Sûreté de fonctionnement

Arbres des défaillances

Arbres des défaillances

Historique

- années 1960 aux Etats-Unis
- utilisés d'abord dans les domaines militaire et aéronautique, ensuite dans le nucléaire, aérospatiale, chimique, …

Contexte

- complexité croissante des systèmes
- combinaisons de défaillances multiples et nombreuses au sein des systèmes

Objectif

C'est une méthode d'analyse qui peut s'appliquer à plusieurs objectifs :

- aide à la détection des dysfonctionnements d'un système
- aide au calcul de fiabilité (vis-à-vis de l'événement non désiré) si on connaît les probabilités d'occurrence des événements de base
- aide à la conception de la maintenance
- aide à la détermination des causes d'accidents (sécurité safety) en vue de leur prévention

Principe

1. identification de l'événement indésirable (on dit aussi redouté)
2. rechercher toutes les combinaisons possibles d'événements entraînant la réalisation de l'événement non désiré
3. représenter graphiquement ces combinaisons au moyen d'une structure arborescente dont l'événement non désiré est la racine

Le processus de construction de l'arbre est déductif. Il est construit jusqu'à l'obtention des causes premières (événements de base) pouvant entraîner l'événement redouté. Ces événements de base doivent être indépendants et tels qu'on en connaisse la probabilité d'occurrence.

L'arbre des causes est constitué des combinaisons d'événements conduisant à l'événement indésirable.

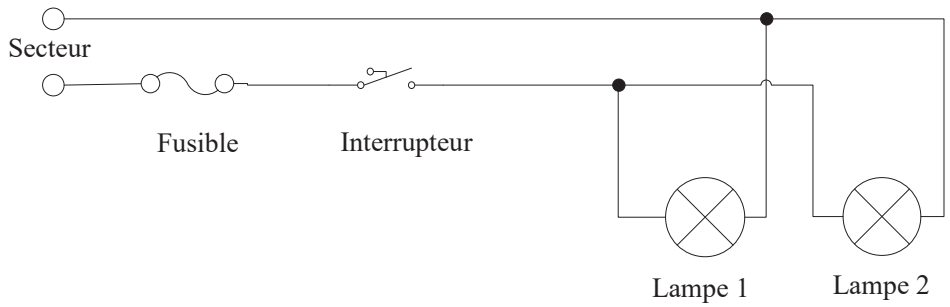
Les combinaisons sont construites à l'aide de portes logiques.

Chaque événement est représenté par un rectangle dans lequel est inscrite la description.

Principe

Exemple

Soit une installation d'éclairage d'une pièce :



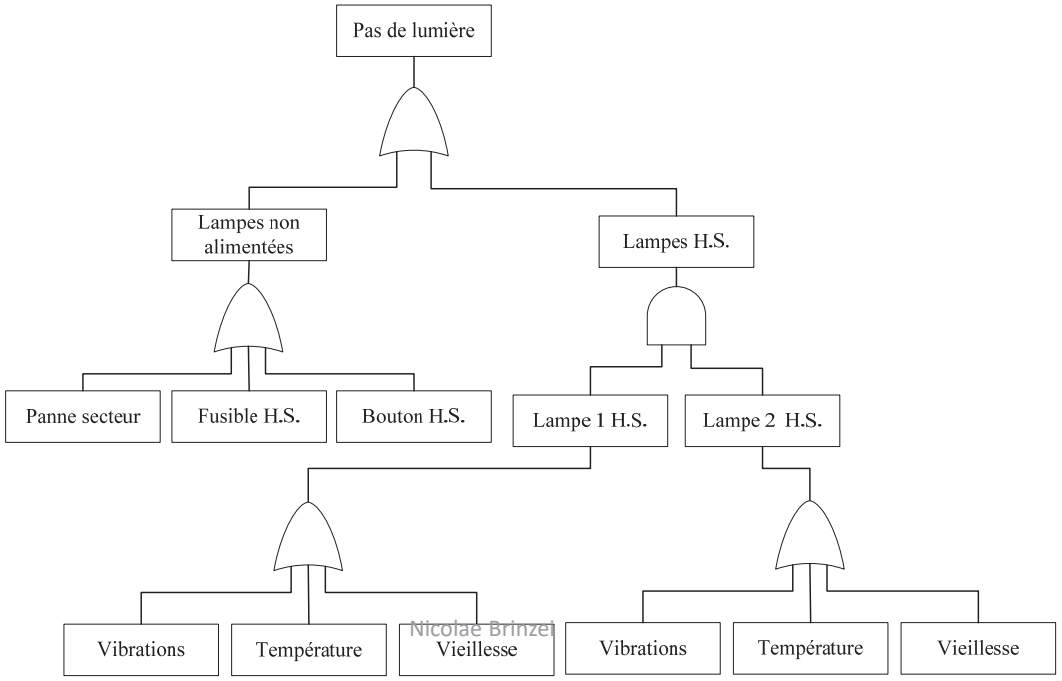
Evénement redouté : pas de lumière dans la pièce.

Causes directes : La lumière est fournie par les lampes. L'absence de lumière est donc due au fait que les lampes ne sont pas alimentées ou les lampes sont défectueuses.

Principe

Exemple

- Les lampes ne sont pas alimentées :
  Causes directes : panne secteur ou fusible H.S. ou interrupteur H.S.
- Les lampes sont défectueuses : lampe 1 HS et lampe 2 H.S.
  Causes directes : température trop élevée ou vibrations ou vieillesse.



Éléments de l'arbre des défaillances

Événement non désiré (ou indésirable ou redouté)

- pour l'analyse de fiabilité : le système tombe en panne (défaillance).
- pour l'étude de la sécurité: l'événement catastrophique à éviter.
- pour l'analyse de disponibilité : le système n'est pas disponible.

Cet événement doit être défini avec précision : pas trop général (⇒ inextricable) ni trop spécifique.

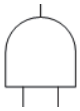
Pour déterminer l'événement non désiré, on peut effectuer une APR (Analyse Préliminaire des Risques).

Pour des systèmes à modes de marches différents ou à missions multiples, les analyses par AdD peuvent être multiples (une par mode ou par mission).

