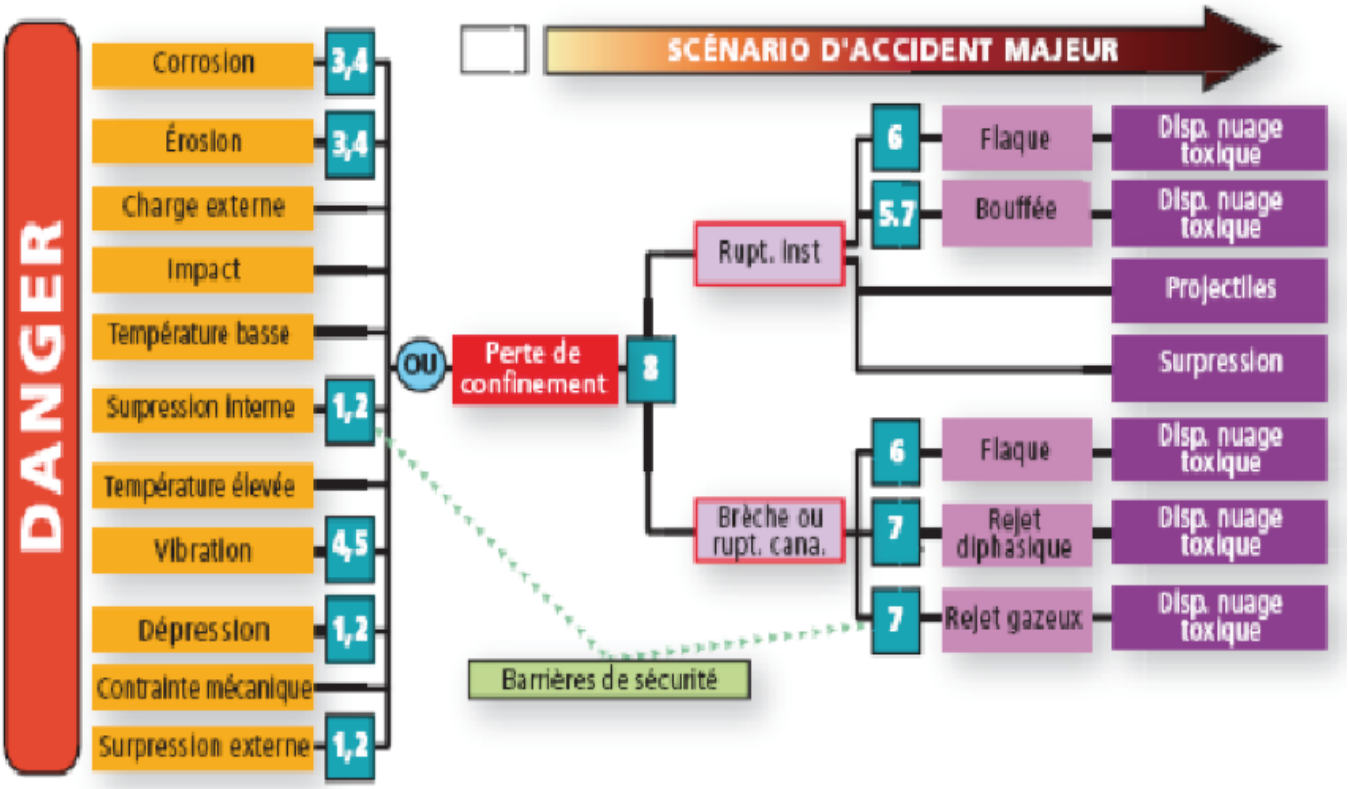
Par exemple, lors de la rupture d'une canalisation ou d'une brèche dans un réservoir, il peut en résulter la formation d'une flaque ou d'un nuage.

Entre cet accident et les récepteurs pouvant être affectés (ex. : employé, public, infrastructure, environnement, etc.), des barrières de protection doivent être installées pour réduire les effets sur ces récepteurs (ex. : un système de gicleurs).

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.

Il est question 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.



