

UNIVERSITÉ DE TECHNOLOGIE DE COMPIÈGNE

UTC

Maitrise des Risques

Cours 9 & TD : les arbres de défaillance et d'événements



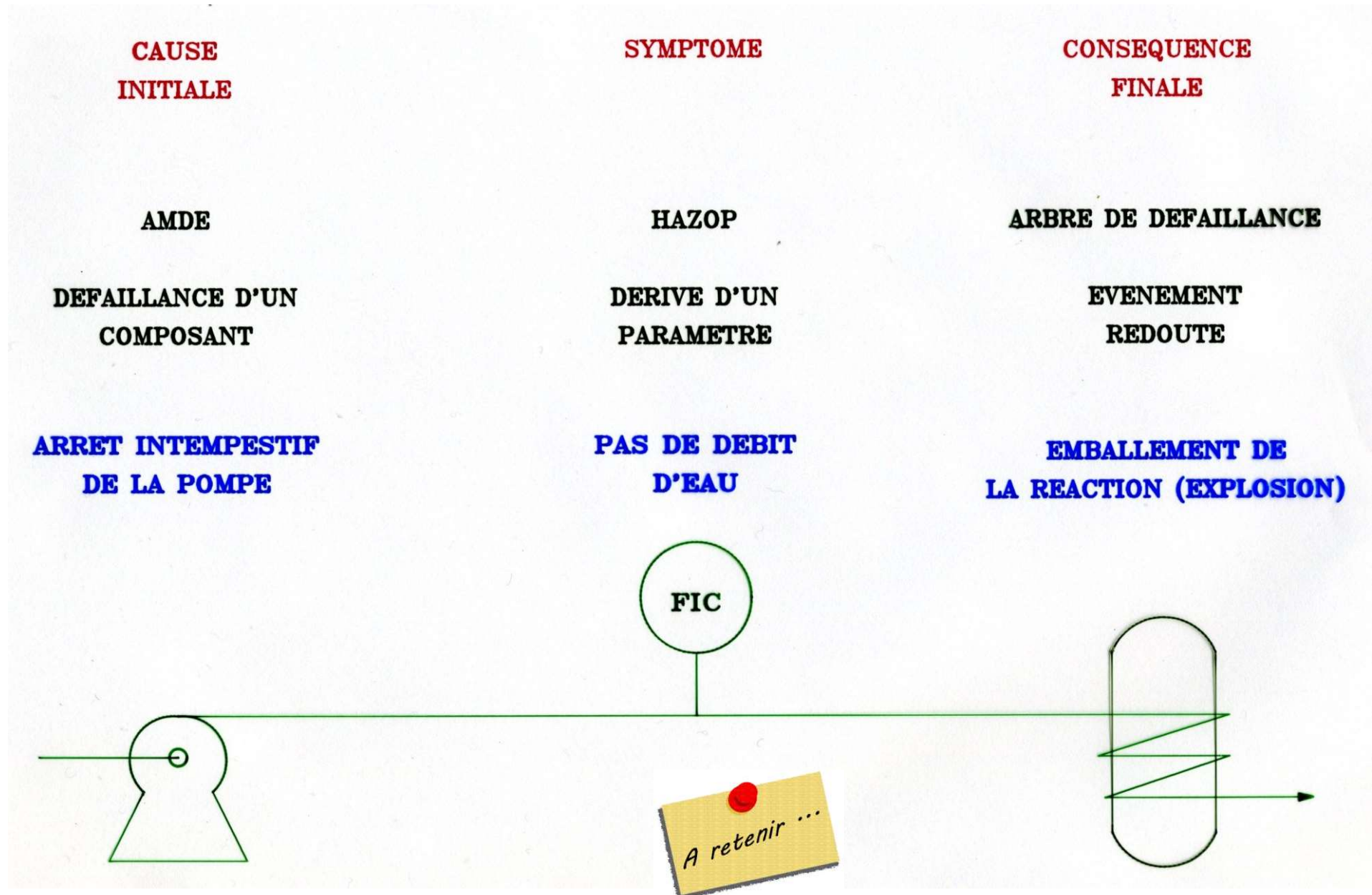
UV TS01

Resp : christophe.proust@utc.fr

donnons un sens à l'innovation



Un pb de sécurité => une méthode ?