Éléments de l'arbre des défaillances

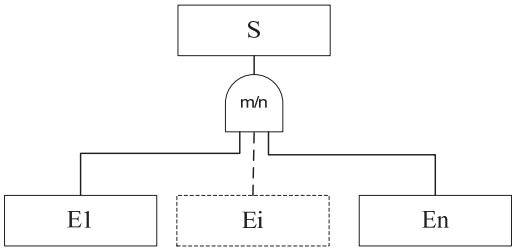
Opérateurs

• opérateur **ET**



• opérateur **OU**

• opérateur **combinaison de m/n**

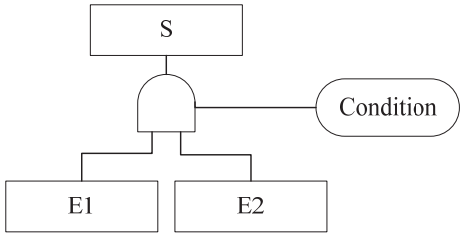


il y a occurrence de S si m événements sont présents sur n attendus

Éléments de l'arbre des défaillances

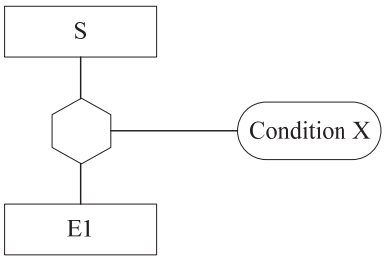
Opérateurs

• aux opérateur ET et OU on peut associer **une condition**



la condition peut être indépendante de E_1 et E_2, ou au contraire porter sur E_1, E_2. exemple E_1 avant E_2, etc.

• opérateur **condition** (opérateur **Si**)



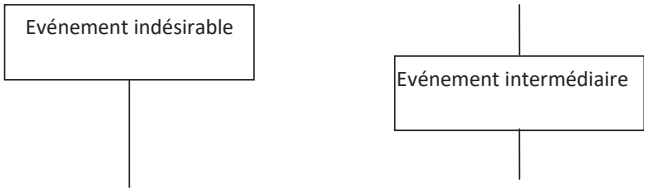
Si condition X :
- Alors :
  {occurrence de S} = {occurrence de E_1}
- Sinon :
  pas d'occurrence de S

Ce symbole est quelquefois aussi utilisé pour affecter un poids numérique à l'occurrence d'un événement. Dans ce cas, on pourra aussi utiliser des opérateurs arithmétiques.

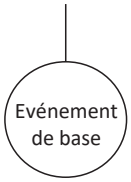
Éléments de l'arbre des défaillances

Événements

- **événements indésirable et intermédiaire** résultants de la combinaison d'autres événements par l'intermédiaire d'un opérateur



- **événement élémentaire (événement de base)**



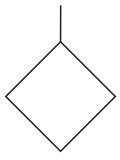
Pour un événement de base, il est inutile d'en chercher les causes, car on en connaît sa probabilité d'occurrence.

C'est par exemple :
- la défaillance première d'un composant
- une erreur humaine élémentaire
- un sous-système indisponible pour cause de maintenance préventive

Éléments de l'arbre des défaillances

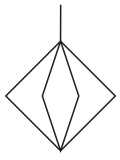
Événements

- **événement non élémentaire** mais dont on ne cherche pas les causes (on ne peut pas ou on ne veut pas le faire ; à développer par un sous-traitant)

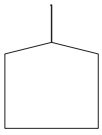


L'analyste ne peut pas poursuivre l'étude faute de connaissances suffisantes sur la structure du système.

- **événement non élémentaire mais on ne peut pas provisoirement le détailler** ; étude à poursuivre ultérieurement.

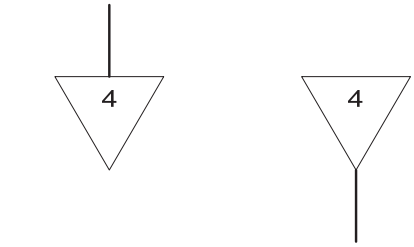


- **événement normal** (non élémentaire) lié au fonctionnement (pouvant avoir une incidence sur les conséquences des défaillances par exemple)



Éléments de l'arbre des défaillances

Transferts de sous arbres



vers le sous-arbre 4

début du sous-arbre 4

Élaboration de l'arbre des défaillances

Il n'y a pas de principe absolu. Cependant l'expérience a permis d'énoncer des règles élémentaires [Villemeur] permettant d'éviter certains écueils.

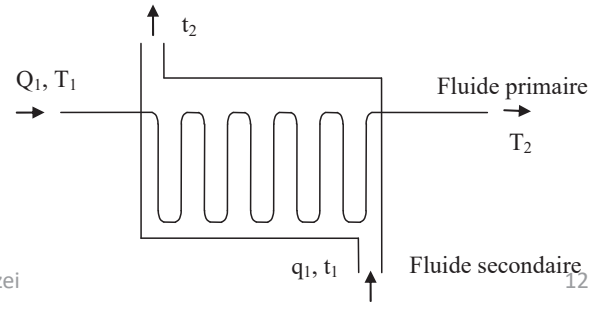
1. Recherche des causes Immédiates (think small), Nécessaires et Suffisantes

La recherche des causes INS doit être effectuée étape par étape de manière aussi rigoureuse que possible. Une importante aide à cette recherche peut être la considération des paramètres physiques et des lois qui régissent le comportement des composants des sous systèmes ou du système.

Exemple

L'échangeur thermique (refroidissement du fluide primaire):

- événement non désiré : **augmentation excessive de T2**



Élaboration de l'arbre des défaillances

Exemple

• causes INS ; après écriture des lois de comportement de l'échangeur :
- détermination des paramètres agissant sur T_2
ex : *baisse de q_1 ou augmentation de t_1*
augmentation de Q_1 ou de T_1
- analyse des défaillances de l'échangeur
ex : *fuite secondaire, fuite primaire*
communication entre les fluides (réactions physico-chimiques)

• on cherche ensuite les causes INS des variations de paramètres (externes à l'échangeur)
ex : pompes, vannes, pertes calorifiques, fuites, bouchons, etc.

