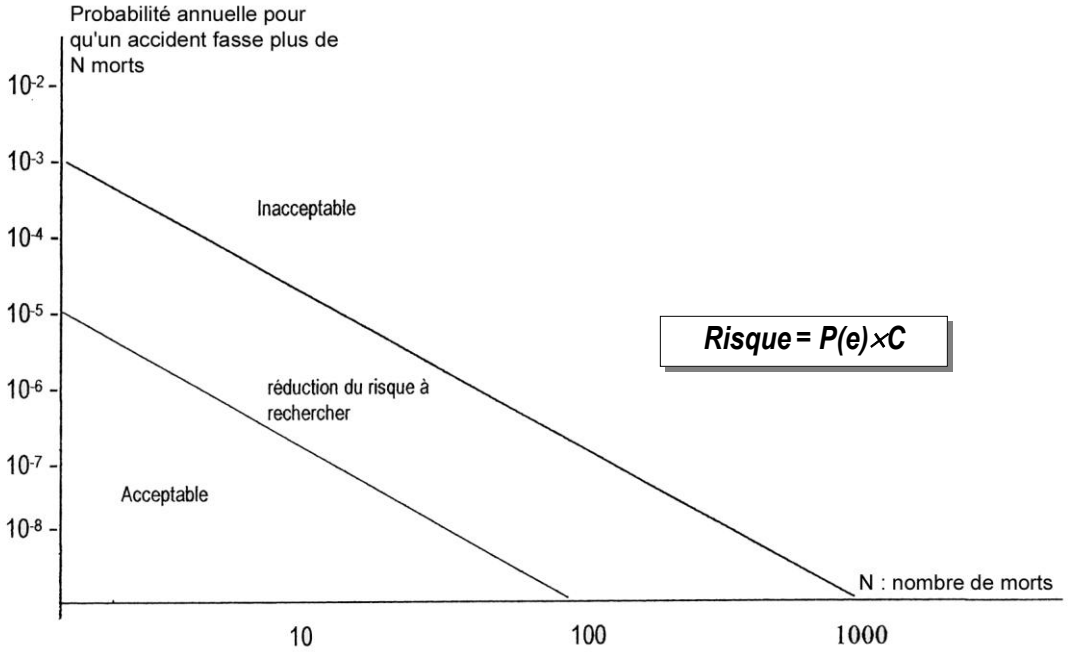
LA SURETE DE FONCTIONNEMENT

I – DEFINITION :

Toute situation de travail ou de la vie quotidienne présente des risques : risques technologiques, économiques, dans les transports, écologiques, sanitaires, naturels, etc. Le risque est l'évaluation d'un **DANGER** et est une notion intuitive et subjective. Le risque a 2 dimensions :

- La probabilité d'occurrence d'un évènement : P(e)
- Les conséquences ou les dommages de l'évènement : C. Un dommage est un préjudice et / ou un dégât direct causé aux personnes et aux biens.



Risque = P(e)×C

Les techniques mises en œuvre pour identifier, analyser et gérer les risques ont été regroupées sous différentes expressions :

- Etudes probabilistes de sûreté dans le nucléaire
- Analyse des risques chez les pétroliers
- Aléatique (du mot aléa), cindynique (du grec cindynos : danger), FMDS
- **Sûreté de fonctionnement ou SDF**

Un système qui a un fonctionnement **sûr** est un système qui réalise ce pourquoi il a été conçu, sans incident mettant sa rentabilité en question et sans accident mettant la sécurité en jeu.

Norme NF X 60-010 : la sûreté de fonctionnement est l'ensemble des aptitudes d'un bien qui lui permettent de remplir sa fonction, au moment voulu, pendant la durée prévue, sans dommage pour lui-même et son environnement. Elle se caractérise par 4 paramètres : fiabilité, maintenabilité, disponibilité et sécurité.

<table>
<tr><td colspan="4">Sûreté de fonctionnement
Aptitude à assurer un service spécifié</td></tr>
<tr><td>Sécurité</td><td colspan="2">Disponibilité
Aptitude à être en état de marche à un instant donné ou pendant un intervalle de temps donné</td><td>+ Logistique de Maintenance</td></tr>
<tr><td>Aptitude à ne présenter aucun danger pour les personnes, les biens et l'environnement.</td><td>+ Fiabilité
Aptitude à ne pas présenter de défaillance dans un intervalle de temps donné.</td><td>+ Maintenabilité
Aptitude à être remis en service dans une durée donnée.</td><td>Politique et moyens de maintenance.</td></tr>
</table>

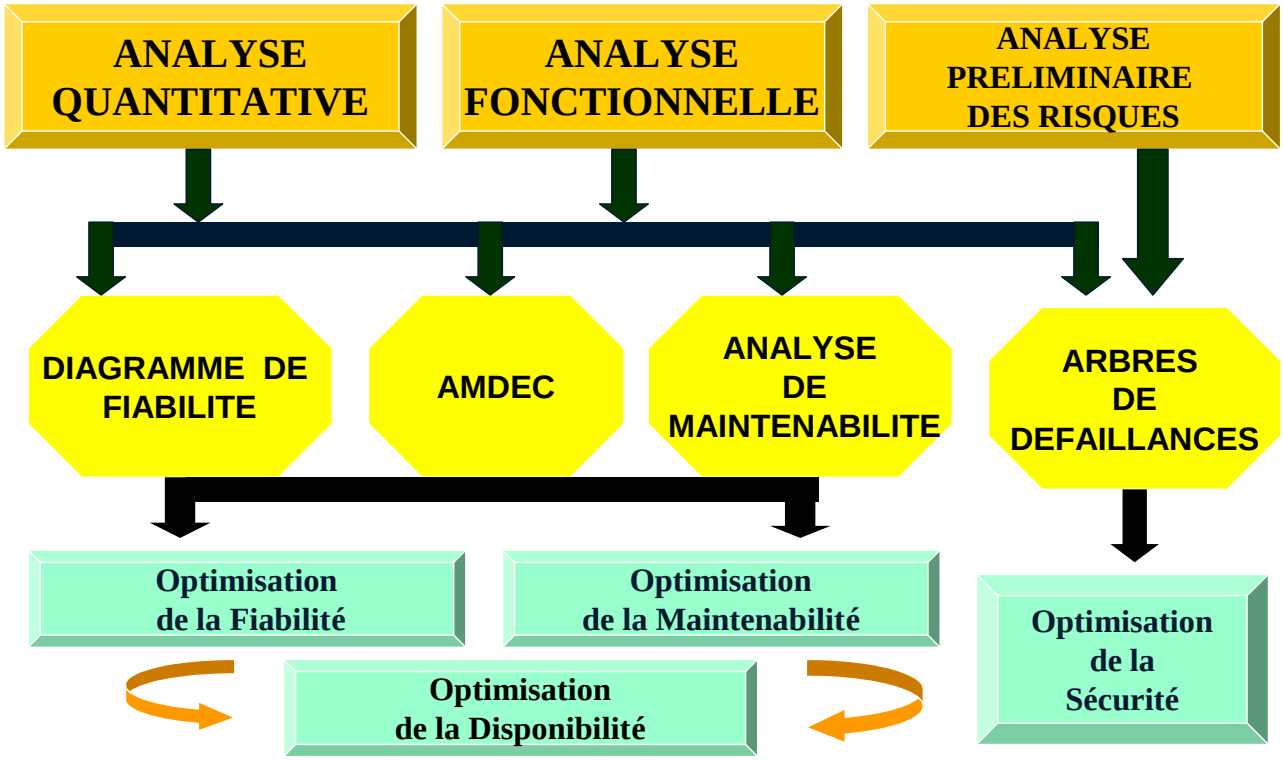
LA SURETE DE FONCTIONNEMENT

Le besoin de sûreté :