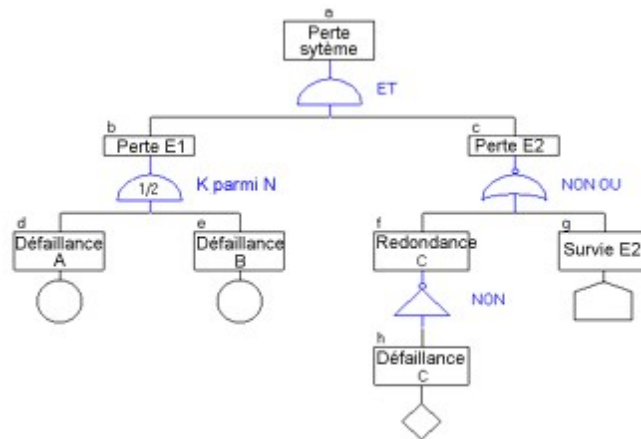
Pourquoi des « arbres » logiques ?

1. Maitriser les risques pour des « ruptures »
technologiques
2. Concevoir des « barrières » de sécurité

Historique

Absence de règle pour de nouvelles technologies :

- Arbre de défaillance pour les missiles (1961 Bell Telephone Laboratories)
- La certification de Concorde





L'arbre des défaillances

Ou des « pannes »

Principes




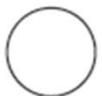


Codifiés dans la norme CEI 61025 : 1990 “ Analyse par Arbre de Panne (APP) ”

Objectifs :

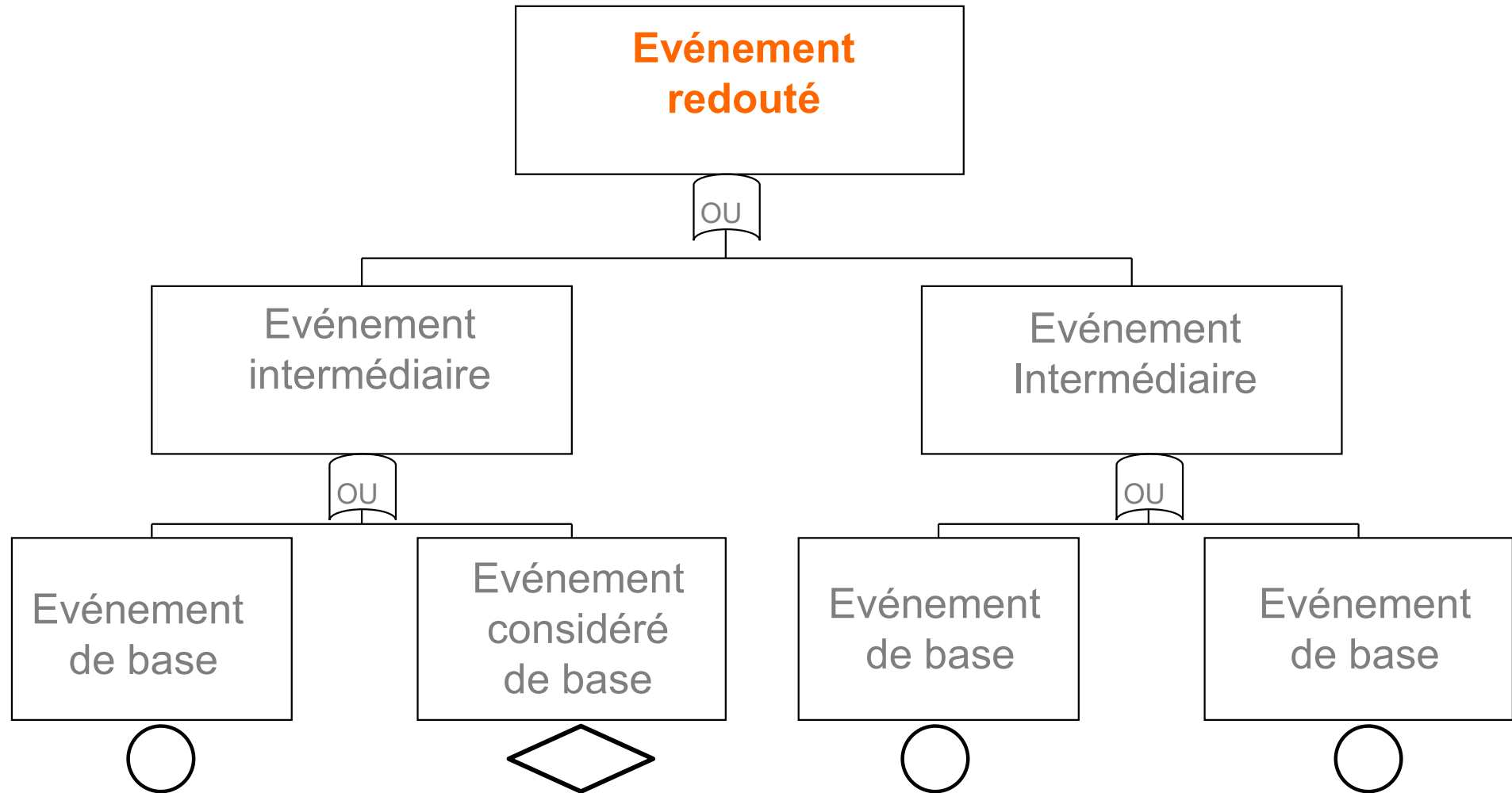
- Déterminer, pour un « événement redouté donné », l'enchaînement et la combinaison logique d'événements précurseurs conduisant à cet événement ;
- Remonter aux évènements élémentaires :
 - Suffisamment connus d'où pas nécessaire d'en identifier les causes,
 - Évènements dont les causes présentent peu d'intérêts,
 - Évènements dont les causes seront étudiées par ailleurs...