Élaboration de l'arbre des défaillances

2. Classement des événements intermédiaires

La recherche des causes INS permet de déceler des événements intermédiaires. Ces événements peuvent être classés en :

a) événement de base

b) événement défaillance de composant

• ce peut être une **défaillance première** (dont la cause directe ou indirecte ne peut être la défaillance d'une autre entité) → remplacement. On peut rapprocher cette définition de la notion de cause interne. Pour les causes externes, on peut distinguer les deux cas suivants :

• ce peut être une **défaillance seconde** (dont la cause directe ou indirecte est la défaillance d'une autre entité et pour laquelle le composant n'a pas été dimensionné) → réparation.

• ce peut être une **défaillance de commande** (dont la cause directe ou indirecte est la défaillance d'une autre entité mais pour laquelle le composant est dimensionné) → pas de réparation.

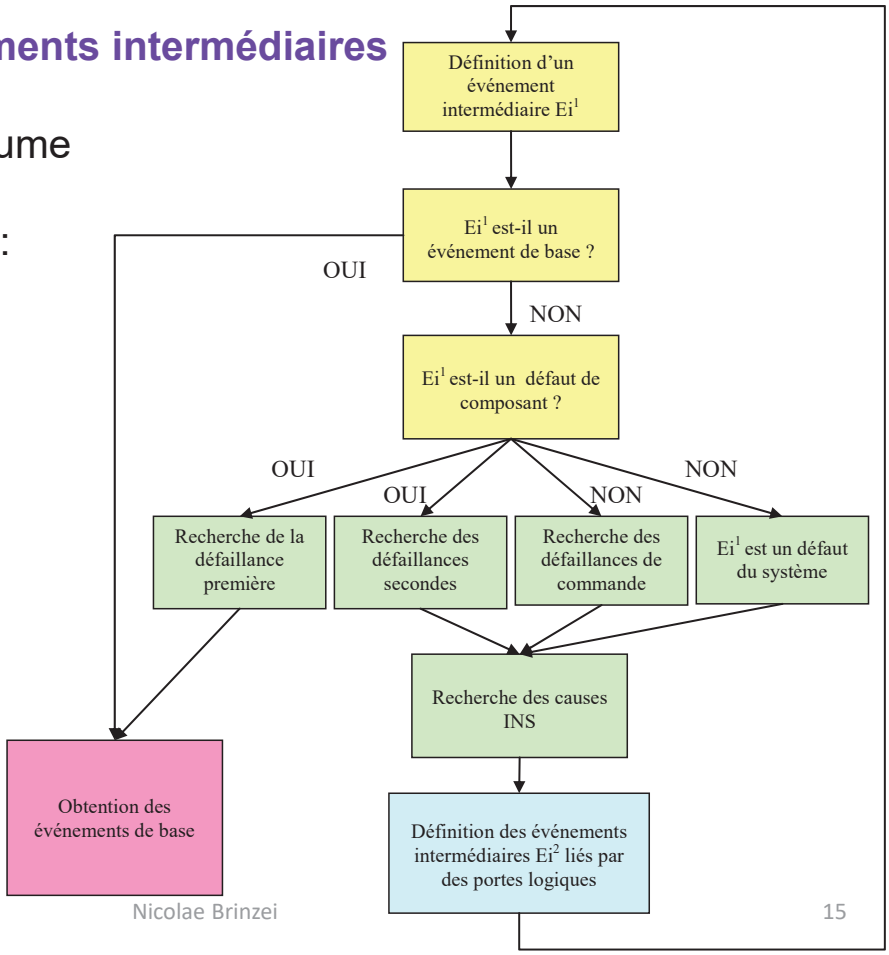
c) défaillance du système

C'est une défaillance non imputable à un seul composant ou à un seul événement ou à une combinaison des 2.

Élaboration de l'arbre des défaillances

2. Classement des événements intermédiaires

Le schéma suivant (d'après [VILLEMEUR]) résume le processus d'analyse des événements intermédiaires :



LORRAINE INP Ensem

Élaboration de l'arbre des défaillances

2. Classement des événements intermédiaires

Si la recherche des causes INS conduit à définir :

a) une défaillance première : on obtient **un événement de base**

b) une ou des défaillances secondes : la recherche de leurs causes INS conduit à définir **des événements intermédiaires** liés par des portes logiques

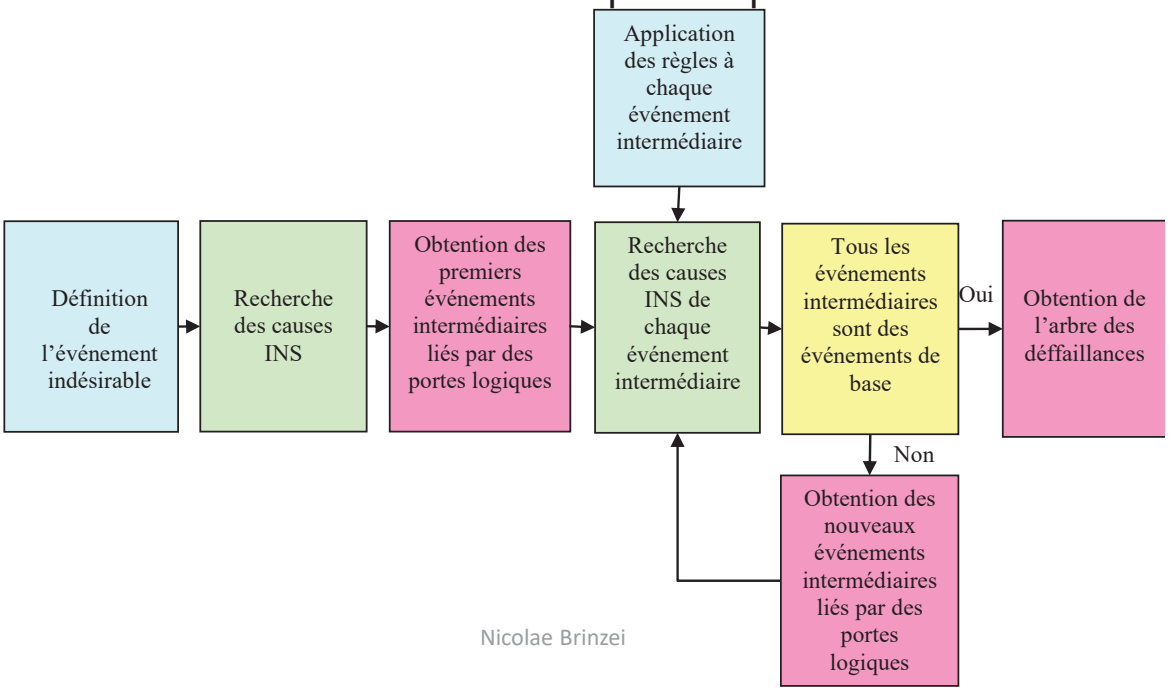
c) une ou des défaillances de commande : de même, la recherche de leurs causes INS conduit à définir **des événements intermédiaires** liés par des portes logiques

Élaboration de l'arbre des défaillances

3. Recherche des causes INS des événements intermédiaires jusqu'à l'obtention des événements de base

On répète la même procédure que précédemment jusqu'à ce que les événements causes soient identifiés comme événements de base.