Les sociétés modernes sont caractérisées par une exigence croissante de sûreté pour les systèmes qui y participent. Cette exigence a pour origines :

- Une dimension humaine : la constatation d'un écart croissant entre la qualification requise pour utiliser un système et celle requise pour maîtriser la compréhension de son fonctionnement conduit à le concevoir de plus en plus sûr.
- Une dimension technico-économique : la complexité et l'interdépendance croissante des systèmes techniques engendrent des risques parfois catastrophiques en cas de défaillance :
  - risques sur les personnes ou sur l'environnement, de par le danger, d'un procédé des secteurs nucléaire ou chimique, du transport de matières dangereuses, etc.
  - risques économiques en cas d'arrêt de production, fatal au produit fabriqué ou aux équipements, en cas d'interruption de service de réseaux d'énergie ou d'informations, etc.
- Une dimension sociale : le niveau de sûreté perçu comme « admissible » est subjectif et évolutif, et fonction de l'évolution des sociétés et des mentalités. Un regard historique, sur l'apparition puis l'évolution de la législation du travail, ou sur l'évolution des connaissances relatives à la disponibilité des systèmes complexes, est éloquent. La comparaison avec la situation de pays encore en voie de développement ne fait que renforcer ce caractère subjectif.

II – OUTILS DE LA SDF :



III – LES ARBRES DE DEFAILLANCE :

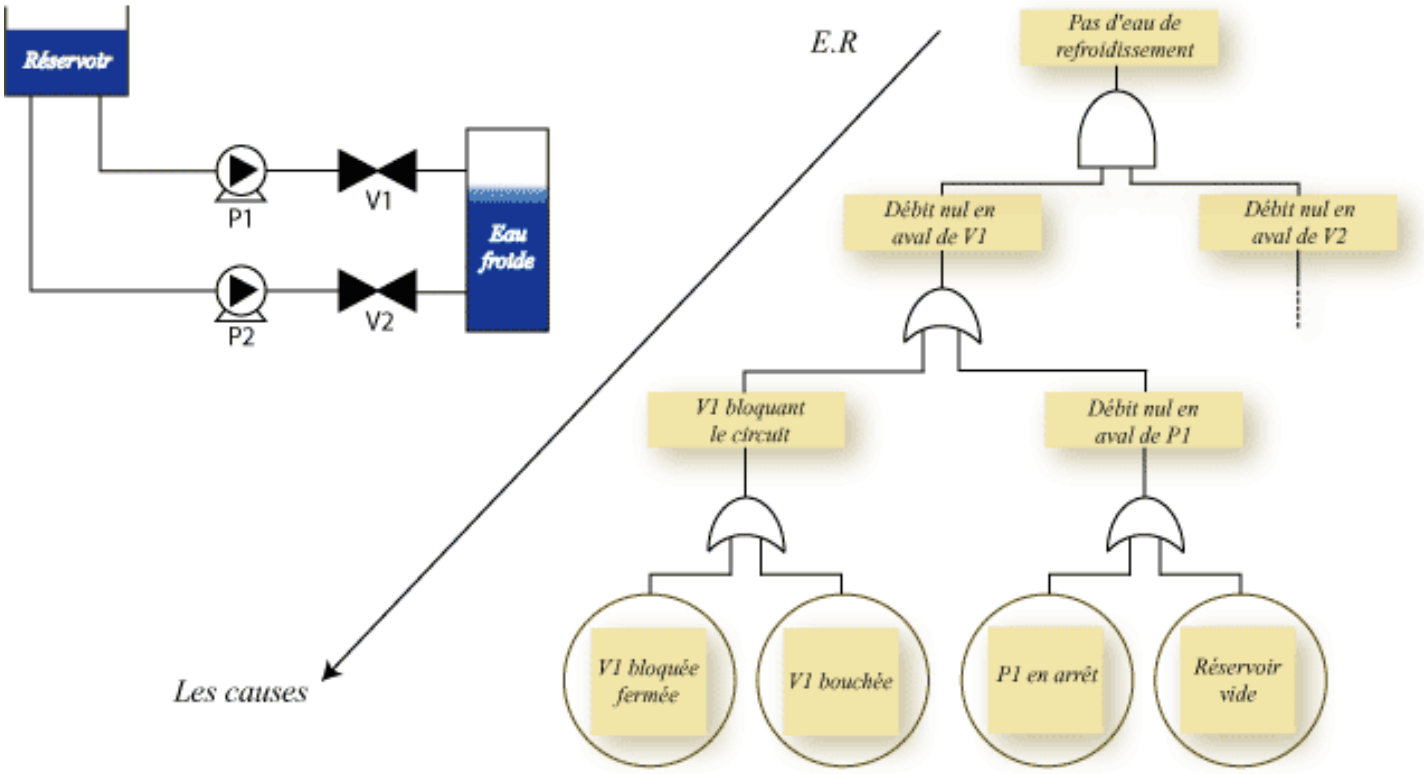
31 – Définition :

Les arbres de défaillances modélisent l'ensemble des combinaisons d'événements, qui conduisent à un événement redouté.

L'arbre de défaillance est une représentation graphique de type arbre généalogique. Il représente une démarche d'analyse d'événement. L'arbre de défaillance est construit en recherchant l'ensemble des événements élémentaires, ou les combinaisons d'événements, qui conduisent à un Evénement Redouté (ER).

L'objectif est de suivre une logique déductive en partant d'un Evénement Redouté pour déterminer de manière exhaustive l'ensemble de ses causes jusqu'aux plus élémentaires.