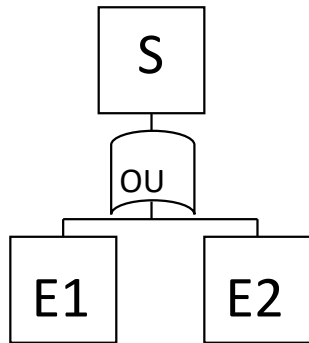
Symboles

Symbole	Description
	Élément intermédiaire Élément relatif à un événement qui a au moins un antécédent « cause » relié avec une porte logique.
	Porte « ET » L'évènement de sortie se réalise si tous les évènements reliés à la porte se réalisent en même temps.
	Porte « OU » L'évènement de sortie se réalise si seulement un seul des évènements reliés à la porte se réalise.
	Élément de base Élément relatif à un événement qui ne nécessite pas de développement, les limites de résolution sont atteintes.
	Transfert Ce triangle indique que l'arbre correspondant à l'évènement auquel il est relié est développé séparément.
	Évènement non développé L'évènement ne sera pas développé car soit ces conséquences sont trop faibles, soit il n'y a pas d'informations disponibles.

Terminologie

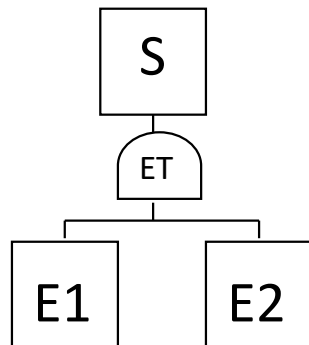


Les portes ET & OU



S est réalisé si :

