Notice de la méthode Arbre des défaillances

Temps de lecture

15 minutes

A - Présentation générale de la méthode APR

1. Objectifs de la méthode

L'arbre de défaillance est une méthode qui part d'un événement final (ou événement redouté) pour remonter vers les causes et conditions, dont les combinaisons et enchainements d'événements peuvent le produire. Il vise à représenter de façon synthétique l'ensemble des combinaisons qui peuvent induire à l'événement étudié. C'est pour cela qu'il est représenté sous forme d'arbre. L'objectif étant de répondre à des questions telles que "comment une défaillance X peut-elle survenir ?" ou "quels sont les scénarios envisageables pouvant aboutir à une défaillance X ?".

La construction et l'utilisation d'un arbre de défaillance se fait dans le cadre d'une étude *a priori* d'un système. Ayant pour point de départ un événement redouté (dysfonctionnement ou accident), la démarche consiste à s'appuyer sur la connaissance des éléments constitutifs du système étudié d'identifier tous les scénarios conduisant à l'événement redouté. L'arbre de défaillance est une représentation des enchaînements qui peuvent conduire à l'événement redouté. C'est le point de départ de la démarche.

Il est possible d'utiliser cette représentation pour calculer la probabilité de l'événement redouté à partir des probabilités des événements élémentaires qui se combinent pour le provoquer. Mais cet aspect ne sera pas traité dans le cadre de cette formation.

La méthode de l'arbre de défaillance est composée d'une partie qualitative, à travers la construction de l'arbre et la recherche des coupes minimales (ensembles d'événements de base, ou de conditions, nécessaires et suffisants à produire la défaillance), et d'une partie quantitative qui vise à évaluer les probabilités d'occurrence au niveau des événements élémentaires, des coupes minimales et au niveau de la défaillance (aspect non traité dans le cadre de cette formation).

2. Champ d'application

L'analyse des risques par arbre des défaillances est appliquée dans de nombreux domaines tels que l'aéronautique, le nucléaire, l'industrie chimique, etc. Lorsque l'événement redouté final est connu car observé, cette méthode peut être utilisée pour analyser a posteriori les causes d'accidents qui se sont produits. On parle alors d'analyse par arbre des causes. L'objectif principal étant de déterminer les causes réelles qui ont conduit à l'accident.

3. Historique de la méthode

La méthode d'arbre des défaillances a été créée en 1962 aux Etats-Unis dans la société BELL dans le cadre du programme Minuteman (missile balistique). Elle a ensuite été développée pour la sûreté nucléaire (rapport Rasmusse) et pour Boeing. Il existe également d'autres appellations pour les arbres des défaillances, telles que l'*arbre des causes, arbre de défauts* et *Fault Tree*.

4. Intérêts de la méthode

Cette méthode permet de visualiser l'ensemble des combinaisons d'événements élémentaires conduisant à une défaillance. Elle permet donc d'avoir une vision globale et logique du fonctionnement et des dysfonctionnements d'un système.

La connaissance des coupes minimales (c'est-à-dire l'ensemble des événements de base ou des conditions nécessaires ou suffisantes à produire l'événement sommet), permet d'identifier, dès la phase de conception, les différents composants d'un système à améliorer pour qu'un événement ne se produise pas. Si on retire à une coupe minimale un seul de ses éléments, la défaillance, soit l'événement sommet, n'est plus générée. Afin de fiabiliser ces systèmes, il est nécessaire d'essayer de supprimer les coupes minimales.

L'identification des coupes minimales peut se faire en descendant l'arbre ligne par ligne. Cela permet ensuite d'éliminer les *redondances d'événements* dans une même coupe (il est inutile de citer plusieurs fois le même événement dans une coupe), d'éliminer les *redondances de coupes* (quand le même ensemble d'événements a été produit par plusieurs voies, il est inutile de le conserver en plusieurs exemplaires) et/ou d'éliminer les *« super-coupes »* qui en contiennent d'autres (quand un ensemble est strictement contenu dans un autre, il n'est utile de garder que le plus petit). La notion de coupe minimale ne sera pas abordée davantage dans cette notice.

5. Limites de la méthode

Cette méthode présente tout de même des limites à prendre en considération lors du choix de la méthode adéquate. En effet, pour que le calcul des probabilités d'occurrence soit correct, les événements intermédiaires doivent être indépendants les uns des autres (aspect non-traité dans le cas de cette formation). De plus, l'arbre des défaillances ne rend pas compte de l'aspect temporel des scénarios d'événements conduisant à la défaillance. Enfin, cette méthode est binaire, un événement peut soit se produire, soit ne pas se produire, ce qui n'est pas forcément représentatif de la réalité du terrain.

