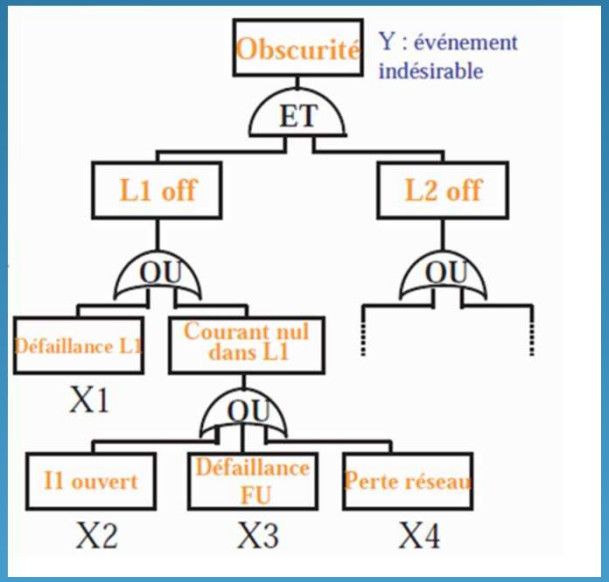
# Chapitre 6
# Arbre de Défaillance




Master 2- Génie Industriel
Spécialité-Ingénierie Logistique

# Chapitre 6

## 6. Arbre de Défaillances

# Sommaire

Démarche apparue dans les années 60 dans les domaines militaire et aéronautique puis nucléaire, chimique etc. ….. En vue d'analyser la fiabilité, la disponibilité et la sécurité,

Nécessité de prendre en compte les combinaisons de pannes: Augmentation de la sécurité des systèmes et donc de la complexité

## 5.5. Arbre de Défaillance

### Introduction

L'AdD est une méthode déductive utilisée dans de nombreux domaines industriels. C'est la méthode d'analyse de la fiabilité de la disponibilité et de la sécurité des systèmes la plus largement utilisée. Elle a pour objectifs de

- Déterminer les diverses combinaisons possibles d'événements qui entraînent la réalisation d'un E*N*S unique
- Quantifier les risques en déterminant la probabilité d'occurrence d'un événement ou d'un scénario

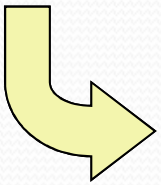
Démarche apparue dans les années 60 dans les domaines militaire et aéronautique puis nucléaire, chimique etc. ….. En vue d'analyser la fiabilité, la disponibilité et la sécurité,

Nécessité de prendre en compte les combinaisons de pannes: Augmentation de la sécurité des systèmes et donc de la complexité

## 6.1. Arbre de Défaillance

### Introduction

L'AdD est une méthode déductive utilisée dans de nombreux domaines industriels. C'est la méthode d'analyse de la fiabilité de la disponibilité et de la sécurité des systèmes la plus largement utilisée. Elle a pour objectifs de



- Déterminer les diverses combinaisons possibles d'événements qui entraînent la réalisation d'un E*N*S unique
- Quantifier les risques en déterminant la probabilité d'occurrence d'un événement ou d'un scénario

Un arbre de défaillance est une méthode-type pour répondre à une question du genre :

«Quelles chances  y a-t-il que le dispositif de détection et extinction automatique d'incendie manque à se déclencher en présence d'un feu et sur quoi peut-on agir pour diminuer cette probabilité ? »

« dans un système avec redondances, quelle est la probabilité finale d'échec en fonction des  probabilités élémentaires des composants et de l'architecture ? ».

- Définition

L'AdD (aussi appelé arbre de fautes) est une technique d'Ingénierie très utilisée dans les études de sécurité et de fiabilité des systèmes statique

- 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 » ou évènement Non Souhaité ENS).

La représentation graphique met donc en évidence les relations causes à effet

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 de l'ENS ou l'ER

## L'AdD est basé sur 2 Etapes

- l´étape Construction
- l´étape Traitement

## 6.1.1. Construction de l'Arbre

Elle est constitué de niveaux successifs d'événement tel que chaque événement à un niveau donné est généré à partir de combinaisons logiques d'événements de niveaux inférieurs.

Cette procédure est itérée jusqu'à atteindre les événements élémentaires appelés événements de base.

L'AdD est créé pas à pas pour atteindre à la base un ensemble d'événements considérés comme élémentaires

La construction de l'Arbre est une phase délicate dont l'accomplissement nécessite la connaissance aussi parfaite que possible du système étudié.

Construire un arbre de défaillance revient à répondre à la question «comment tel événement peut-il arriver ? », ou «quels sont tous les enchaînements possibles qui peuvent aboutir à cet événement ? ».

**Elle débute par la définition précise d'un ENS.**

La première étape réside dans la définition de l'évènement à étudier d'une façon explicite et précise

**ENS ou ER** constitue l'événement sommet de l'arbre

L'identification a lieu en amont de la construction, en se servant de méthodes qui permettent d'identifier les risques tout en explorant les causes et les effets

La question-clé est : "Que se passerait-il si..?"