- E1 est réalisé
- E2 est réalisé
- E1 et E2 sont réalisés

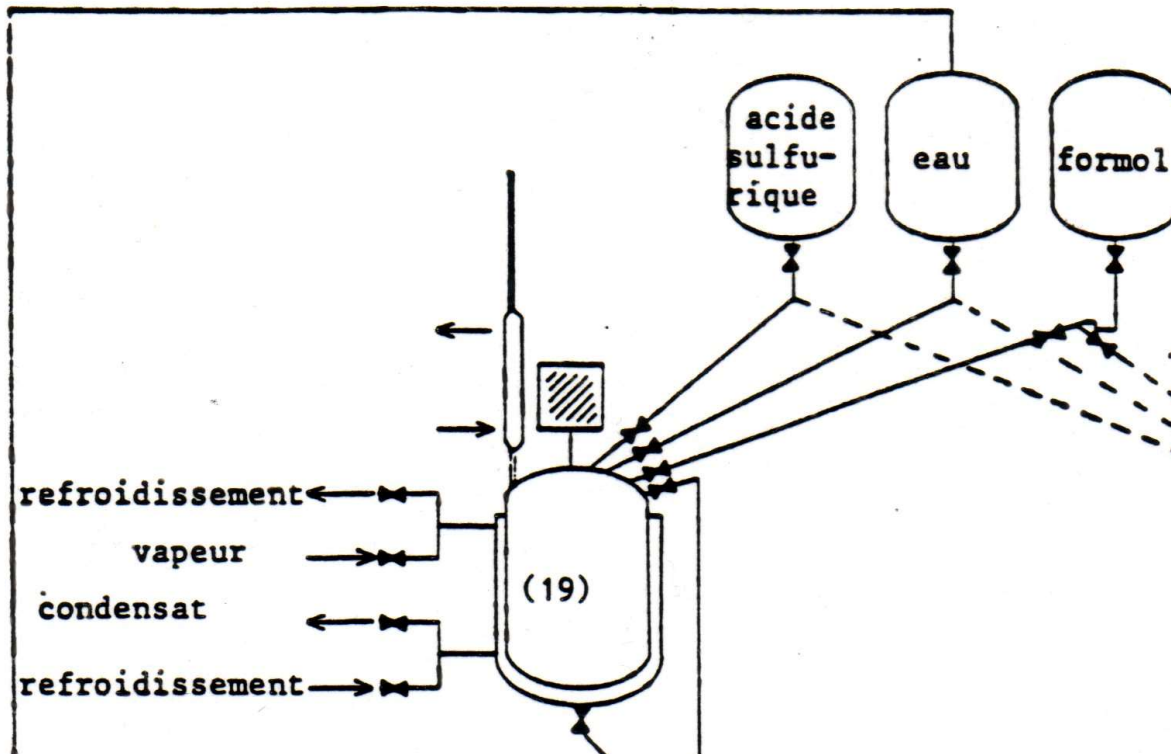


S est réalisé si et seulement si :