B - Application de la méthode APR

1. Démarche générale

Dans chaque arbre de défaillance, un événement indésirable, appelé événement sommet (*top e*vent), événement redouté ou encore événement non souhaité, est étudié. L'arbre de défaillance est généralement présenté de haut en bas. La ligne la plus haute, ou sommet de l'arbre, comporte uniquement la défaillance que l'on cherche à analyser. Les lignes inférieures vont détailler le ou les événement de la ligne supérieure en présentant la ou les combinaisons susceptibles de produire l'événement auquel elles sont rattachées. Ces relations sont présentées par des connecteurs logiques OU ou ET.

Les conditions ou événements causant directement l'événement sommet, appelés événements intermédiaires, sont listés comme descendants de l'événement sommet. La relation entre elles est représentée par un connecteur logique. Ce genre de décomposition est fait jusqu'à l'événement de base.

L'événement de base (*basic event*) est l'événement pertinent servant d'élément de référence dans le modèle (ex. défaillance de composants, erreur humaine ou atteinte de l'environnement).

La démarche générale s'agence de la manière suivante :

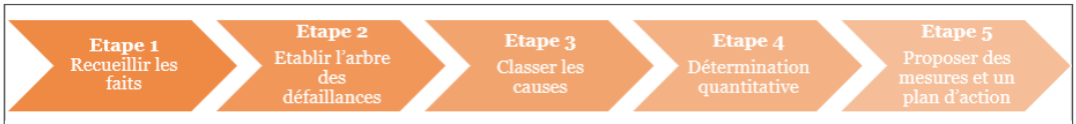


Illustration 1 : Etapes générales de la méthode de l'arbre des défaillances.

Dans cette notice, nous développerons l'étape 2 qui permettra, à la suite, de classer les causes (étapes 3).

2. Les différentes étapes de la méthode

Les principales étapes pour construire un arbre de défaillance sont de définir l'événement sommet à étudier, d'examiner le système et d'élaborer l'arbre de défaillance à l'aide de symboles et de connecteurs logiques.

Dans un second temps, afin d'analyser l'arbre pour la partie qualitative, il faut calculer des coupes minimales et valider de manière qualitative l'arbre. Pour la partie quantitative, il faut recueillir des données correspondant aux événements élémentaires, de calculer la probabilité des connecteurs et de la racine de l'arbre afin d'analyser les résultats obtenus pour trouver des solutions. Les parties qualitatives et quantitatives ne seront pas détaillées dans cette formation.

La construction de l'arbre se déroule donc de la manière suivante :

1/ Définition de l'événement sommet (ou indésirable)

La première étape consiste à définir l'événement sommet, c'est-à-dire la défaillance, de façon explicite et précise afin que l'arbre construit réponde bien aux attentes de l'étude.

Cet événement sommet doit être décomposé en événements intermédiaires pour rechercher les causes internes au sous-système, les causes amont/aval (ou de commande) et les causes externes. On considère ensuite chaque événement intermédiaire comme un nouvel événement sommet. Cette démarche sera réitérée jusqu'à l'obtention d'événements de base qui sont des événements qui ne se décomposent plus en événements plus fins.

Dans l'exemple suivant, un opérateur doit intervenir dans une salle équipée de deux lampes reliées à un interrupteur. Cependant, cette dernière est sans lumière. On représentera l'événement sommet dans un rectangle et on le définira comme "salle sans lumière".

2/ Examen du système

La deuxième étape consiste à décrire l'ensemble des événements par des combinaisons logiques (conjonction ou disjonction), pouvant engendrer l'événement sommet. Pour cela, il faut au préalable recueillir des données factuelles de manière objective, sans interpréter ni émettre de jugement, afin d'identifier l'ensemble des facteurs qui ont donné lieu à l'accident. Il y aura donc des événements moins globaux que l'événement sommet, que l'on nommera événements intermédiaires, et un connecteur logique qui les relie à l'événement sommet.