L'ENS est alors décomposé en événements intermédiaires qui sont, seuls ou en conjonction, les causes immédiates de son apparition

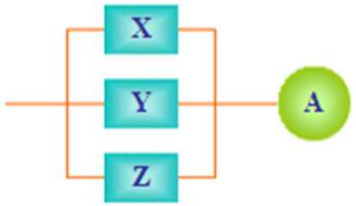
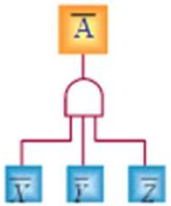
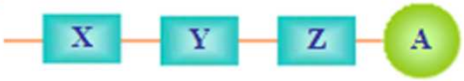
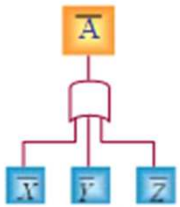
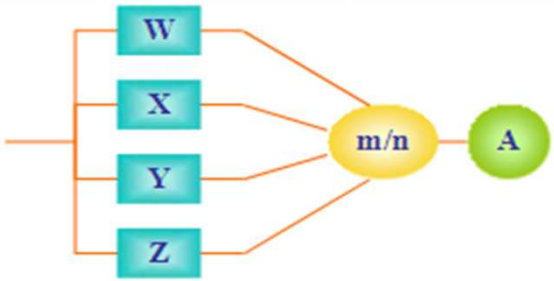
Les causes de ces événements intermédiaires sont à leur tour recherchées et ce processus déductif se poursuit jusqu'à atteindre des événements dont la décomposition s'avère impossible ou inutile

Ces derniers événements sont appelés événements primaires ou événements élémentaires

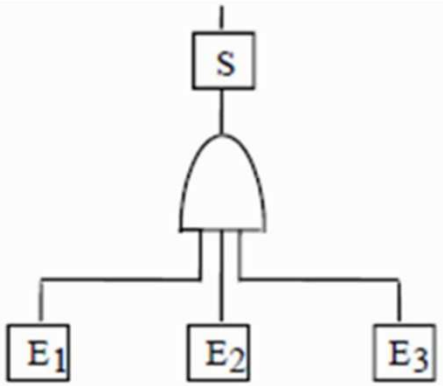
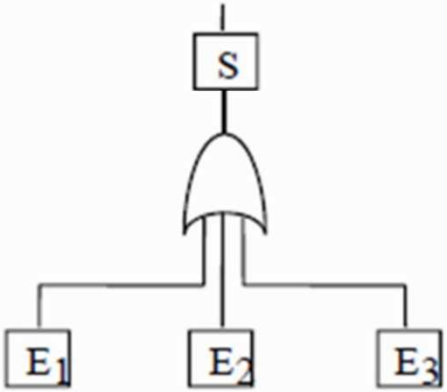
La décomposition d'un événement- intermédiaire en ses événements- causes s'effectue à l'aide d'opérateurs logiques appelés portes.

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

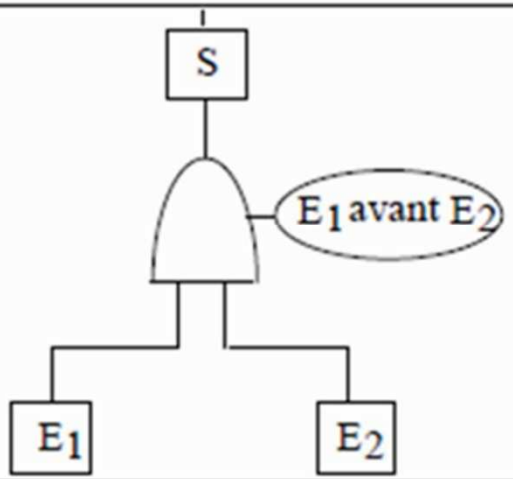
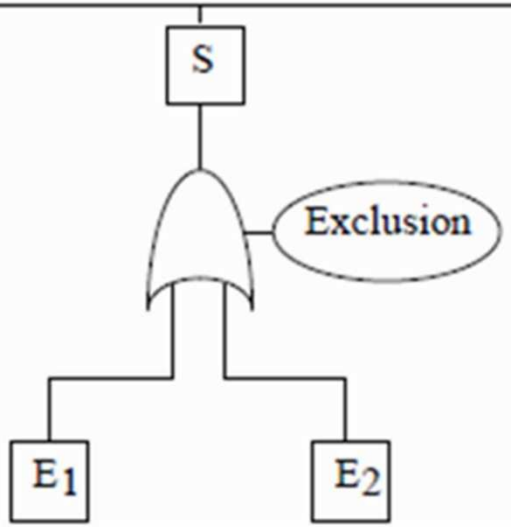
- Evènements ;
- Portes ;
- Symboles de transfert.

| Représentation fonctionnelle | Opérateur (Dysfonctionnel) | Symbole |
|---|---|---|
| OU   | ET |   |
| ET   | OU |   |
|   | COMBINAISON (m, n) |   |

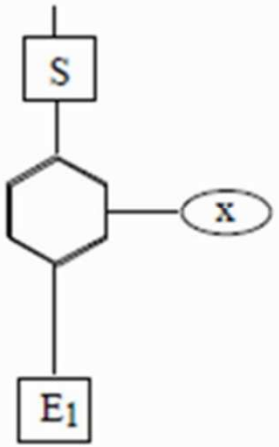
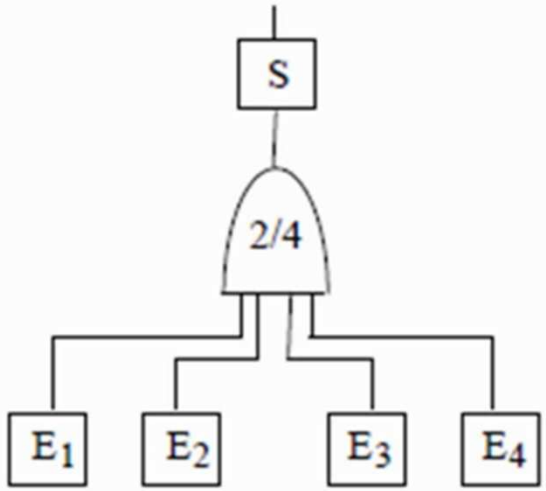
## ❑ Typologie et représentation graphique des portes

| *Symbole* | *Nom du Symbole* | *Signification du symbole* |
|---|---|---|
|  | Porte ET | L'événement de "sortie" (ici S) de la porte ET est généré si tous les événements d'entrée (ici $E_1$, $E_2$ et $E_3$) sont présents simultanément |
|  | Porte OU | L'événement de "sortie" (ici S) de la porte OU est généré si l'un au moin des événements d'entrée (ici $E_1$ ou $E_2$ ou$E_3$) est présent : la porte est appelée aussi OU exclusif |