- E1 et E2 sont tous les deux réalisés

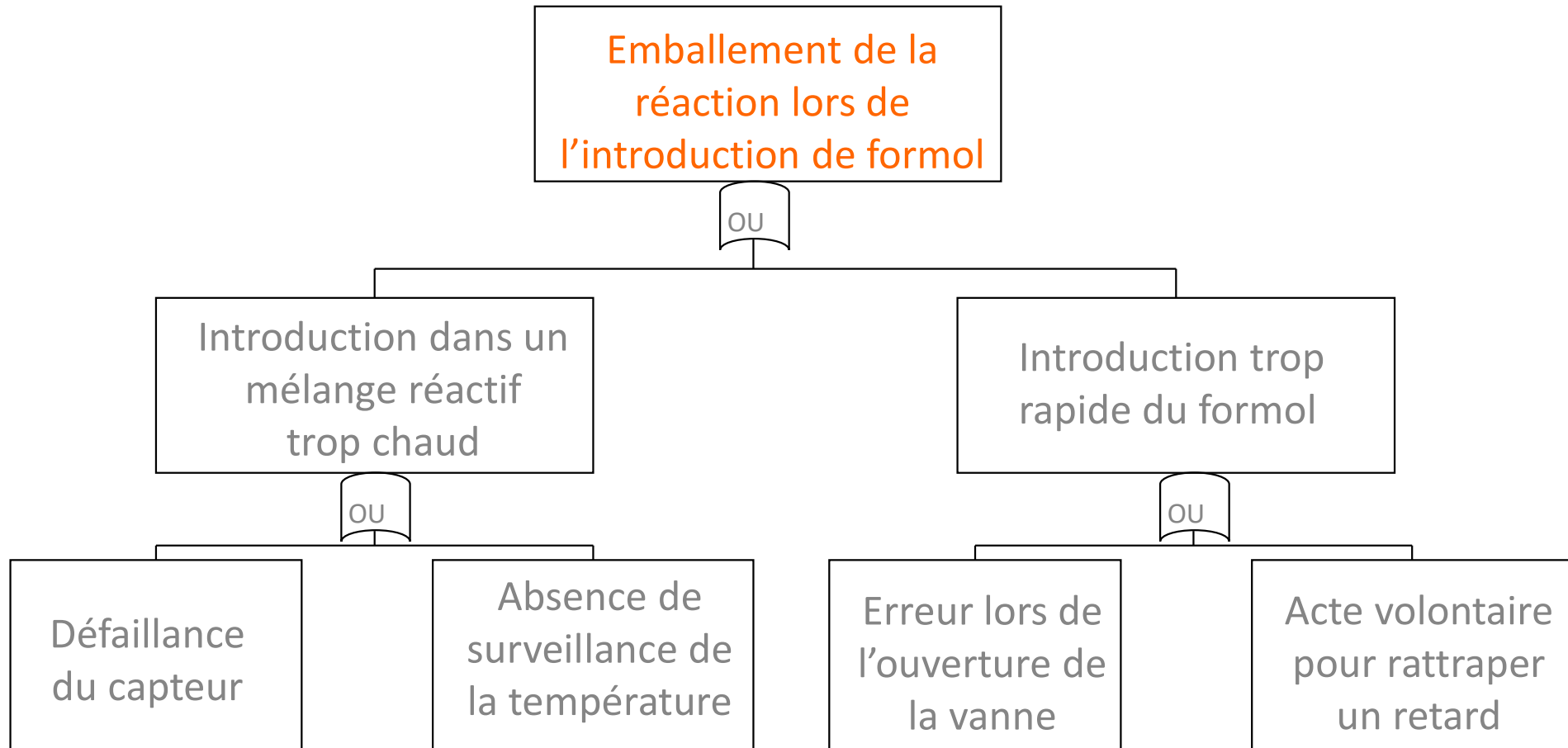


Construction d'un arbre



1. Chargement du naphthalène
2. Fusion du naphthalène
3. Sulfonation par addition H_2SO_4
4. **Addition de formol**
5. Précipitation du produit
6. Neutralisation par solution de
7. Chaux
8. Filtration du produit

Construction d'un arbre



« Réduction » de l'arbre

Pour :

- Visualiser les événements de base ou chemin (scénarios) « critiques »
- Supprimer les doublons pour estimer une probabilité de l'ERC
- Identifier les moyens d'agir (« barrières de sécurité »)

Définitions :

- coupe : ensemble d'événements (de base) dont la réalisation « simultanée » entraîne la réalisation de l'événement redouté
- coupe minimale : coupe ne contenant aucune autre coupe
- ordre : nombre d'événements de la coupe

Objectif de la réduction : arriver à une expression logique du type

$$A = C1+C2+C3+ \dots$$

$$\text{avec } C_i = B1.B2.B3\dots$$

A retenir ...

- Opérateur **OU** (+, U)

- 1) $A+B+C=(A+B)+C=A+(B+C)$
- 2) $A+B=B+A$
- 3) $A+A=A$
- 4) $A+1=1$
- 5) $A+0=A$
- 6) $1+1=1$

- Opérateur **ET** (x, ., \cap)

- 7) $A.B.C=(A.B).C=A.(B.C)$
- 8) $A.B=B.A$
- 9) $A.A=A$
- 10) $A.1=A$
- 11) $A.0=0$
- 12) $1x1=1 ; 1x0=0$
- 13) $A.(B+C)=A.B+A.C$
- 14) $A+A.B=A$
- 15) $A+B.C=(A+B).(A+C)$

- Opérateur Non (ou préfixe n)