La figure suivante résume l'ensemble des phases précédentes :



Élaboration de l'arbre des défaillances

4. Nécessité de réitérer la démarche

La démarche précédente doit être itérée pour deux raisons essentielles :

- la recherche des causes de certains événements entraîne souvent une recherche plus approfondie dans la connaissance du système impliquant souvent la redéfinition ou le rajout d'événements intermédiaires
- la remise en cause de certaines limites pouvant amener à redéfinir le niveau composant

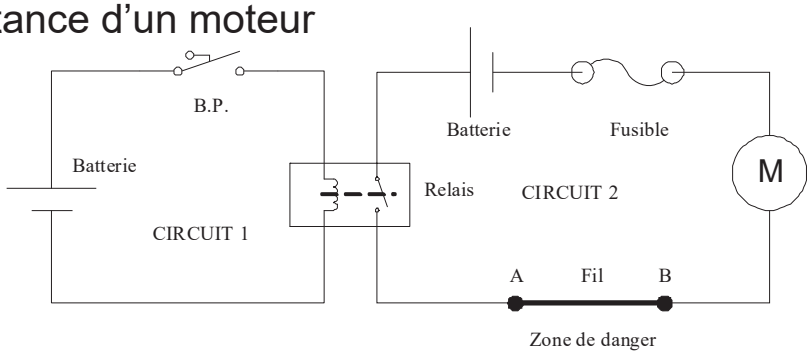
5. Autres règles

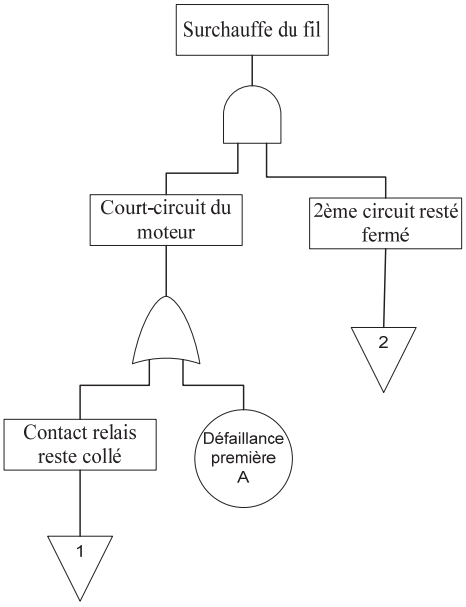
- compléter les portes : définir tous les événements d'entrée d'une porte avant d'entreprendre l'analyse de l'un d'entre eux
- pas de porte à porte : il doit toujours y avoir un événement décrit entre une sortie et une entrée
- les causes sont antérieures aux conséquences ; on évite ainsi des branches fictives ou parfois des boucles !
- il n'y a pas de miracle ; la propagation d'une défaillance ne peut être arrêtée par l'apparition d'une autre défaillance !

Élaboration de l'arbre des défaillances

Exemple extrait de [Villemeur]

Système de commande à distance d'un moteur





Evénement indésirable : surchauffe du fil AB

Suppose que la seule cause de l'augmentation du courant est le court circuit du moteur et que l'on n'a pas pu interrompre le circuit 2

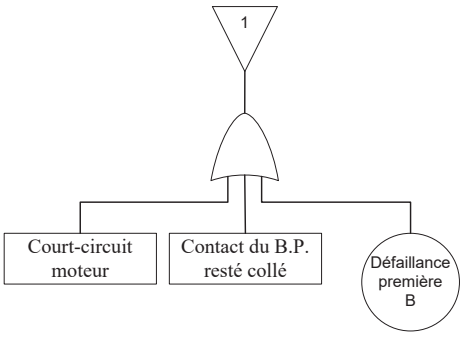
Etude de défaillance du composant moteur :

- défaillance première : le moteur est lui-même la cause de son court circuit (vieillesse)
- défaillance seconde : le contact du relais est resté fermé alors qu'il aurait dû être ouvert suite à la détection d'un fonctionnement anormal
- défaillance de commande : il n'y en a pas

LORRAINE INP Ensem

Élaboration de l'arbre des défaillances

Exemple extrait de [Villemeur]



Etude de défaillance du composant relais :

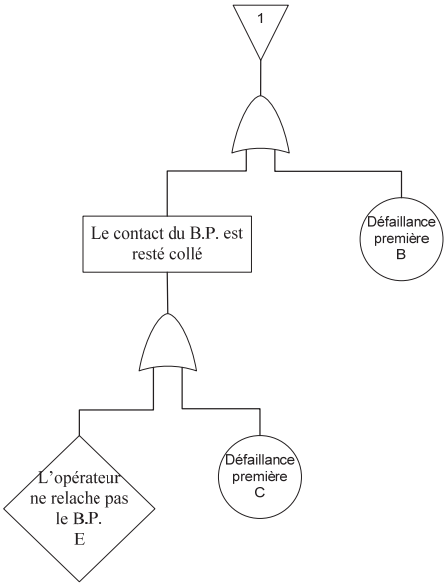
- défaillance première : blocage mécanique du relais
- défaillance seconde : le relais est resté collé par suite d'un courant trop élevé qui ne peut être dû qu'au court circuit du moteur
- défaillance de commande : le relais n'a pas pu être commandé parce que le bouton poussoir est resté collé

Remarque

Nous obtenons une incohérence due au non respect de la règle d'antériorité des causes sur les conséquences, la défaillance seconde n'est donc pas justifiée, il faut donc la supprimer.