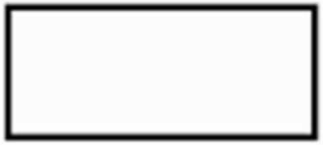
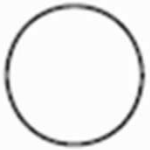
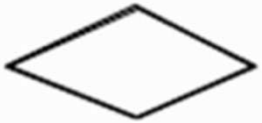
## ❑ Typologie et représentation graphique des portes (suite)

| *Symbole* | *Nom du Symbole* | *Signification du symbole* |
|---|---|---|
|  | Porte ET avec condition | L'événement de "sortie" (ici S) est généré si tous les événements d'entrée (ici $E_1$ et $E_2$) sont présents et si la condition (ici $E_1$ est présent avant $E_2$) est réalisée |
|  | Porte OU avec exclusion | L'événement de "sortie" (ici S) de la porte OU est généré si l'un au moin des événements d'entrée (ici $E_1$ ou $E_2$ ou $E_3$) est présent et si la condition est réalisée (ici, il faut que $E_1$ et $E_2$ ne soient pas présents simultanément);<br>la porte est appelée aussi OU EXCLUSIF |

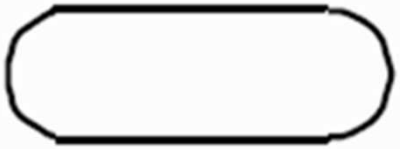
## ❑ Typologie et représentation graphique des portes (suite)

| *Symbole* | *Nom du Symbole* | *Signification du symbole* |
|---|---|---|
|  | Porte SI | L'événement de "sortie" (ici S) est généré l'événements d'entrée (ici $E_1$) est présent et si la condition X est réalisée |
|  | Porte COMBINAISON m/n (ici 2/4) | L'événement de "sortie" (ici S) est généré si m des événements d'entrée sont présents (ici il suffit que 2 des événements $E_1$, $E_2$, $E_3$, $E_4$ soient présents) |

## ❑ Typologie et représentation graphique

| *Symbole* | *Nom du Symbole* | *Signification du symbole* |
|---|---|---|
|  | rectangle | Représentation d'un événement (événement indésirable ou intermédiaire) résultant de la combinaison d'autres événements par l'intermédiaire d'une porte logique. |
|  | cercle | Représentation d'un événement élémentaire ne nécessitant pas de futur développement |
|  | losange | Représentation d'un événement qui ne peut être considéré comme élémentaire mais dont les causes ne sont pas et ne seront pas développées |

## ❑ Typologie et représentation graphique (Suite)

| *Symbole* | *Nom du Symbole* | *Signification du symbole* |
|---|---|---|
|  | double losange | Représentation d'un événement dont les causes ne sont pas encore développées mais le seront ultérieurement |
|  | maison | Représentation d'un événement de base qui est un événement survenant normalement pendant le fonctionnement du système. |
|  | ovale | Représentation d'un événement conditionnel qui peut être utilisé avec certaines portes logiques |

- Définition des évènements de base
  - Elémentaire
    - Généralement une défaillance
    - Phénomène assez connu pour ne pas le développer plus (probabilité faible)
  - Non élémentaire et non développé
    - Evènement étant une cause externe du système étudié ( alimentation HS)
    - Porte  ET avec plus de trois branches
  - Non élémentaire et non développé momentanément
    - Pas de renseignement suffisants
    - A développer par un fournisseur ou a documenter

- Détermination de toutes les causes menant à l'EI
  - Evènements Elémentaires
  - Ils sont organisés soit en panne simple soit en combinaison de pannes
  - Ils touchent
    - Défaillance de commande (rupture d'alimentation, défaillance logicielle
    - Défaillance intrinsèques (conception, utilisation, agression extérieure, erreur humaine, procès,
  - Les défaillances prises en compte sont fonction des limites de l'étude
    - Agressions extérieures
    - Problèmes de procès
    - Erreur humaine

- le système est soit
  - Non commandé, mauvaise commande ou pas de commande. Une commande peut être
    - Un flux: information (électrique, électromagnétique, etc.), matière (gaz, liquide, etc.)
      - ex: pas d'alimentation (carburant, électricité etc. ) à l'entrée d'un moteur. Pas de commande issue d'un calculateur. Mauvaise information issue d'un capteur
    - Une interaction mécanique: contact, tension, support, etc.
      - ex: pas de transmission du mouvement de translation ensemble bielle /manivelle

## ❑ Typologie et représentation graphique (Suite)

| *Symbole* | *Nom du Symbole* | *Signification du symbole* |
|---|---|---|
|  | triangle | La partie de l'arbre des causes qui suit le symbole  est transféré à l'emplacement indiqué par le symbole  |
|  | triangle inversé | Une partie semblable, mais non identique à celle qui duit le symbole  est transféré à l'emplacement indiqué par le symbole  |

# 6.1.2. Procédure de Construction de l'Arbre

La construction de tout arbre comporte deux phases distinctes

La première phase est celle de la définition du système étudié, pour l'accomplir il est nécessaire de:

- Définition du système

- Préciser clairement les limites et la mission du système
- Connaître l'environnent du système et son impact sur le système.
- Énumérer les différents constituants, SS ou composants et d'expliciter leur état initial et leur fonction
- En déduire leurs modes de défaillances

En effet, un potentiomètre dont la fonction est de délivrer entre deux de ses bornes une ddp peut en être empêcher s'il est en court-circuit ou en circuit ouvert. Il en résulterait un comportement non binaire de ce composant ce qui pourrait induire de sérieuses difficultés au niveau du traitement quantitatif.