16) $\overline{\overline{A}} = A$

17) $A + \overline{A} = 1$

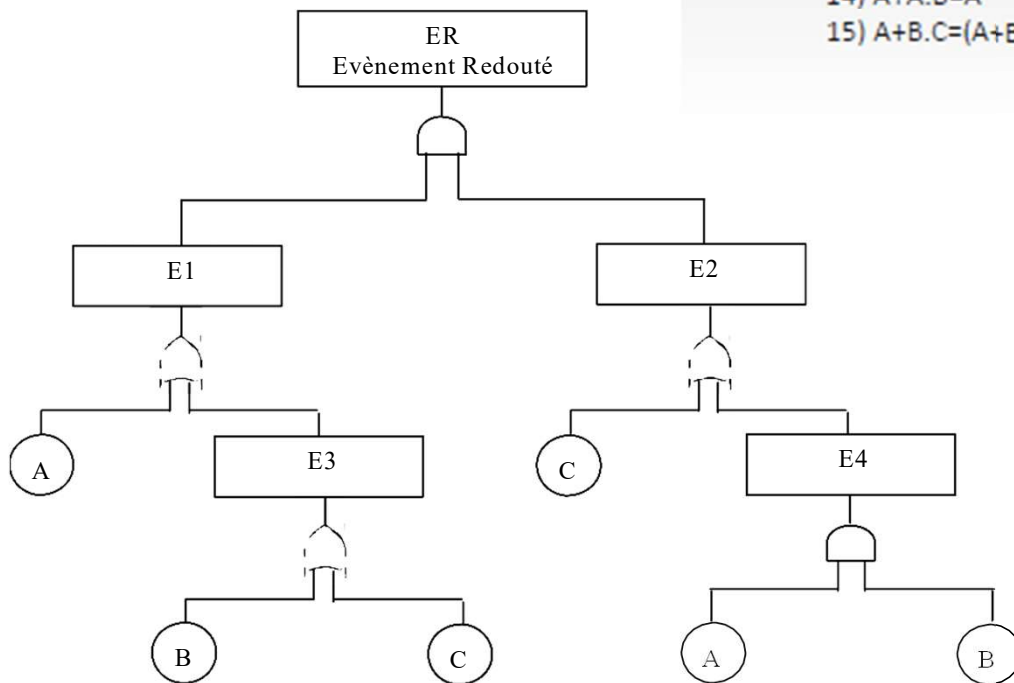
18) $A.\overline{A} = 0$

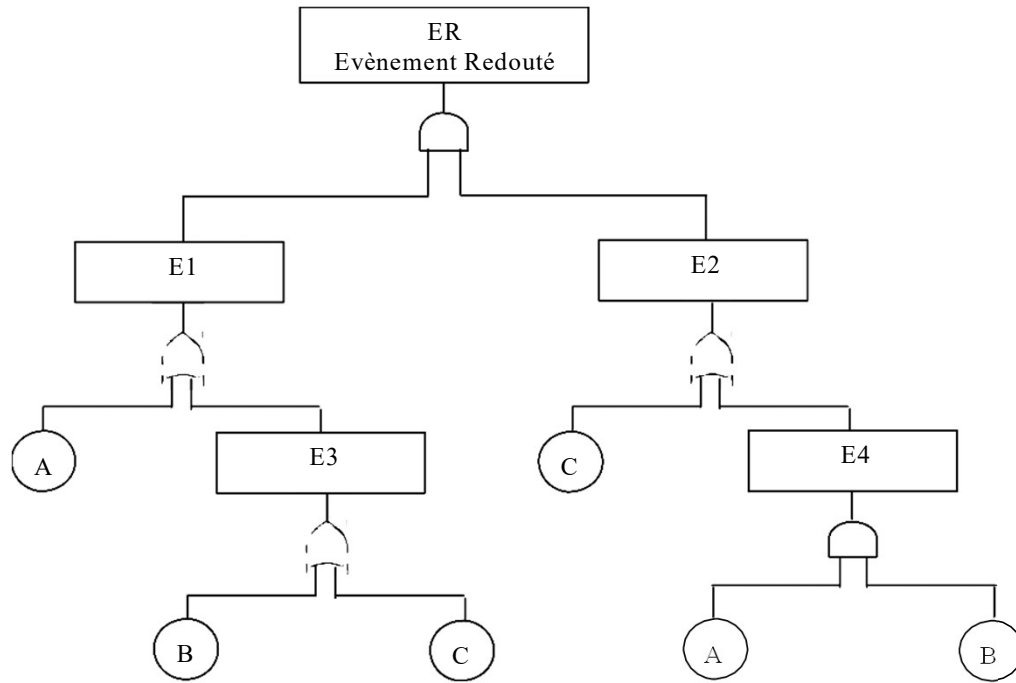
19) $A + \overline{A}B = A + B$

- Loi de Morgan

20) $\overline{A.B.....} = \overline{A} + \overline{B} + \dots$

21) $\overline{A+B+...} = \overline{A}.\overline{B}....$





$$ER = E1.E2$$

$$ER = (E3+A).(E4+C)$$

$$ER = E3.E4 + E3.C + A.E4 + A.C$$

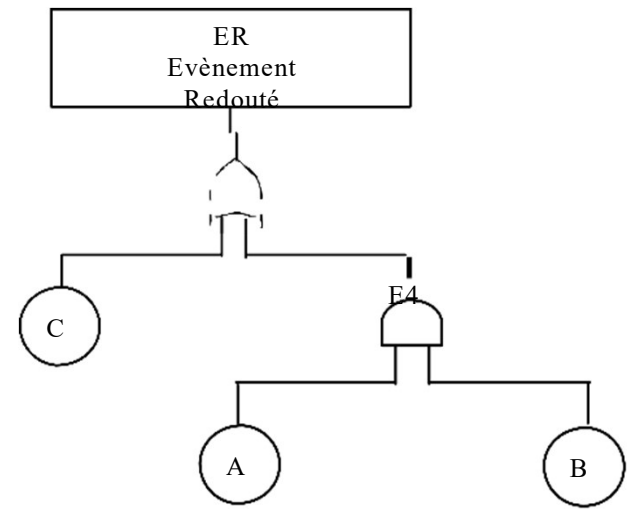
$$ER = (B+C).A.B + (B+C).C + A.A.B + A.C$$

$$ER = A.B.B + A.B.C + B.C + C.C + A.A.B + A.C$$

$$ER = A.B + A.B.C + B.C + C + A.B + A.C$$

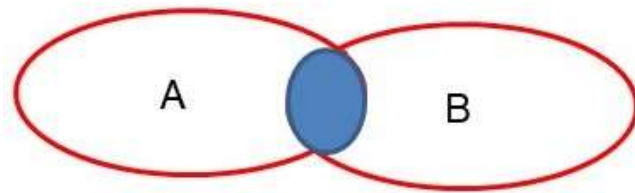