Événements initiateurs, causes possibles	Barrières de sécurité de prévention	
Surpression interne	Soupape de sécurité, disque de rupture (1)	Chaîne de sécurité automatique (détection et asservissement) (2)
Corrosion	Spécification des matériaux de construction, procédures d'inspection (3)	Revêtements spéciaux internes ou externes, protection cathodique (4)
Vibration	(3)	(5)
Événements secondaires	**Barrières de sécurité de protection**	
Flaque	Bassin de rétention (6)	Procédures générales d'urgence (alerte, mobilisation, etc.) (8)
Bouffée	Confinement de protection (5)	(7)(8)
Rejet diphasique	Dispositif d'extraction de traitement des gaz (7)	(8)
Rejet gazeux	(7)	(8)

Figure 8 : Représentation détaillée d'un scénario d'accident par l'approche nœud papillon avec les barrières de sécurité

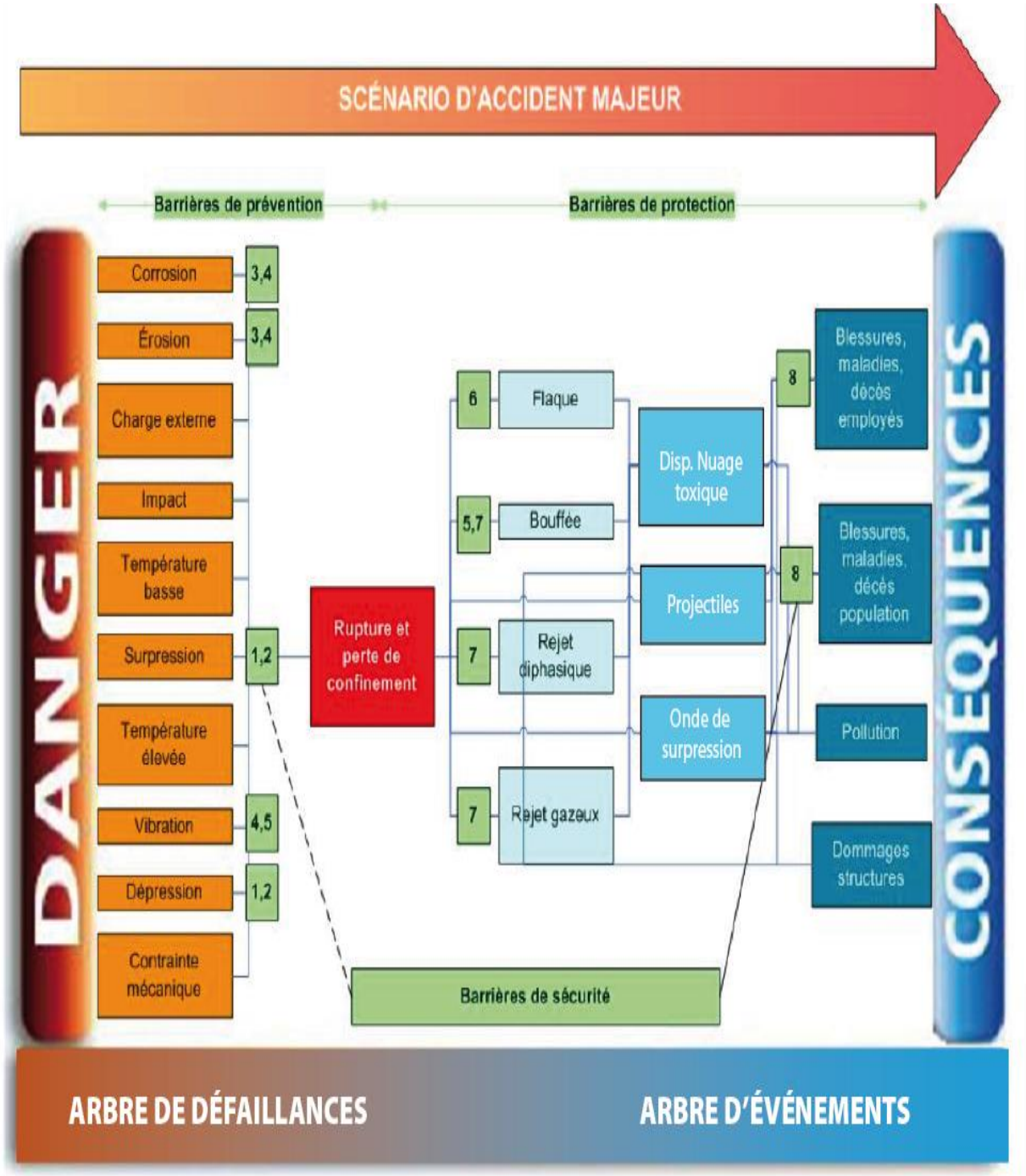


Figure 9 : Autre représentation détaillée d'un scénario d'accident par l'approche nœud papillon

3.5 / Méthode de Markov (MdM)

Figure 10 : Andrei Andreyevich Markov

3.5.1/ Modèles a Etats Transitions

La Méthode de l'Espace d'Etat (MEE) a été développée pour l'analyse de sureté de fonctionnement de système réparable.