## ❑ Définition de événement non souhaité

La définition de l'ENS doit se faire sans ambiguïté

Construction de l'arbre

C'est une démarche systématique qui requiert un minimum de rigueur indispensable si l'on désire éviter certaines omissions et prétendre à une relative exhaustivité.

A cette fin il est conseillé de s'astreindre à respecter les quelques règles générales que nous rappellerons ci-après.

## ❑ Règles de construction

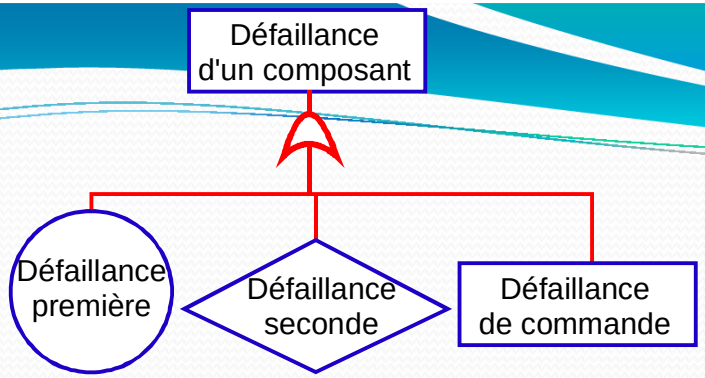
### Règle 1: " **quoi et quand** "

L'analyste doit s'efforcer d'expliciter le libellé de l'événement - sommet et ensuite, de tout événement intermédiaire en précisant en quoi il consiste quand il s'est manifesté

**Le moteur refuse de démarrer lorsqu'il est alimenté.**

### Règle 2 " **Classification des événements en "défaut concernant le composant« et "défaut concernant le système"**

Si l'évènement concerne le composant il est alors la sortie d'une porte OU ayant trois entrées




Règle 3 " **Cause (s) immédiate (s)"**

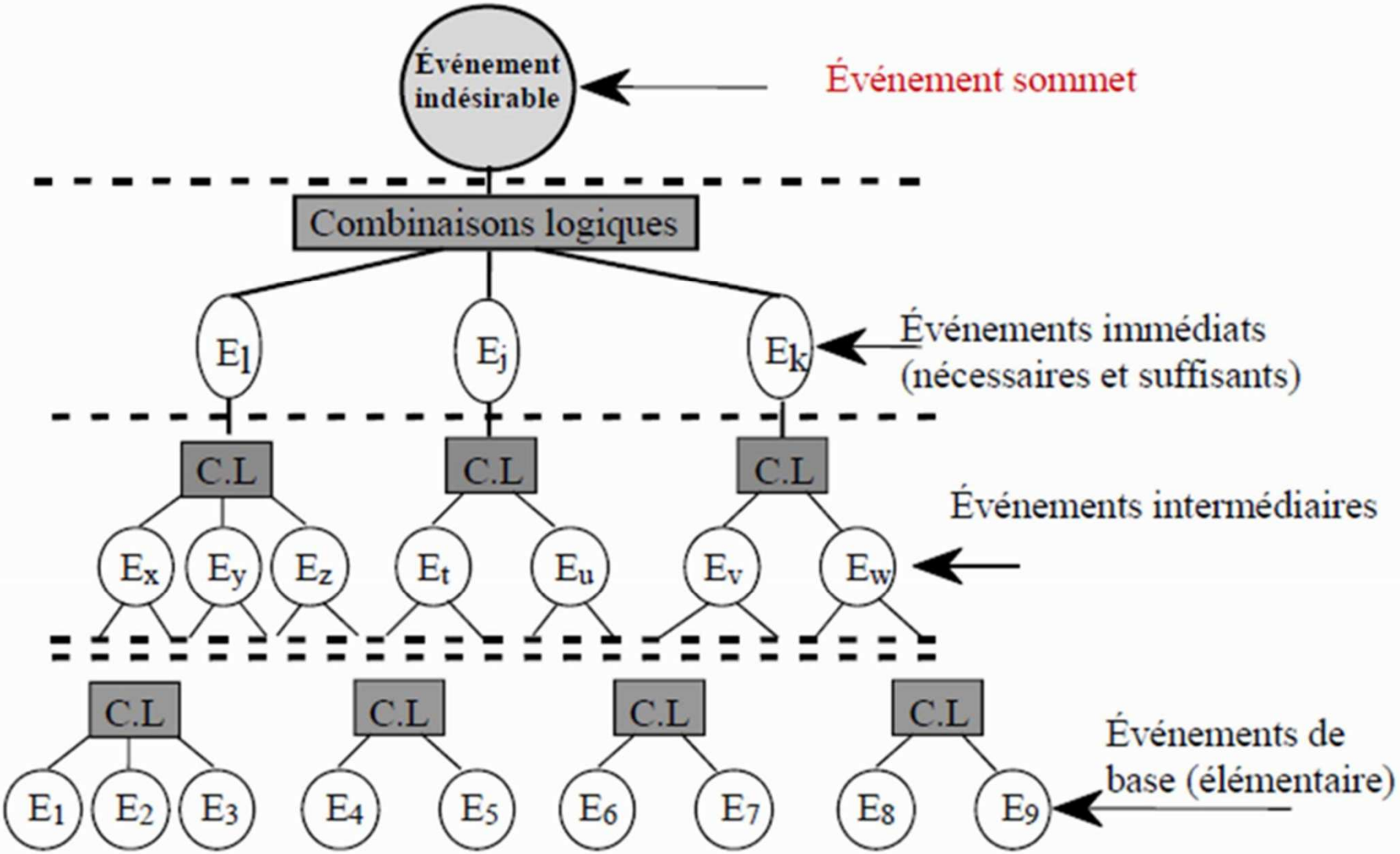
Règle 4 " **Pas de porte à porte. Pas de connexion directe entre deux portes "**