Exemple :



32 – Objectifs :

Les objectifs des arbres de défaillance sont résumés en quatre points :

- La recherche des **événements** élémentaires, ou leurs combinaisons qui **conduisent à un ER**.
- La représentation graphique **des liaisons entre les événements**. Il existe une représentation de **la logique de défaillance du système** pour chaque ER ; ce qui implique qu'il y aura autant d'arbres de défaillances à construire que d'ER retenus.
- **L'analyse qualitative** qui permet de déterminer les faiblesses du système. Elle est faite dans le but de proposer des modifications afin d'améliorer la fiabilité du système. La recherche des éléments les plus critiques est faite en déterminant les chemins qui conduisent à un ER. Ces chemins critiques représentent des scénarios qui sont analysés en fonction des différentes modifications qu'il est possible d'apporter au système. L'analyse des scénarios qui conduisent à un ER est faite à partir des arbres de défaillances. Il est alors possible de disposer des **"barrières de sécurité"** pour éviter les incidents.
- Enfin, il est possible d'**évaluer la probabilité** d'apparition de l'ER connaissant la probabilité des événements élémentaires : c'est l'**analyse quantitative** qui permet de déterminer les caractéristiques de fiabilité du système étudié. L'objectif est en particulier de définir la probabilité d'occurrence des divers événements analysés. Les calculs reposent sur les équations logiques tirées de la structure de l'arbre de défaillance et des probabilités d'occurrence des événements élémentaires.

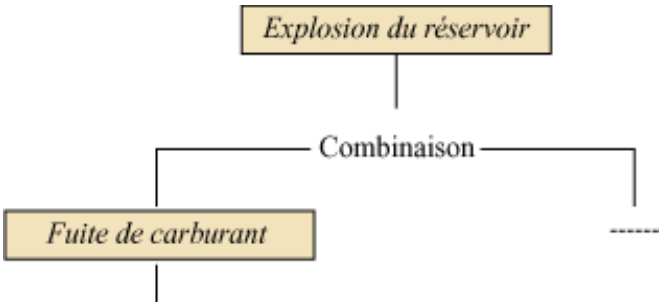
33 – Evènements :

Événement redouté : l'événement redouté est l'événement indésirable pour lequel on fait l'étude de toutes les causes qui y conduisent. Cet événement est unique pour un arbre de défaillance et se trouve au "sommet" de l'arbre. Avant de commencer la décomposition qui permet d'explorer toutes les combinaisons d'événements conduisant à l'événement redouté, il faut défini avec précision cet événement ainsi que le contexte de son apparition.

L'événement redouté est représenté par un rectangle au sommet de l'arbre comme par exemple l'explosion du réservoir de carburant d'un véhicule :

Événements intermédiaires : les événements intermédiaires sont des événements à définir comme l'événement redouté. La différence avec l'événement redouté est qu'ils sont des causes pour d'autres événements. Par exemple c'est la combinaison d'événements intermédiaires qui conduit à l'événement redouté.

Un événement intermédiaire est représenté par un rectangle comme l'événement redouté. Dans notre exemple c'est la combinaison d'une fuite de carburant avec d'autres événements qui est susceptible de provoquer l'explosion du réservoir :



Événements élémentaires : les événements élémentaires sont des événements correspondants au niveau le plus détaillé de l'analyse du système. Dans un arbre de défaillance, ils représentent les défaillances des composants qui constituent le système étudié. Pour fixer le niveau de détail de l'étude, on considère en général que les événements élémentaires coïncident avec la défaillance des composants qui sont réparables ou interchangeables.

Les événements élémentaires sont représentés par des cercles. Dans notre exemple c'est la combinaison des défaillances « Joint percé » et « Vanne bloquée ouverte » qui provoque une fuite de carburant :

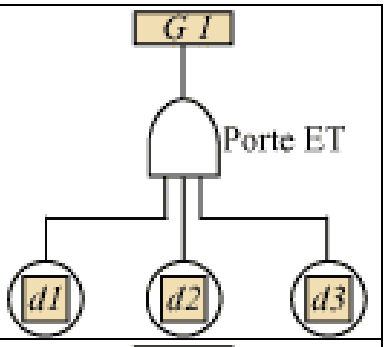
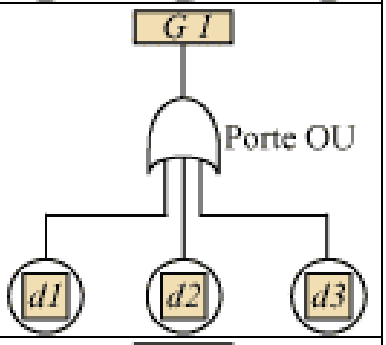
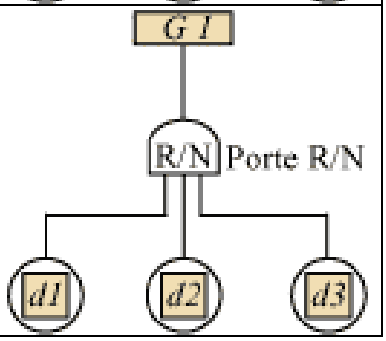
Résumé de la symbolique des événements :

Il existe d'autres types d'événements définis par la norme. Leurs symboles ainsi que leurs significations sont répertoriés dans le tableau suivant :

Symbole	Nom	Signification
	Rectangle	Evénement redouté ou événement intermédiaire
	Cercle	Evénement intermédiaire
	Losange	Evénement élémentaire non développé
	Double losange	Evénement élémentaire dont le développement est à faire ultérieurement
	Maison	Evénement de base survenant normalement pour le fonctionnement du système

34 – Portes logiques :

Les portes logiques permettent de représenter la combinaison logique des événements intermédiaires qui sont à l'origine de l'événement décomposé.

Porte ET : L'événement G1 ne se produit que si les événements élémentaires d1, d2 et d3 existent simultanément	
Porte OU : L'événement G1 se produit de manière indépendante si l'un ou l'autre des événements élémentaires d1, d2 ou d3 existe.	
Porte R/N : Si R=2 et N=3 alors il suffit que deux des événements élémentaires d1, d2, d3 soient présents pour que l'événement G1 se réalise.	

35 – Transferts de sous arbres :

Il existe pour les arbres de défaillances une symbolique normalisée qui permet de faire référence à des parties de l'arbre qui se répètent de manière *identique** ou de manière *semblable*[+] pour éviter de les redéfinir. L'objectif est de réduire la taille du graphique. Le tableau suivant présente les symboles ainsi que les significations qui sont utilisés.

Symbole	Nom	Signification
	Triangle	La partie de l'arbre qui suit le premier symbole se retrouve identique, sans être répétée, à l'endroit indiqué par le second symbole.
	Triangle inversé	La partie de l'arbre qui suit le premier symbole se retrouve semblable mais non identique à l'endroit indiqué par le second symbole.

* *Identique : même structure, même événements.*

[+] *Semblable : Même structure mais avec des événements différents.*

36 – Construction d'un arbre de défaillance :

La construction de l'arbre de défaillance repose sur l'étude des événements entraînant un événement redouté. Les 2 étapes suivantes sont réalisées successivement en partant de l'ER et en allant vers les événements élémentaires.

1) Dans un 1er temps, définir l'événement redouté (l'événement intermédiaire, ou l'événement élémentaire) analysé en spécifiant précisément ce qu'ils représentent et dans quel contexte il peut apparaître.
2) Puis dans un 2ème temps, représenter graphiquement les relations de cause à effet par des portes logiques (ET, OU) qui permettent de spécifier le type de combinaison entre les événements intermédiaires qui conduisent à l'événement analysé.