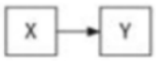
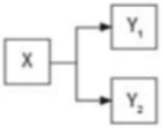
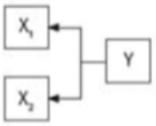
	Enchaînement	Disjonction	Conjonction
Définition	Un événement Y a une seule cause X	Deux ou plusieurs événements Y ont une seule et même cause X	Un événement Y a plusieurs causes immédiates X
Arbre de défaillances			
Caractéristiques	X est nécessaire et suffisant à lui seul pour que Y se produise	X est nécessaire et suffisant à lui seul pour que Y1 et Y2 se produisent	Les événements X1 et X2 sont nécessaires ensembles pour que Y se produise

Tableau 1. Différentes notions de l'arbre des défaillances.

Si nous reprenons notre exemple de "salle sans lumière", l'événement « salle sans lumière » peut être causé directement par une des trois conditions suivantes :

- Une coupure d'électricité
- Une défaillance de l'interrupteur
- Une défaillance des ampoules

La relation entre l'événement racine et ces trois conditions est donc indiquée par un connecteur de type OU.

Entre les trois conditions, la défaillance de l'interrupteur peut être considérée comme un événement de base sans cause directe. Quant à l'événement « coupure d'électricité », on peut identifier deux causes :

- Une défaillance d'alimentation
- Une défaillance du fusible

Le connecteur entre « coupure d'électricité » et ces deux causes du type événements de base est du type "OU". Si nous considérons les deux ampoules indépendantes l'une de l'autre, alors pour qu'il y ait une défaillance des ampoules nous devons avoir les deux ampoules en panne au même temps. Dans ce cas-là, le connecteur utilisée est un connecteur "ET". La défaillance d'une des deux ampoules est considérée comme un événement de base. Nous avons alors fini la construction de l'arbre de défaillance de cet événement indésirable.

3/ Élaboration de l'arbre des défaillances

Il existe un ensemble de symboles normalisés permettant de représenter l'événement sommet, les événements intermédiaires, les événements de base et les connecteurs. L'arbre des défaillances peut être construit avec l'outil PowerPoint.

Les principaux symboles utilisés sont regroupés dans le tableau suivant :