Résumé des règles importantes de la construction de l'arbre de défaillance

- Partir de l'ER(sommet de l'arbre),
- Imaginer les évènements intermédiaires possibles expliquant l'évènement sommet,
- Considérer chaque évènement intermédiaire comme un nouvel évènement sommet
- Imaginer les causes possibles de chaque évènement au niveau considéré,
- Descendre progressivement dans l'arbre jusqu'aux évènements de base.

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

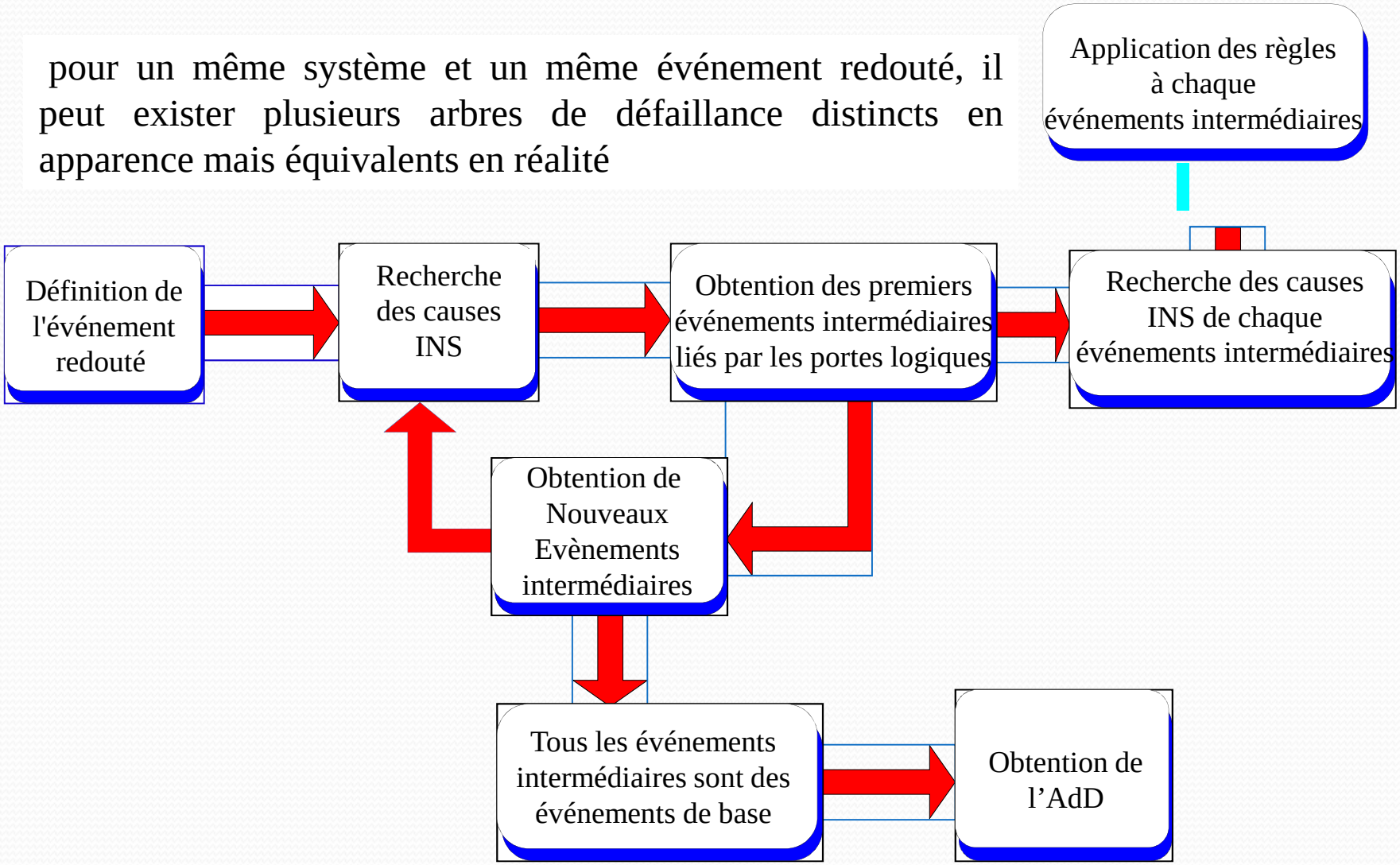
## ❑ Construction



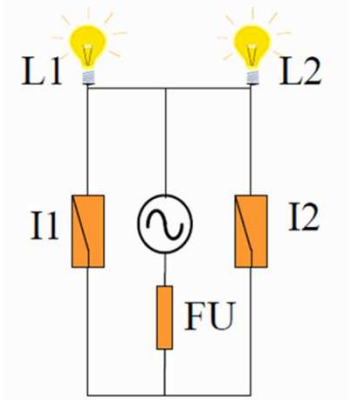
## ❑ Conclusion

Pour tout système, il existe autant d'arbres de défaillances distincts que d'événements redoutés différents retenus.

pour un même système et un même événement redouté, il peut exister plusieurs arbres de défaillance distincts en apparence mais équivalents en réalité