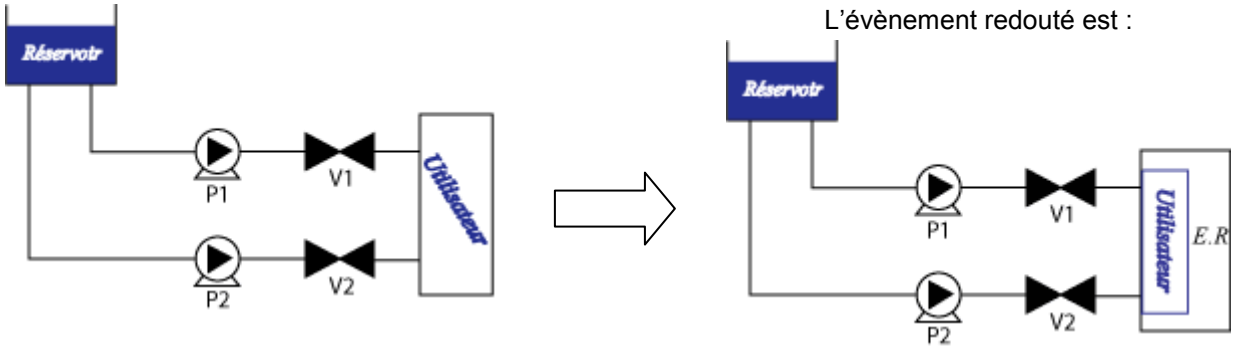
Pour pouvoir appliquer cette méthode il est nécessaire de :

- Vérifier que le système a un fonctionnement cohérent.
- Connaître la décomposition fonctionnelle du système.
- Définir les limites du système (le degré de finesse de l'étude dépend des objectifs).
- Connaître la mission du système et son environnement pour déterminer le ou les événements redoutés qu'il est nécessaire d'étudier.
- Connaître les modes de défaillance des composants. C'est par exemple en s'appuyant sur une analyse de type AMDEC que les branches de l'arbre pourront être construites.

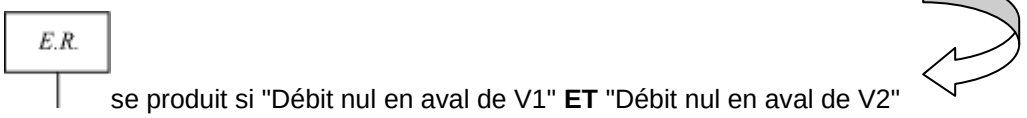
Règles de construction

- expliciter les faits et noter comment et quand ils se produisent
  - pour l'événement redouté
  - pour les événements intermédiaires
- effectuer un classement des événements :
  - événement élémentaire représentant la défaillance d'un composant
    - défaillance première
    - défaillance de commande
  - événements intermédiaires provenant d'une défaillance de composant. C'est par exemple un mode de défaillance.
  - événements intermédiaires provenant du système indépendamment du composant. C'est par exemple une configuration particulière.
- rechercher les « causes immédiates » de l'apparition de chaque événement intermédiaire afin d'éviter l'oubli d'une branche
- éviter les connexions directes entre portes : elles sont en général dues à une mauvaise compréhension du système ou à une analyse trop superficielle.
- supprimer les incohérences comme par exemple : un événement qui est à la fois cause et conséquence d'un autre événement.

Exemple de construction :