Les arbres de défaillances, vus dans la partie précédente, permettent de bonnes descriptions statiques de système mais ne prennent pas en compte les reconfigurations, comme les réparations.

Les premières utilisations des processus stochastiques dans les années 50 utilisaient des processus markoviens ; des généralisations ont ensuite été faites.

Dans cette partie nous nous concentrons sur les processus markoviens.
Andrei Markov a publié ses premiers résultats en 1906, qui ont ensuite été généralisés à un espace d'états infini dénombrable par Andrei Kolmogorov en 1936.

Un processus stochastique est un ensemble de variables aléatoires (Xt) $t \geq 0$ a valeurs dans l'ensemble des observations.

Un processus est markovien si la probabilité de passage de l'étape présente à la suivante ne dépend pas du passe.

$$P(Xt \in A \mid Xtn \in An; \ldots ; X1 \in A1) = P(Xt \in A \mid Xtn \in An)$$

3.5.2 / Construction d'un modèle

Considérons un système compose de n composants, chaque composant ayant un nombre fini d'états de fonctionnement et de panne ; ce système est supposé réparable et chaque composant est réparé après constatation de la panne.

Le système est donc composé :

- des états de fonctionnement : un état de bon fonctionnement ou tous les composants fonctionnent, et des états ou certains composants sont en panne mais le système reste fonctionnel,

- des états de pannes : ou suffisamment de composants sont en panne pour affecter le système globale.

La construction du modèle se fait en 3 étapes

1. recensement de tous les états du système. Si chaque composant a 2 états (ok ou panne) et si le système a n composants, le nombre maximal d'états est 2n. Au cours de la vie du système, des états de panne peuvent apparaitre à la suite de défaillance ou disparaitre a la suite de réparation ;

2. recensement de toutes les transitions possibles entre ces différents états et l'identification de toutes les causes de ces transitions. Les causes des transitions sont généralement des défaillances des composants ou la réparation de composants ;

3. calcul des probabilités de se trouver dans les différents états au cours d'une période de vie du système, calcul des temps moyens (MTTF, MTBF, MTTR . . .)

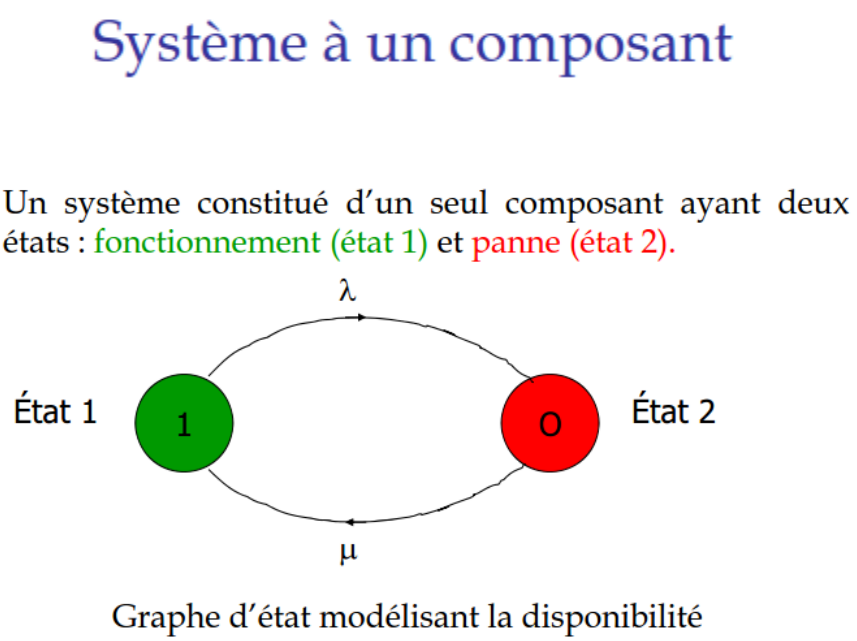


Figure 11: Exemple Graphe de Markov