$$ER = A.B + C + A.C$$

$$ER = A.B + C$$



Sous l'hypothèse d'indépendance statistique => calcul de Probabilités

- $P(A.B) = P(A).P(B/A) = P(B).P(A/B)$ et si **A et B indépendants** => $P(A.B) = P(A).P(B)$
- $P(A+B) = P(A)+P(B)- P(A.B)$ et si **A et B indépendants** => $P(A+B) = P(A)+P(B)- P(A).P(B) \approx P(A)+P(B)$ si $P()$ petites
- $P(A+B+C) = P(A)+P(B)+P(C) - (P(A).P(B)+P(A).P(C)+P(B).P(C)) + P(A).P(B).P(C) \approx P(A)+P(B)+P(C)$ si $P()$ petites (A, B et C indépendants)



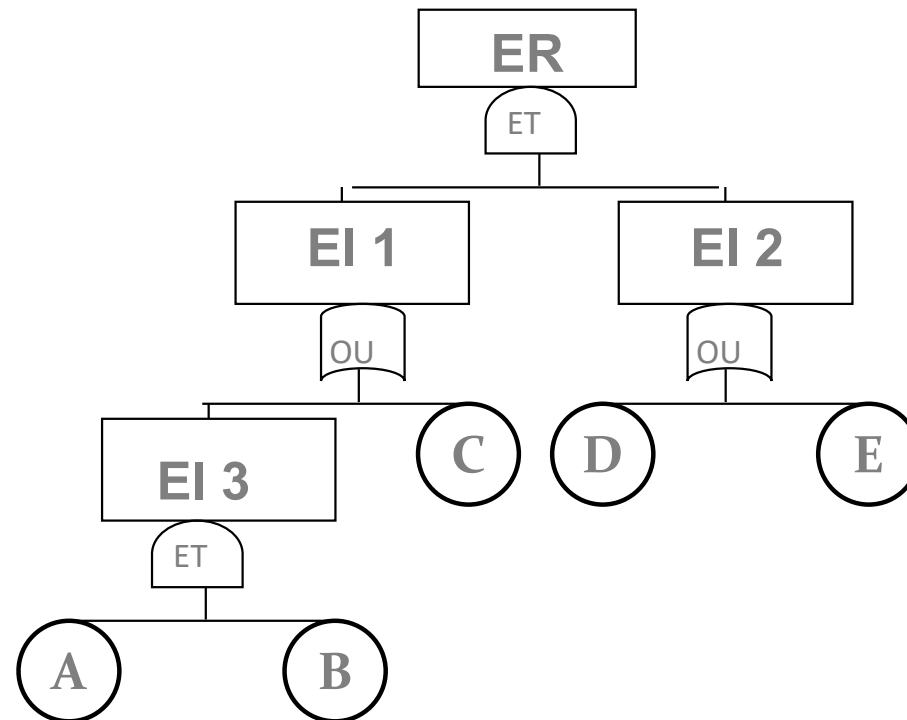
$$A+B = \text{red oval}$$

$$A.B = \text{blue oval}$$

... mais il faut d'abord réduire , ex :