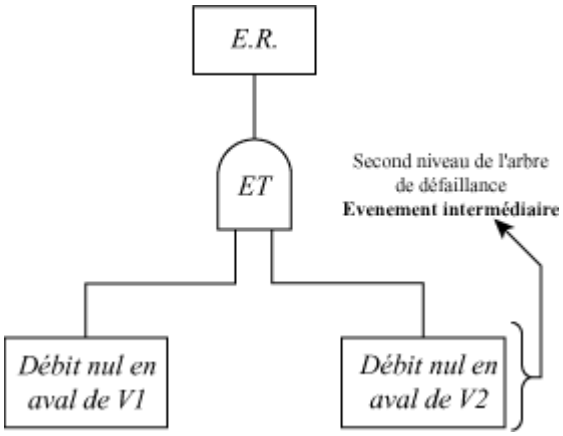


ER : le système utilisateur est non alimenté

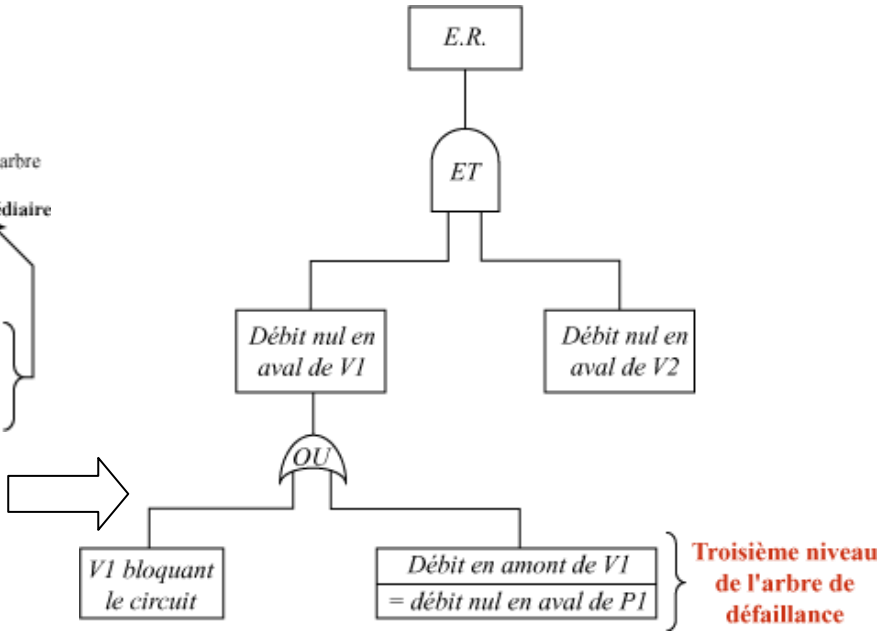


LA SURETE DE FONCTIONNEMENT

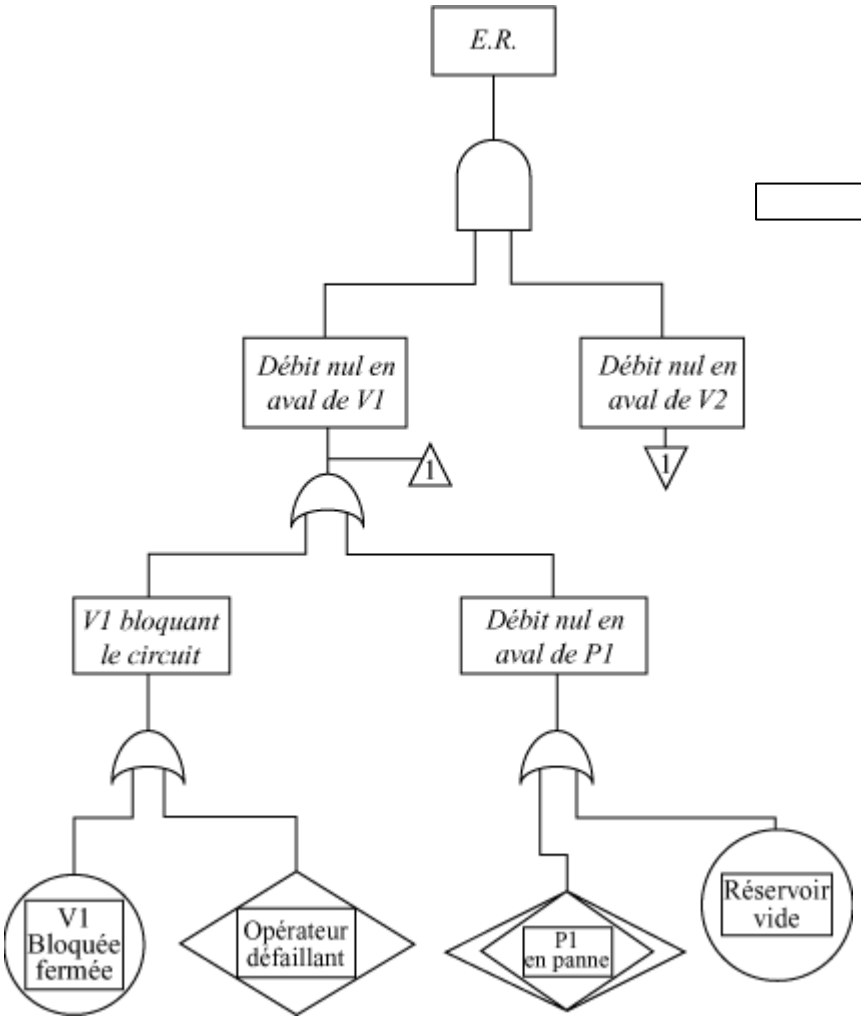
Le début de l'arbre est le suivant :



La suite de l'arbre est alors :

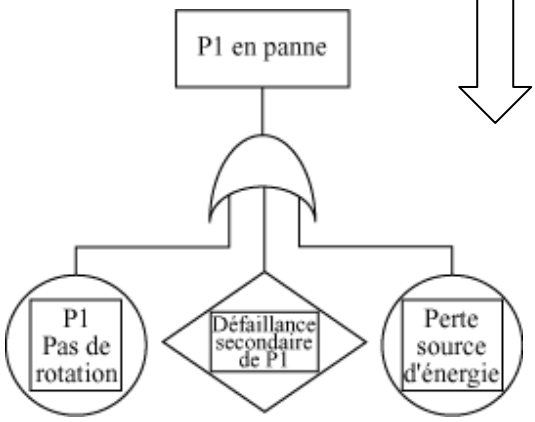


On en arrive alors à l'arbre de défaillance complet :



<u>1 - Défaillance première</u> : blocage de la vanne en position fermée (un vieillissement) ➔ événement élémentaire "**V1 bloquée fermée**".

<u>2 – Défaillance de commande</u> : Puisque la vanne est manuelle, cette défaillance serait due à l'opérateur qui n'aurait pas ou mal effectué l'ouverture de V1 ➔ événement élémentaire non développé "**opérateur défaillant**".



<u>Défaillance première</u> : pas de rotation de la pompe ➔ événement élémentaire "P1 - Pas de rotation"

<u>Défaillance secondaire</u> : défaillance due à une cause extérieure ou à une utilisation particulière. Ici un corps étranger qui obstrue la pompe ➔ événement élémentaire non développé "Défaillance secondaire de P1"

<u>Défaillance de commande</u> : puisque la pompe est électrique, cette défaillance serait due à la perte de la source d'énergie ➔ événement élémentaire "Perte source d'énergie"

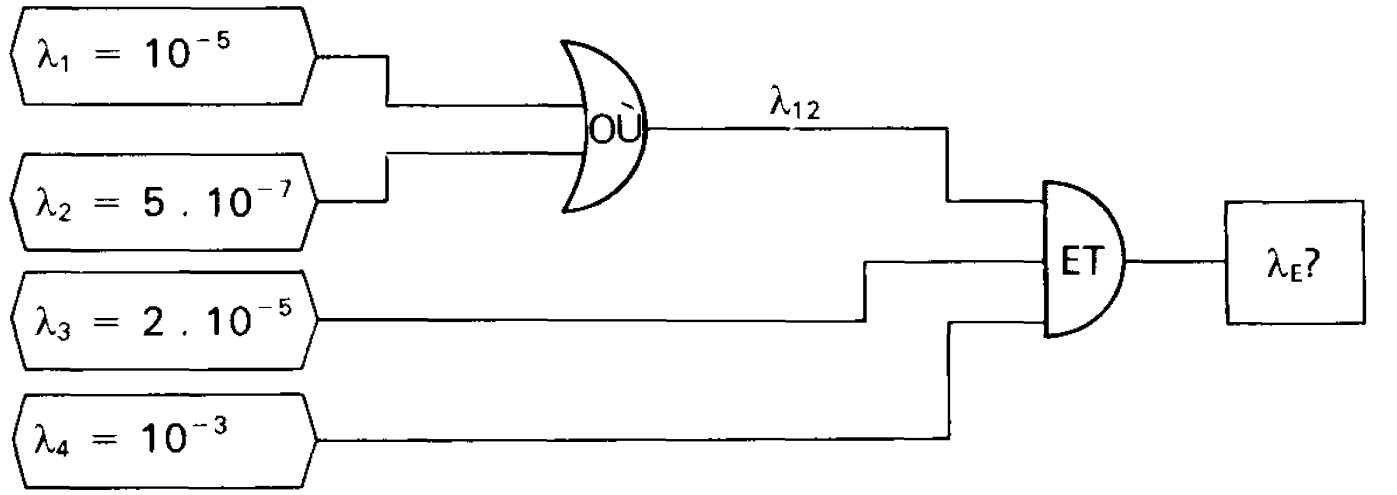
37 – Analyse quantitative des arbres de défaillance :

Hypothèses de quantification :

- On utilisera le taux de défaillance λ estimé de chaque composant élémentaire, bien entendu en le supposant constant. Cependant, il est possible d'intégrer la notion de temps dans l'arbre de défaillance dans le cas des systèmes réparables.
- Systèmes non réparables : pas d'intervention de maintenance possible en cours de mission, une défaillance d'un composant subsiste jusqu'à la fin de la mission.
- Systèmes réparables : intervention possible, la défaillance est corrigée en cours de mission.