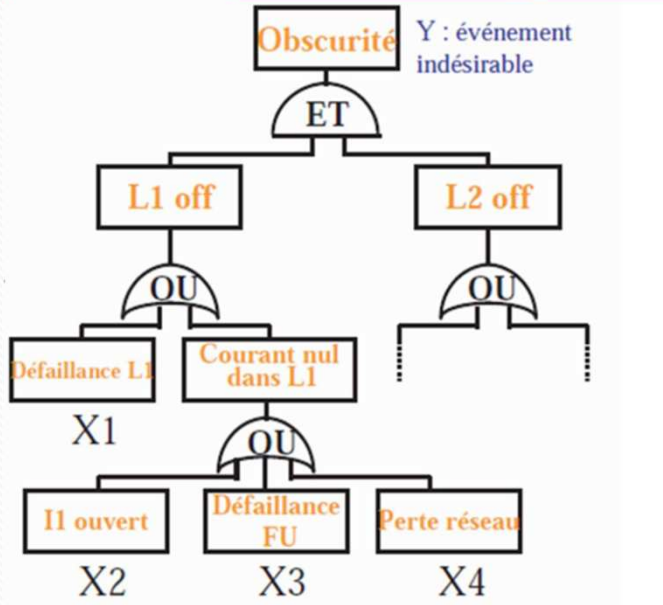


## ❑ Exemple

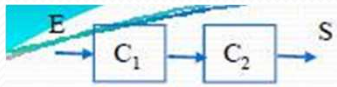



**Mission indésirable**

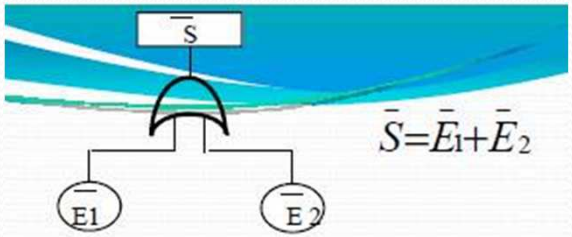
**Obscurité**



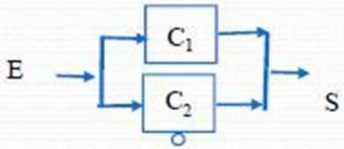

## ❑ Analogie entre DdF et AdD



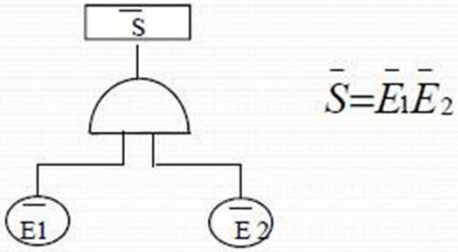

$S=E_1E_2$




$\bar{S}=\bar{E}_1+\bar{E}_2$




$S=E_1+E_2$




$\bar{S}=\bar{E}_1\bar{E}_2$

# 6.1.3. Traitement de l'Arbre

Cette seconde phase de traitement, à laquelle on peut adjoindre une étude complémentaire, constitue l'analyse quantitative

Etablir la liste de toutes ces combinaisons d'événements connus sous le non de coupes et extraire les coupes minimales du système.

Une coupe est une conjoncture d'événements élémentaires dont l'occurrence simultanée est nécessaire et suffisante pour que l'événement redouté se produise

Les coupes minimales peuvent être obtenues soit manuellement si la taille de l'AdD est réduite, soit, à l'aide de codes informatiques basés sur des algorithmes mathématiques.

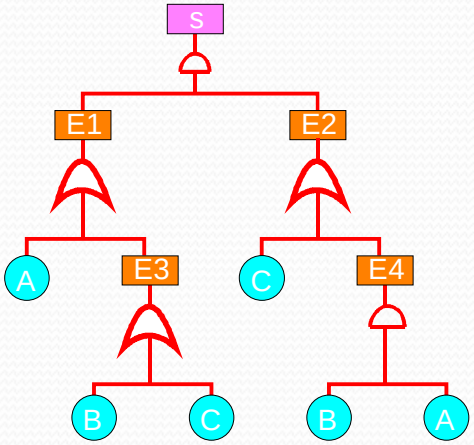
Les algorithmes de simulation du type Monté Carlo**;**

Les algorithmes de détermination et de manipulation algébrique de l'expression booléenne de l'événement- sommet de l'arbre

Les algorithmes qualifiés de matriciels

## ❑ Algorithme Algébrique

Pour déterminer les coupes minimales de cet arbre il est d'abord nécessaire de donner pour chaque porte l'équation booléenne équivalente puis, par substitution successives celle de l'événement sommet S.




### o Algorithme descendant

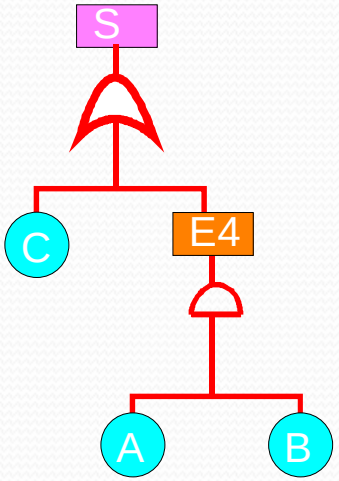
$$S = E_1 . E_2$$
$$= (A + E_3) . (C + E_4)$$
$$= (A.C) + (A. E_4) + ( E_3 . C) + ( E_3 . E_4)$$