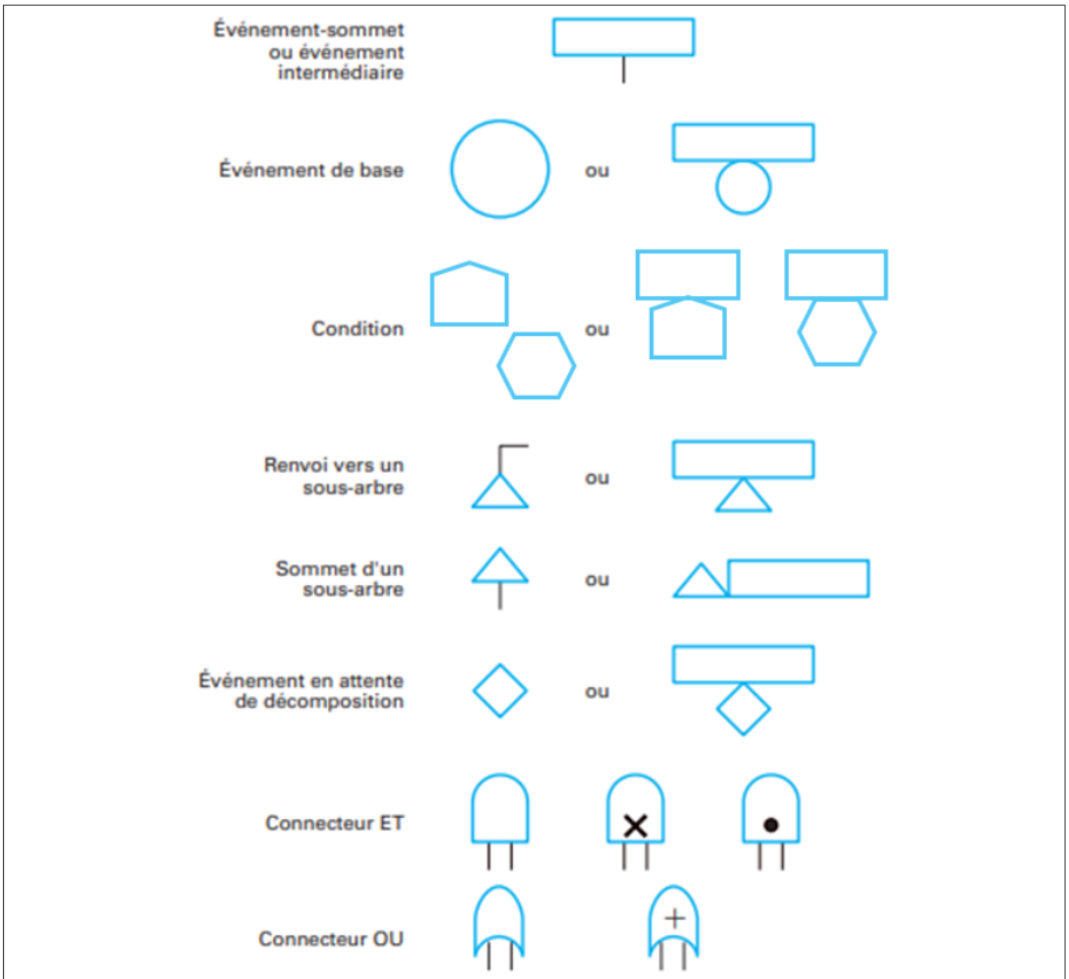


Tableau 2. Différents symboles de l'arbre des défaillances.

Exemple d'un arbre de défaillance pour l'exemple précédent :

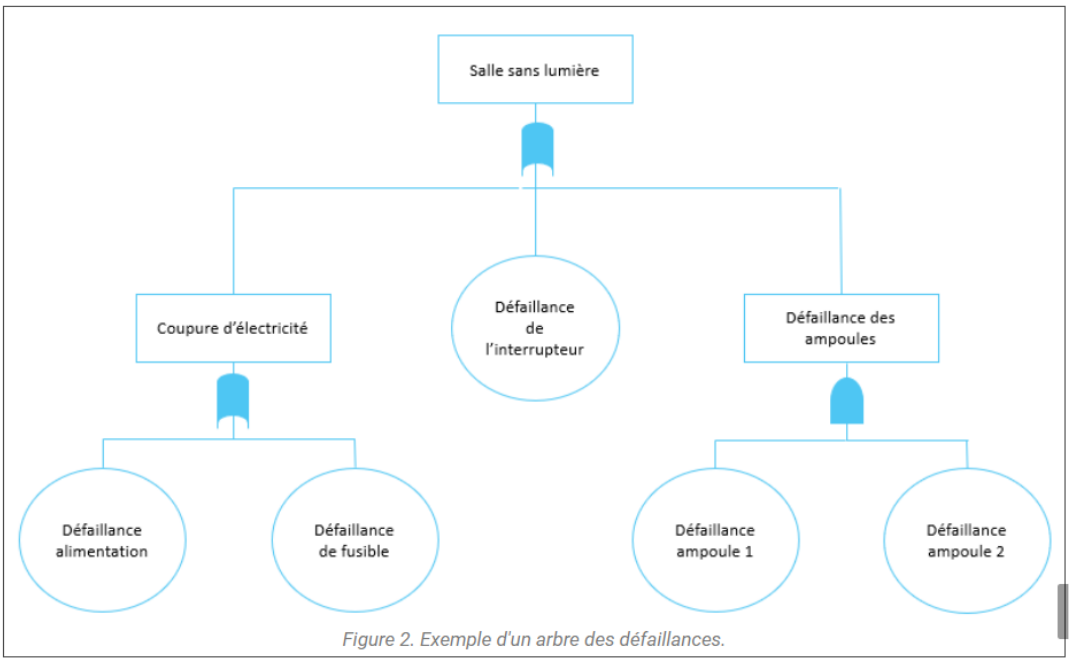


Figure 2. Exemple d'un arbre des défaillances.

Evaluez-vous !

Démarches préalables

Qu'est-il primordial de faire avant de construire l'arbre des défaillances ?

- [ ] Définir l'événement sommet
- [x] Collecter les données relatives à l'événement étudié
- [ ] Commencer à faire une ébauche de l'arbre des défaillances
- [ ] Décrire le système étudié

Application

Qu'est-ce que l'événement sommet ? (Choix multiples)

- [x] Une défaillance
- [x] Un événement redouté
- [x] Un événement non-souhaité
- [x] Un événement indésirable

Quelles sont les réponses correctes concernant les événements intermédiaires ? (Choix multiples)

- [ ] Ce sont des événements causant indirectement l'événement sommet
- [x] Ce sont des événements causant directement l'événement sommet
- [x] Les événements intermédiaires sont représentés par un rectangle dans l'arbre des défaillances
- [ ] Les événements intermédiaires sont représentés par un cercle dans l'arbre des défaillances