Porte ET : $\lambda = \prod_{i=1}^{n} \lambda_i$	Porte OU : $\lambda = \sum_{i01}^{n} \lambda_i$

Exemples :



Quatre composants élémentaires.

$$\lambda_{12} = \lambda_1 + \lambda_2$$
$$\lambda_{12} = 10^{-5} + 5 . 10^{-7} = 105 . 10^{-7}$$
$$\lambda_{12} \simeq 10^{-5}$$

La puissance la plus faible est souvent négligée.

$$\lambda_E = \lambda_{12} . \lambda_3 . \lambda_4$$
$$\lambda_E = 10^{-5} . 2 . 10^{-5} . 10^{-3}$$
$$\lambda_E = 2 . 10^{-13} = \varepsilon$$

Remarque :

Dans le cas de systèmes réparables, l'arbre de défaillance est dépendant du temps. Il faut alors prendre en compte « μ », taux de réparation de chaque composant, caractérisant la maintenabilité du système analysé. La démarche, de forme semblable, aboutit à caractériser la disponibilité du système.

38 – Intérêt de la résolution des arbres de défaillances :

La résolution permet, connaissant les λ_i des composants, de prévoir le λ résultant de l'ensemble et de déceler les branches fragiles de l'arbre qui affectent le λ résultant.

Il devient donc possible :

- au niveau de la conception, de déceler les organes dont il faut améliorer la fiabilité, ou qu'il faut mettre en redondance.
- au niveau de la logistique, de prévoir les organes fragiles à approvisionner.
- au niveau du diagnostic, d'orienter le diagnostic vers les composants à prendre en compte de façon prioritaire dans les tests et les logigrammes de dépannage.

Ces prévisions étant possibles sans résultats opérationnels directs du système concerné.

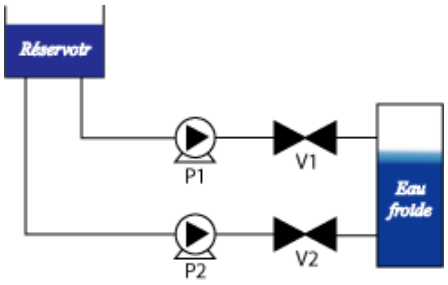
IV – LES DIAGRAMMES DE FIABILITE :

41 – Définition :

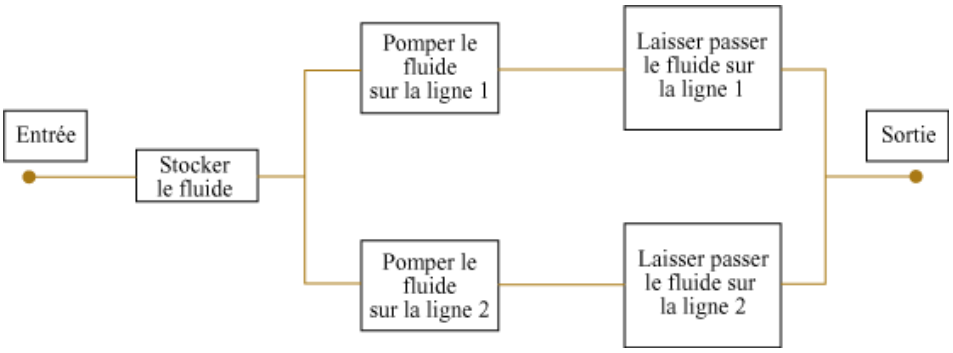
Les diagrammes de fiabilité modélisent l'ensemble des missions à réaliser pour garantir le succès de la mission du système.

Le diagramme de défaillance est une représentation graphique sous forme de boîtes ou de blocs. Il représente une démarche d'analyse par décomposition fonctionnelle du système en sous fonction ou mission. Le diagramme de fiabilité est construit en recherchant la mission de chaque sous ensemble qui permet d'atteindre la mission globale du système, les boîtes peuvent représenter des fonctions ou des composants.

Exemple :



Représentation de l'enchaînement des missions à réaliser :



42 – Objectifs :

Un diagramme de fiabilité est un modèle qui permet de représenter le comportement d'un système sous une vue fonctionnelle. Cette modélisation ne permet pas de prendre en compte les réparations des composants. Cette modélisation est donc utilisée uniquement pour l'analyse de la fiabilité des systèmes.

La modélisation repose sur la définition des missions ou des fonctions de chaque constituant du système. Le diagramme de fiabilité décrit les liens entre les composants. L'objectif est de dissocier toutes les opérations à réaliser pour aboutir au succès de la mission du système. Le diagramme de fiabilité donne alors une représentation graphique facile à interpréter et qui permet des analyses de fiabilité.

D'un point de vue qualitative, l'analyse permet de déterminer les faiblesses du système. Elle est faite dans le but de proposer des modifications afin d'améliorer la fiabilité du système. La recherche des éléments les plus critiques est faite en déterminant les chemins qui conduisent à la réussite de la mission du système et la recherche des composants apparaissant dans le plus grand nombre de ces chemins. L'analyse des scénarios qui conduisent à l'échec de la mission est alors possible ; l'objectif est de disposer des **"barrières de sécurité"** pour éviter les incidents.

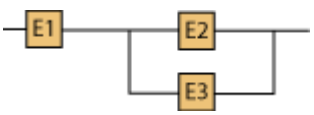
Enfin, il est possible d'évaluer la probabilité de réussite de la mission connaissant la probabilité de sucés des sous missions des constituants. Cette analyse quantitative a pour objectif en particulier de définir la probabilité de bon fonctionnement du système. Les calculs reposent sur les probabilités de réussite des missions des constituants du système.

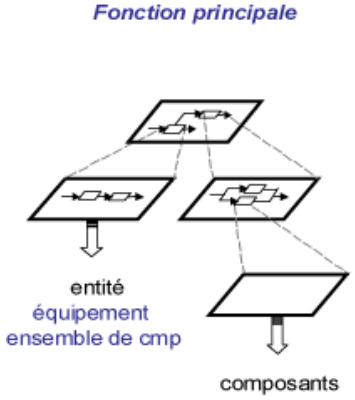
43 – Construction du diagramme de fiabilité :

La méthode d'analyse par diagramme de fiabilité repose sur une décomposition du système en sous-systèmes ; chaque entité étant modélisée par des blocs :

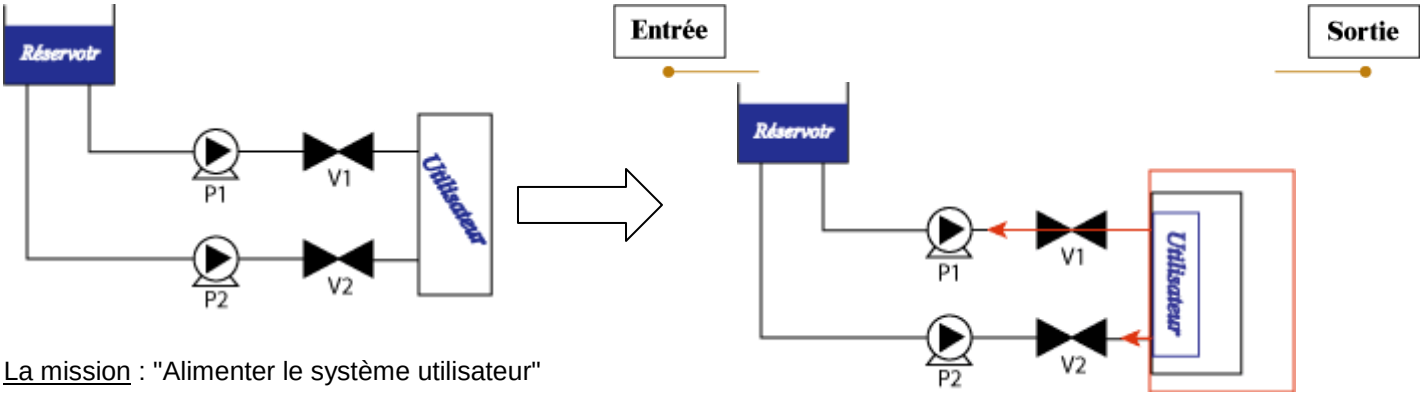
- Les sous-systèmes
- Les fonctions
- Les composants