### o Algorithme ascendant

$$E_1 = A + E_3 = A + B + C$$
$$E_2 = C + E_4 = C + A. B$$
$$S = E_1 . E_2 = (C + A. B)(A + B + C)$$
$$S=AC+AAB+BC+ABB+CC+ABC$$

o Les deux algorithmes précédents conduisent à l'arbre réduit ci dessous

**S=C + A . B**



## ❑ Algorithme Matriciel

On ne présente que l'algorithme descendant dû à Fussell et Veseley. Il repose sur la constatation suivante: Une porte OU augmente le nombre de coupes alors qu'une porte ET augmente leur longueur

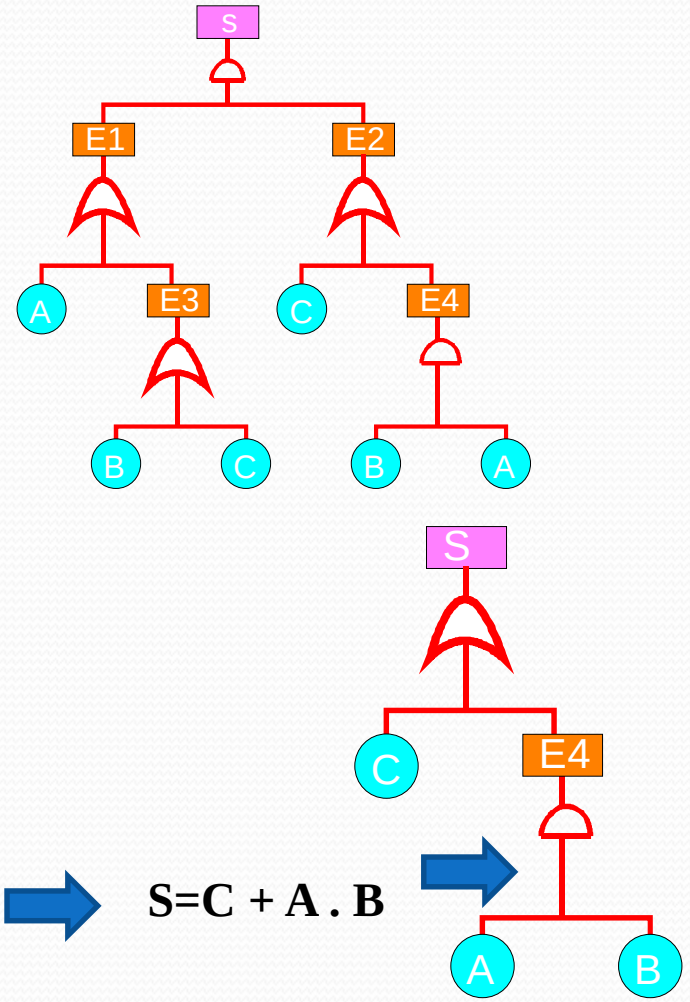
$$[ET\ 1] \Rightarrow [OU\ 2 \quad OU\ 3] \Rightarrow \begin{bmatrix} A & OU\ 3 \\ OU\ 4 & OU\ 3 \end{bmatrix}$$

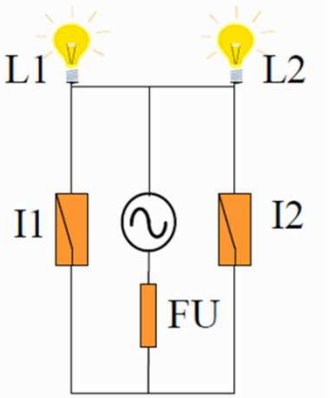
$$\begin{bmatrix} A & OU\ 3 \\ B & OU\ 3 \\ C & OU\ 3 \end{bmatrix} \Rightarrow \begin{bmatrix} A & C \\ A & ET\ 5 \\ B & OU\ 3 \\ C & OU\ 3 \end{bmatrix} \Rightarrow \begin{bmatrix} A & C \\ A & A & B \\ B & OU\ 3 \\ C & OU\ 3 \end{bmatrix}$$

$$\begin{bmatrix} A & C \\ A & B \\ B & C \\ B & ET\ 5 \\ C & OU\ 3 \end{bmatrix} \Rightarrow \begin{bmatrix} A & C \\ A & B \\ B & C \\ B & A & B \\ C & OU\ 3 \end{bmatrix} \Rightarrow \begin{bmatrix} A & C \\ A & B \\ B & C \\ A & B \\ C & C \\ C & ET\ 5 \end{bmatrix}$$

$$\begin{bmatrix} A & C \\ A & B \\ B & C \\ A & B \\ C & C \\ C & A & B \end{bmatrix}$$

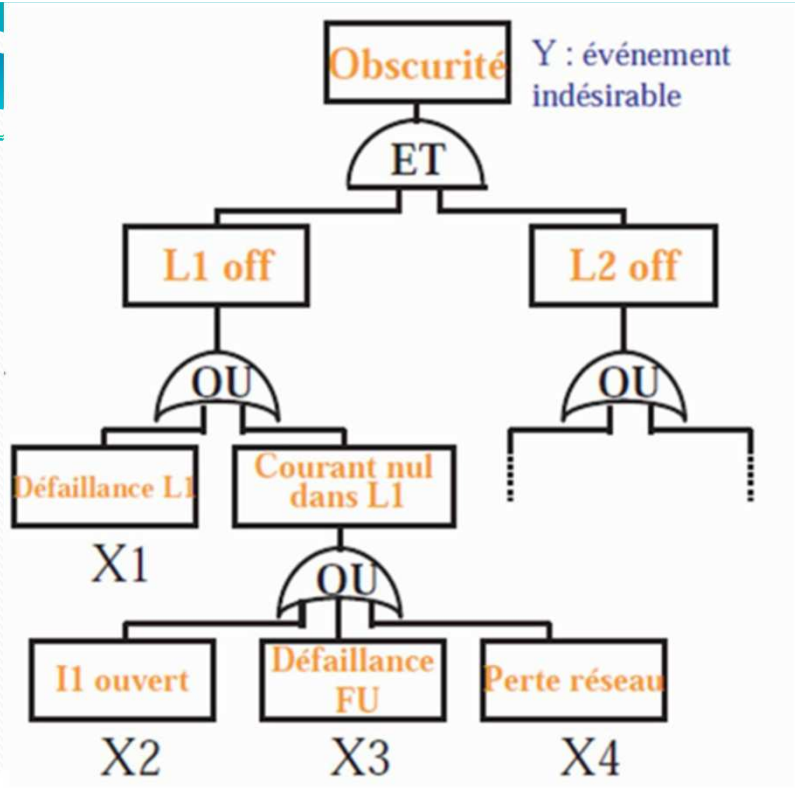
Soit après réduction $\begin{bmatrix} C \\ A & B \end{bmatrix}$ ⇒ **S=C + A . B**