Élaboration de l'arbre des défaillances

Exemple extrait de [Villemeur]



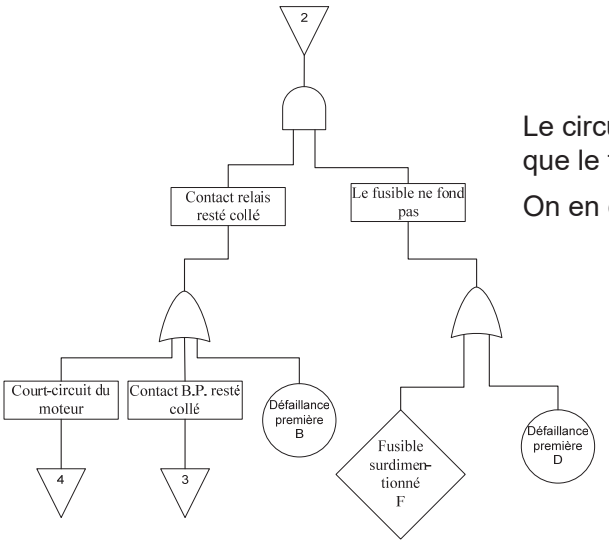
On peut ainsi continuer par la recherche des causes de défaillance du composant « bouton poussoir ».

On ne cherche pas pour le moment à détailler les causes de la défaillance de commande du contact du B.P. C'est une faute de l'opérateur.

Élaboration de l'arbre des défaillances

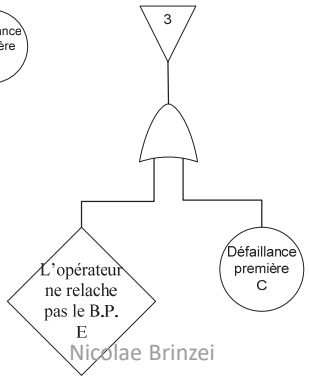
Exemple extrait de [Villemeur]

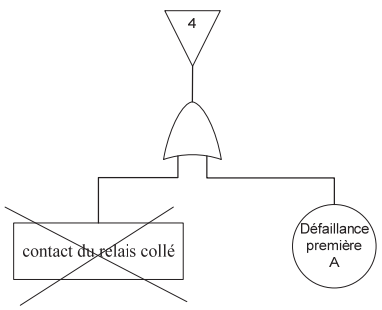
Etude des causes de défaillance du 2ème circuit :



Le circuit est resté fermé parce que le contact relais est resté collé et que le fusible n'a pas fondu.

On en cherche donc les causes





Il y a ici encore incohérence. Le collage du relais ne peut être la cause de lui-même.

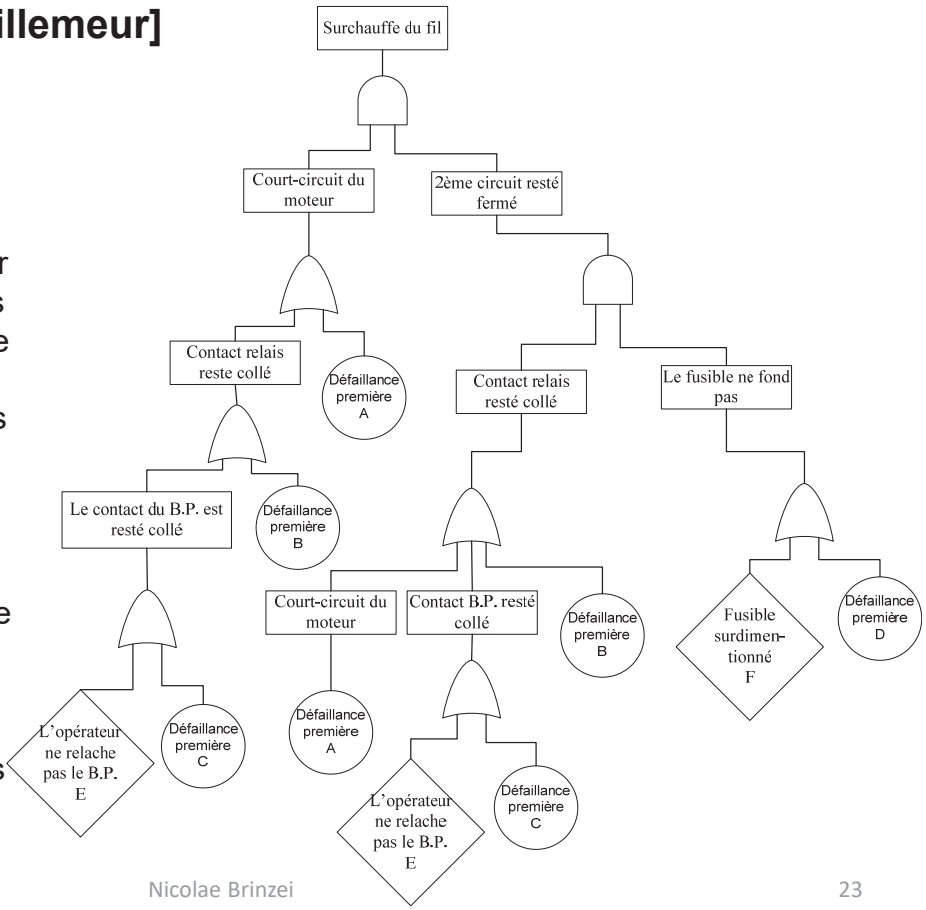
Élaboration de l'arbre des défaillances

Exemple extrait de [Villemeur]

Remarque

On a retenu seulement les défaillances essentielles, les plus probables. On ne cherche pas par exemple à déterminer des causes éventuelles dues à des défauts de conception des composants. On suppose qu'ils ont fait eux-mêmes l'objet de telles analyses, rendant ainsi très peu probables ce genre de défauts.