Puis une recherche des liens entre les blocs est faite :



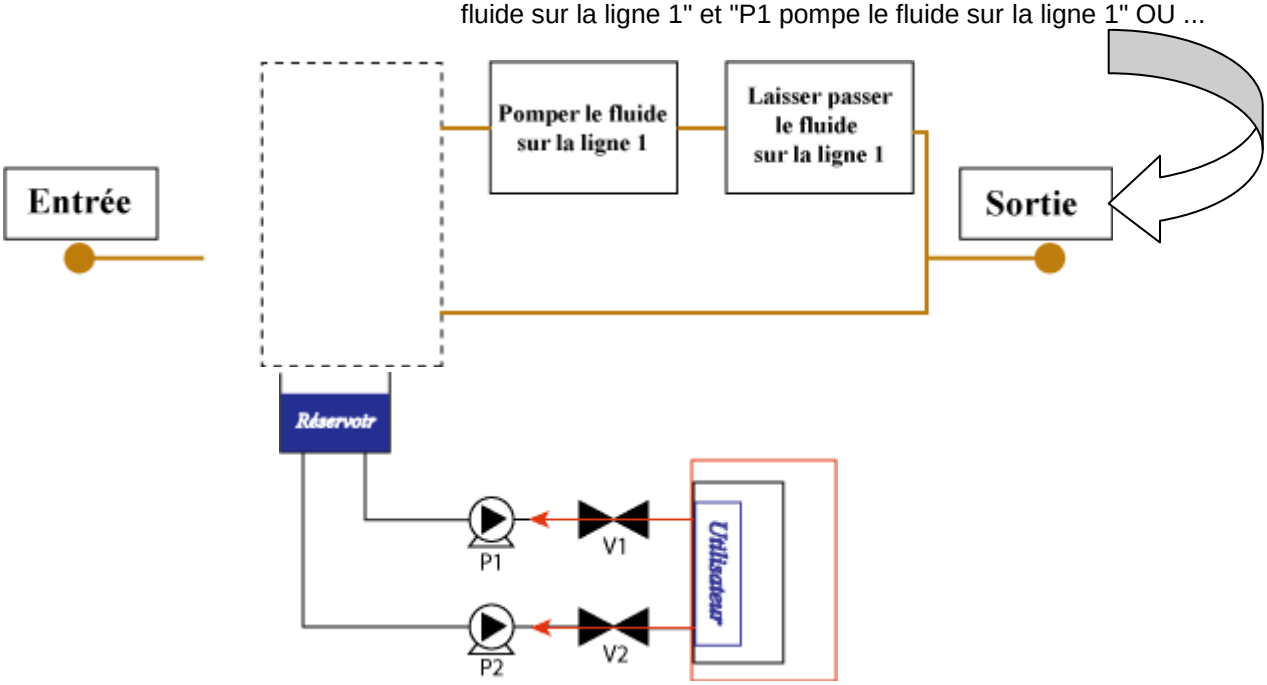


LA SURETE DE FONCTIONNEMENT

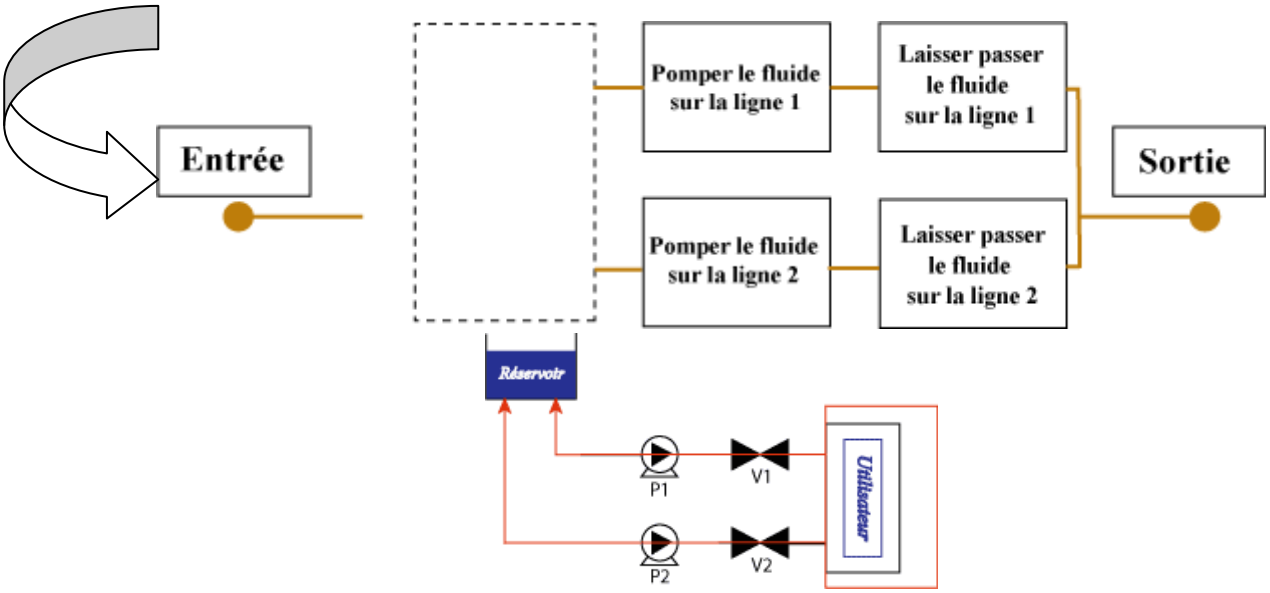


La mission : "Alimenter le système utilisateur"