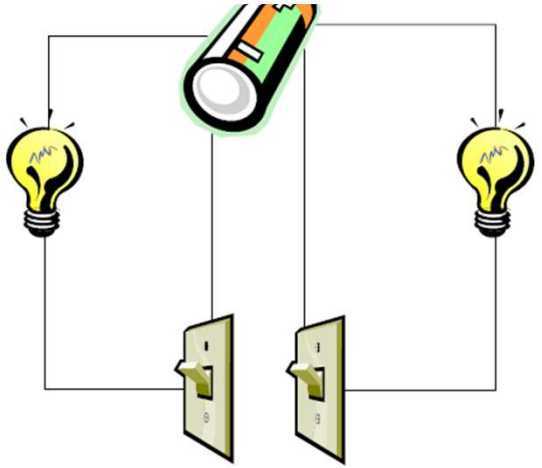



Mission indésirable

Obscurité



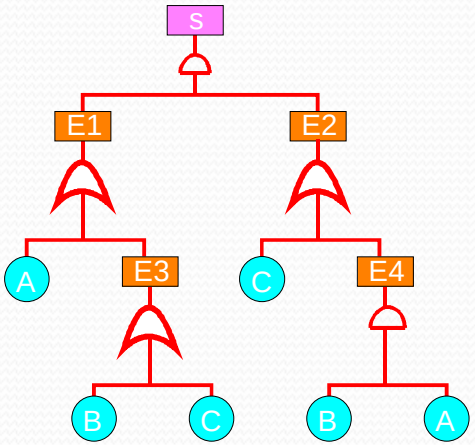

Probabilités
Interrupteur Off =50%
Ampoule grillée=1%
Batterie vide=1%



E.R : Pas d'éclairage

# 6.1.4. Coupes minimales

- une « coupe » est un ensemble d'événements entrainant l'événement indésirable
- une « coupe minimale » ou « chemin critique » est la plus petite combinaison d'événements entrainant l'événement indésirable cad, si un des événements d'une coupe minimale ne se produit pas, l'événement indésirable ne se réalise pas
- un AdD a un nombre fini de coupes minimales
  - une « coupe minimale d'ordre 1» représente les simples défaillances qui entrainent l'événement indésirable
  - une « coupe minimale d'ordre 2» représente les doubles défaillances qui, se produisant en même temps, entrainent l'événement indésirable
- les « coupes minimales» d'ordre minimal représentent en effet les « maillons faibles » du système




**S=C + A . B**

Coupe minimale d'ordre 1, la défaillance de C
Coupe minimale d'ordre 2, la défaillance de A ET B

## Conclusion

Les AdD sont utilisés particulièrement pour l'étude de fiabilité des systèmes complexes. Ils permettent de modéliser les relations causales de défaillance d'un système entre les différentes entités basiques qui peuvent provoquer une défaillance globale du système et ainsi estimer la probabilité d'apparition d'une défaillance.

### Avantages :

- L'analyse par AdD est la plus couramment utilisée dans le cadre d'études de fiabilité, de disponibilité ou de sécurité des systèmes.
- Son aspect, 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.
- Le processus de construction de l'arbre basé sur une méthode déductive permet à l'analyste de se focaliser uniquement sur les événements contribuant à l'apparition de l'événement redouté.
- Une fois la construction de l'arbre terminée, deux modes d'exploitation sont possibles:
  - l'exploitation qualitative
  - l'exploitation quantitative
- 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.

## Limites :

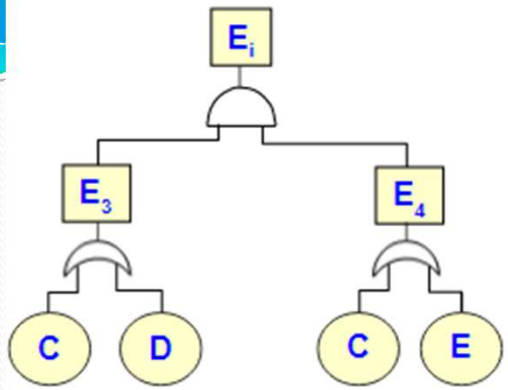
L'utilisation de l'arbre de défaillances devient inefficace ou difficilement applicable lorsque les caractéristiques suivantes apparaissent :

- 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.
- 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.
- 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.
- 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

# 6.2. Exercices d'application

## Exercice 1

1. Réduire l'arbre de défaillance
2. Identifier les coupes minimale
3. Quel est le diagramme de Fiabilité correspondant




## Exercice 2

Considérons l'AdD de la figure ci contre

1. Calculer l'événement non désiré E1 en fonction des événements élémentaires
2. Rechercher les coupes minimales
3. Donner le digramme bloc fiabilité correspondant