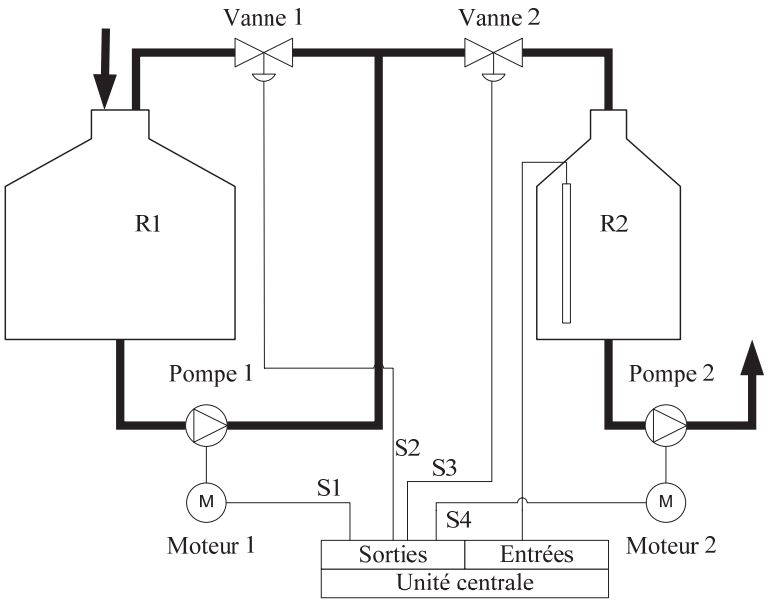
Une analyse type AMDE préalable peut grandement faciliter la construction de cet arbre en ce sens qu'elle aura répertorié les causes possibles des défaillances des différents constituants du système (retenir les modes de défaillances et leurs causes).



Élaboration de l'arbre des défaillances

Exercice

Dans une installation chimique deux réacteurs R1 et R2 sont mis en œuvre dans un cycle de production. Le réacteur R1 met en œuvre une opération de purification du produit initialement introduit, par recyclage au moyen de la pompe 1, vanne 1 ouverte et vanne 2 fermée. Pour transférer le produit lorsque la purification est suffisante, on ouvre la vanne 2 et on ferme la vanne 1. La réaction 2 nécessite le contrôle du niveau dans le réacteur qui ne doit pas excéder un maximum correspondant à un risque. Lorsque la réaction 2 est terminée, on vidange le réacteur 2 à l'aide de la pompe 2 (on suppose que son débit est toujours supérieur à celui de la pompe 1).



Élaboration de l'arbre des défaillances

Exercice

Le système de commande de l'installation est constitué d'une unité centrale programmable et d'unités d'entrées-sorties faisant interface avec les capteurs et actionneurs. On suppose pour la suite que le système de commande exécute deux tâches : la tâche de diagnostic et la tâche de commande qui élabore les sorties à partir des ordres reçus et des données issues des capteurs. L'utilisation d'un capteur analogique de niveau dans le réacteur 2 permet à la tâche de diagnostic d'identifier les défaillances du capteur par analyse périodique de la cohérence des informations délivrées. On peut alors décider une action de sécurité comme par exemple la vidange.

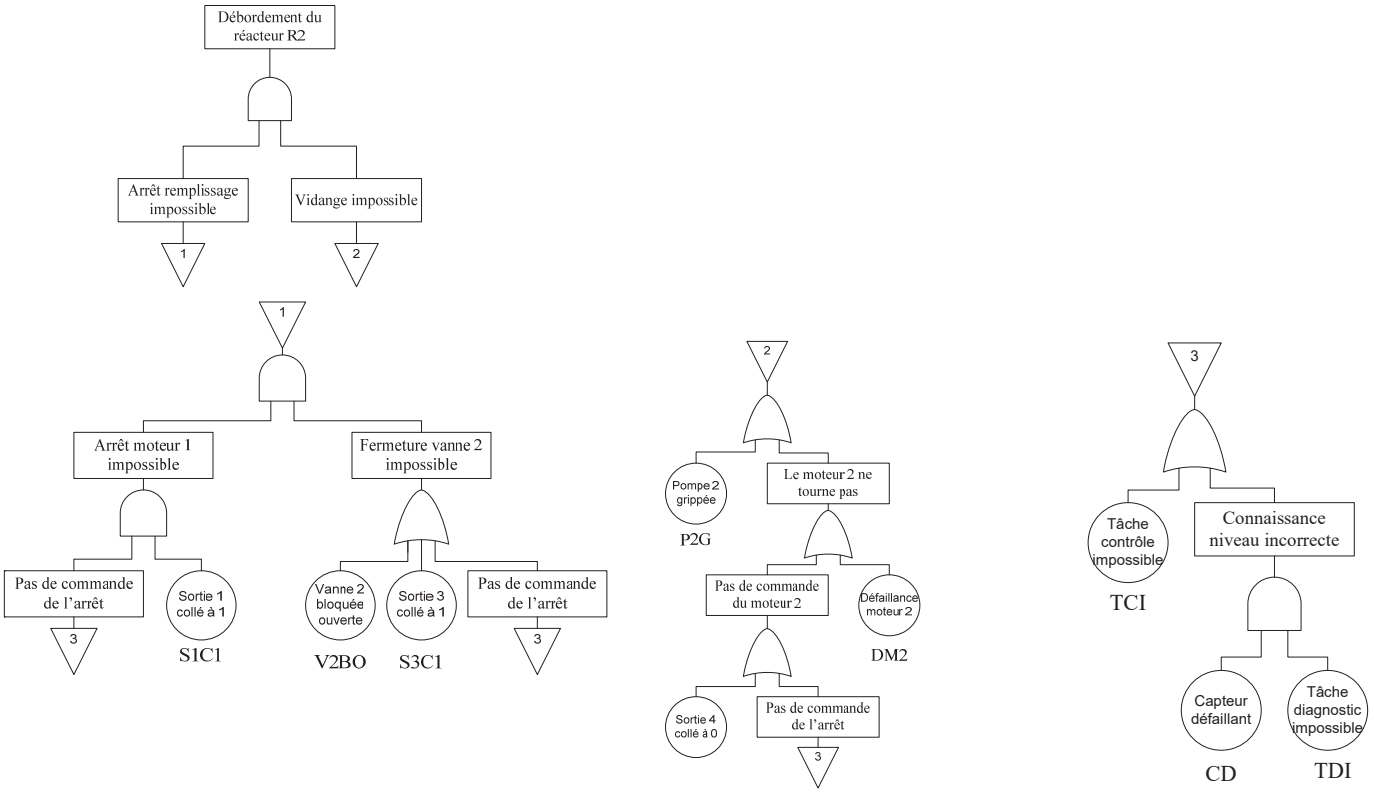
Les modes de défaillances retenus sont les suivants :

- capteurs de niveau : - valeur erronée
- pompes : - blocage
  - moteur H.S.
- vannes : - bloquée ouverte
  - bloquée fermée
- commande : - incapacité à exécuter une tache (diagnostic ou commande)
  - état d'une sortie bloqué

Toutes les autres défaillances sont considérées comme infiniment peu probables (rupture des canalisations, des câbles électriques, ...).