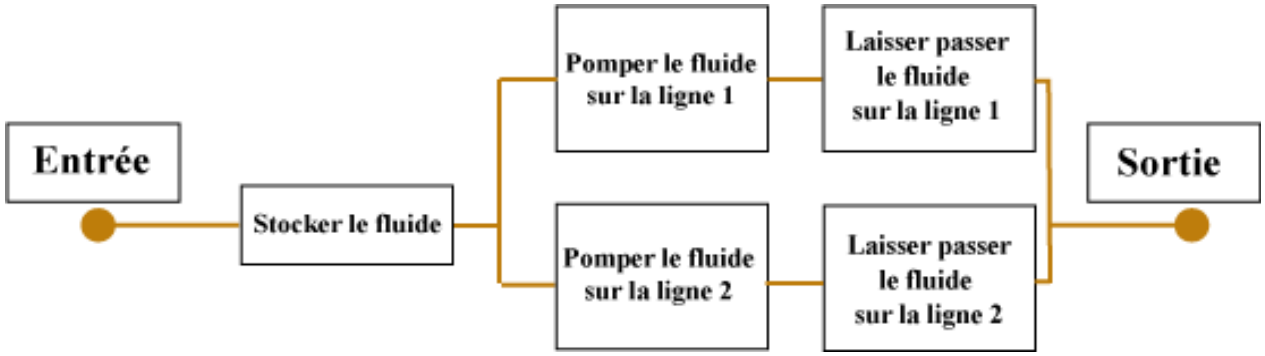
Pour la réussite de la mission, il faut que : "V1 laisse passer le fluide sur la ligne 1" et "P1 pompe le fluide sur la ligne 1" OU ...



Pour la réussite de la mission, il faut que : ("V1 laisse passer le fluide sur la ligne 1" et "P1 pompe le fluide sur la ligne 1" OU "V2 laisse passer le fluide sur la ligne 2" et "P2 pompe le fluide sur la ligne 2») ET ...

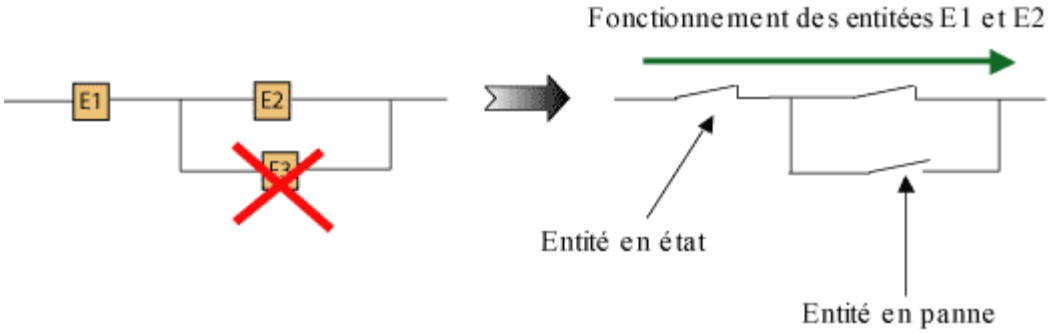


ARBRE DE FIABILITE COMPLET



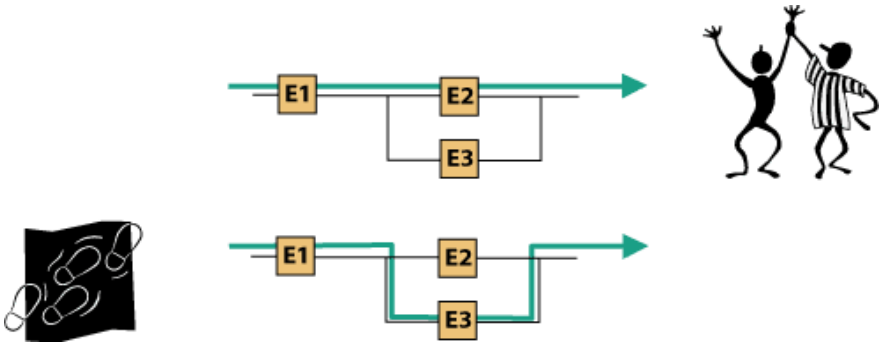
44 – Liens ou chemins de succès :

Un bloc est considéré comme un **interrupteur fermé** lorsque l'entité est en état de fonctionnement ou un **interrupteur ouvert** lorsque l'entité est en état de panne. Si le "signal" qui entre dans le diagramme en ressort, le système est déclaré en état de fonctionnement et la mission est réussie, sinon le système est en panne.



Un **Lien** ou **chemin de succès** est un ensemble d'entités dont le fonctionnement assure le succès de la mission du système. Un **chemin de succès minimal** est une des plus petites combinaisons d'entités qui lorsqu'elles sont en fonction permettent d'assurer la fonction requise pour le système.

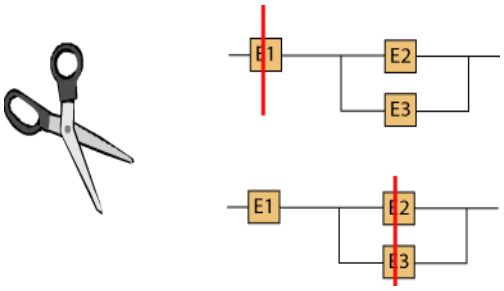
Exemple : dans le système représenté par ce diagramme de fiabilité, il existe deux chemins de succès minimal :



45 – Coupes :

Une **coupe** est un ensemble de blocs ou d'entités qui conduit à la panne (ou à la non réussite de la mission du système) si ces blocs ne peuvent plus réaliser leurs fonctions (ex : défaillance de composant).

Une coupe est un ensemble d'entités qui apparaissent dans tous les chemins de succès. Si l'ensemble des entités d'une coupe est en panne alors aucun chemin de succès ne permet de conduire à la réussite de la mission du système. Une **coupe minimale** est la plus petite combinaison d'entités entraînant l'échec de la mission du système (elle ne contient aucune autre coupe).



46 – Diagrammes de fiabilité élémentaire :

Le diagramme série : La panne de l'un ou de l'autre des éléments entraîne la panne du système

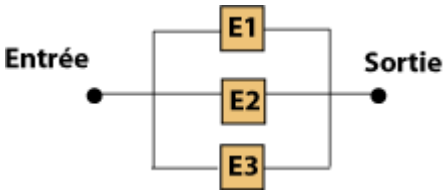
Chemins de succès ou liens minimaux : E1, E2

Coupes minimales :
E1
E2

Le diagramme parallèle (ou redondance active) : La panne de tous les éléments entraîne la panne du système. Si un seul des éléments fonctionne alors il conduit au fonctionnement du système.

Chemins de succès ou liens minimaux :
E1
E2
E3

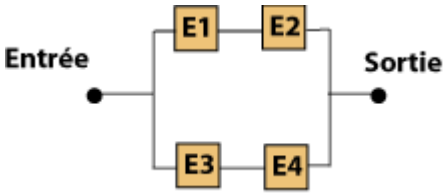
Coupes minimales :
E1, E2, E3



Le diagramme série / parallèle :

Chemins de succès ou liens minimaux :
E1, E2
E3, E4

Coupes minimales :
E1, E3 E2, E3
E1, E4 E2, E4



Le diagramme parallèle / série :

Chemins de succès ou liens minimaux :
E1, E2 E3, E2
E1, E4 E3, E4

Coupes minimales :
E1, E3
E2, E4