Élaboration de l'arbre des défaillances

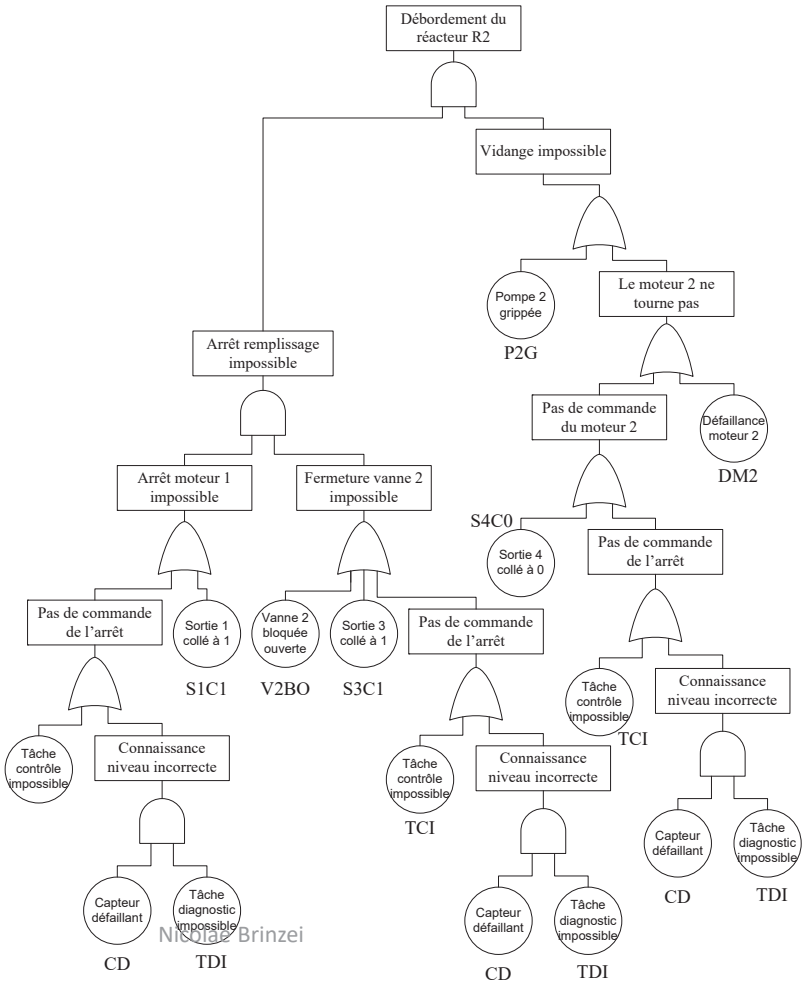
Exercice



Élaboration de l'arbre des défaillances

Exercice

AdD final



Coupes minimales. Implicants premiers

Coupe

Définition

Une **coupe** est un ensemble d'événements entraînant l'événement indésirable.

Exemple

Dans l'exemple du circuit de commande du moteur on a recensé 6 événements de base :

A - Défaillance première du moteur
B - Défaillance première du relais
C - Défaillance première du bouton poussoir
D - Défaillance première du fusible
E - Défaillance de l'opérateur
F - Surdimensionnement du fusible

Les coupes sont nombreuses. On les représente par l'expression logique (monôme) de l'intersection des variables booléennes associées aux événements.

Par exemple A.B.F représente une coupe (les événements A, B et F) mais aussi B.F.

Coupes minimales. Implicants premiers

Coupe

Définition

Une **coupe minimale** est un ensemble d'événements tel qu'il ne contient pas un sous-ensemble d'événements qui soit aussi une coupe.

Les événements d'une coupe minimale sont donc tous nécessaires pour entraîner l'événement sommet.

Exemple

Dans l'exemple du circuit de commande du moteur, la coupe ABF contient la coupe BF, ABF n'est donc pas minimale.

Définition

L'**ordre d'une coupe** correspond au nombre d'événements qu'elle contient (nombre de termes du monôme logique).

Remarque

Plus l'ordre est petit, plus la coupe est critique (points faibles du système).

LORRAINE INP Ensem

Coupes minimales. Implicants premiers

Coupe

Exercice

Donner deux exemples de coupes d'ordre 2, 3, 4 et 5 de l'installation chimique traitée précédemment.

Exercice

Trouver deux coupes minimales de l'installation chimique.

Coupes minimales. Implicants premiers

Réduction de l'arbre des défaillances

L'objectif est de rechercher les coupes minimales d'ordre minimal. Pour cela, il faut simplifier l'expression logique définissant l'événement indésirable à partir des événements de base, ou en réduisant directement le logigramme représenté par l'AdD.

Exemple

Dans l'exemple du circuit de commande du moteur, l'expression logique de l'événement redouté (sommet de l'arbre) est :

$$S = [((E + C) + B) + A] \cdot [(F + D) \cdot (B + A + (C + E))]$$

Cette fonction peut être simplifiée (d'une manière générale, on peut utiliser les techniques de réduction des fonctions booléennes : tables de Karnaugh, …).

Ici, par simplification directe (Idempotence de l'opération ET et distributivité des opérations ET et OU) :

$$S = AF + AD + BF + BD + CF + CD + EF + ED$$

Coupes minimales. Implicants premiers

Le polynôme réduit (et irréductible) obtenu contient toutes les coupes minimales (chaque monôme premier représente une coupe). Dans l'exemple, elles sont toutes d'ordre 2, il faudra donc toujours une double défaillance pour entraîner l'événement indésirable.

Exercice

Donner le polynôme réduit de l'événement sommet de l'exercice traitant l'installation chimique et en déduire la liste des coupes minimales.

Coupes minimales. Implicants premiers

Implicants premiers

Il ne faut pas confondre les coupes minimales avec les implicants premiers d'une fonction logique. En effet, dans une coupe minimale, on ne peut trouver de variable complémentée (non occurrence d'événement). En effet, il faut supposer que l'étude qui vient d'être faite concerne les systèmes cohérents, c'est à dire tels que :

- la panne de tous les composants ⇒ la panne du système
- le fonctionnement de tous les composants ⇒ le fonctionnement du système
- si le système est en panne, aucune défaillance supplémentaire ne peut rétablir le fonctionnement du système.

Pour les systèmes non-cohérents, leur analyse peut conduire à l'utilisation d'implicants premiers en généralisant ainsi la notion de coupe.

Analyse quantitative

La probabilité d'avoir l'événement indésirable est égale à celle d'avoir au moins une coupe vraie parmi toutes les coupes :

$$P[S] = P[C_1 + C_2 + \ldots + C_n]$$

où le signe plus représente l'opérateur OU

La probabilité d'une coupe est égale au produit des probabilités de chacun de ses événements élémentaires.

Les coupes étant des combinaisons des événements de base, deux coupes sont corrélés lorsqu'elles ont en commun un ou plusieurs événements de base.

Le calcul de P[S] doit donc faire appel au principe d'inclusion-exclusion des probabilités (théorème de Sylvester-Poincaré) :

$$P[S] = \sum_{i=1}^{n} P[C_i] - \sum_{j=2}^{n}\sum_{i=1}^{j-1} P[C_i.C_j] + \sum_{J=3}^{n}\sum_{k=2}^{j-1}\sum_{i=1}^{k-1} P[C_i.C_j.C_k] - .... + (-1)^n P[C_1.C_2....C_n]$$

Analyse quantitative

Remarque *Les probabilités de coupes sont en général faibles et d'autant plus que leur ordre est élevé et que la fiabilité des composants est grande (la défaillance première d'un composant a une probabilité égale à 1-R(t)).*

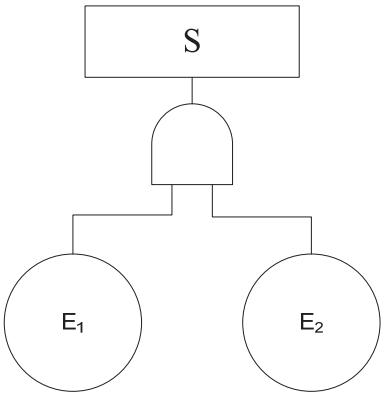
En conséquence, on ne calcule pas tous les termes de P[S] qui constituent une suite alternée décroissante. P[S] est toujours encadrée par la somme des k premiers termes et celle des k+1 premiers termes. Par exemple :

$$\sum_{i=1}^{n} P[C_i] - \sum_{j=2}^{n} \sum_{i=1}^{j-1} P[C_i.C_j] \leq P[S] \leq \sum_{i=1}^{n} P[C_i]$$

On arrête les calculs lorsque la correction apportée par la prise en compte du k+1è terme est inférieure à la précision de calcul désirée.

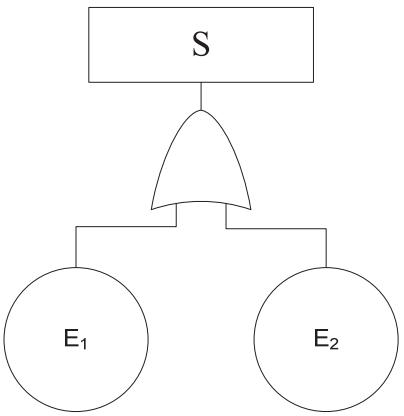
Analyse quantitative

Si les coupes sont constituées seulement des événements de base disjoints entre les coupes, on peut établir directement sur l'arbre réduit la probabilité de l'événement indésirable :



$P[S] = P[E_1 \text{ et } E_2]$
$= P[E_1].P[E_2/E_1]$
$= P[E_2].P[E_1/E_2]$

Si E_1et E_2 sont indépendants,
$P[S] = P[E_1].P[E_2]$
$P[S] = (1-R_1).(1-R_2)$



$P[S] = P[E_1 \text{ ou } E_2]$
$= P[E_1]+P[E_2]- P[E_1].P[E_2]$

Si E_1 et E_2 sont indépendants,
$P[S] = P[E_1]+P[E_2]$
$P[S] = (1-R_1)+(1-R_2)$

où E_i est l'événement défaillance du composant dont la fiabilité est R_i

Analyse quantitative

Remarque

Il existe des méthodes permettant de faire le calcul exact de la probabilité de l'événement sommet sans utiliser le théorème de Sylvester-Poincaré. Ces méthodes consistent à rechercher une expression du polynôme représentant l'événement sommet dans laquelle les monômes soient disjoints.

On peut citer en particulier la méthode des diagrammes de décision binaires (BDD) fondée sur le théorème de Shannon.

Bibliographie

[Aubry04] Sûreté de fonctionnement, Cours à l'Institut de Sûreté Industrielle, Nancy, 2004.

[Limnios05] Arbres de défaillances, 2ème édition, Editions Hermès-Lavoisier, 2005 (*Cote bibliothèque: Eole 519.2 LIM 2ed*).

[Limnios07] Fault trees, Editions ISTE, 2007 (*Cote bibliothèque: Eole 519.2 LIM*).

[Villemeur88] Sûreté de fonctionnement des systèmes industriels, Edition Eyrolles, 1988.

[Iddir14] Études des dangers : arbre de défaillances (méthode d'analyse détaillée des risques ADR), Techniques de l'Ingénieur, 2014.

[Haimes04] Risk modeling, assessment and management, 2nd edition, Wiley-Interscience, 2004 (*Cote bibliothèque: 1er niveau - Espace ouvrages 363 HAI*).

[Bertsche08] Reliability in Automotive and Mechanical Engineering, Springer, 2008 https://link-springer-com.bases-doc.univ-lorraine.fr/book/10.1007/978-3-540-34282-3.