Calculer $P(ER)$:

1. « Porte à porte »
2. Par les « coupes » après réduction de l'arbre



$$P(A) = 0,35$$

$$P(B) = 0,45$$

$$P(C) = 0,25$$

$$P(D) = 0,18$$

$$P(E) = 0,20$$

... « porte à porte »

$$ER = EI1.EI2$$

$$EI2 = E+D$$

$$EI1 = EI3+C$$

$$EI3 = A.B$$

$$P(A) = 0,35$$

$$P(B) = 0,45$$

$$P(C) = 0,25$$

$$P(D) = 0,18$$

$$P(E) = 0,20$$

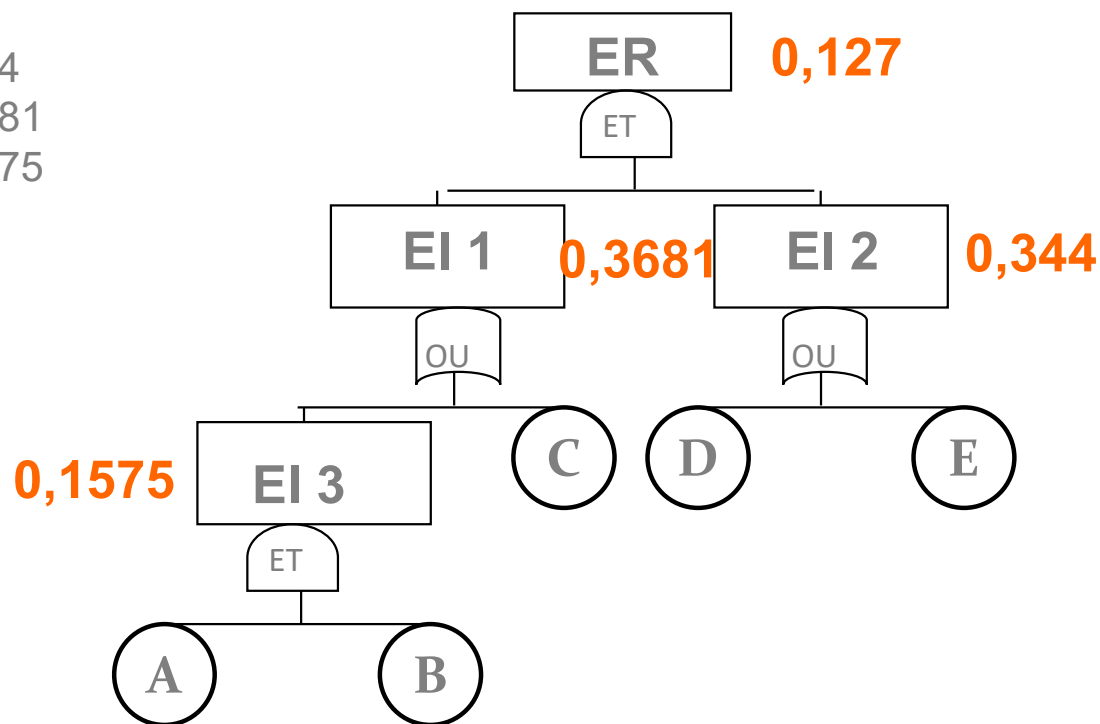
$$P(ER) = P(EI1).P(EI2)$$

$$P(EI2) = P(E) + P(D) - P(E).P(D) = 0,344$$

$$P(EI1) = P(EI3) + P(C) - P(EI3).P(C) = 0,3681$$

$$P(EI3) = P(A).P(B) = 0,1575$$

$$P(ER) = 0,127$$



...après réduction de l'arbre

$$ER = EI1.EI2$$

$$EI2 = E+D$$

$$EI1 = EI3+C$$

$$EI3 = A.B$$

$$ER = (E+D).(A.B+C)$$

$$ER = CD+CE+ABD+ABE$$

$$P(ER) \approx P(CD)+P(CE)+P(ABD)+P(ABE)$$

$$P(CD) \approx P(C).P(D) = 0,045$$

$$P(CE) \approx P(C).P(E) = 0,05$$

$$P(ABD) \approx P(A).P(B).P(D) = 0,0284$$

$$P(ABE) \approx P(A).P(B).P(E) = 0,0315$$

$$P(ER) \approx 0,1549$$

Calcul précis => 0,146

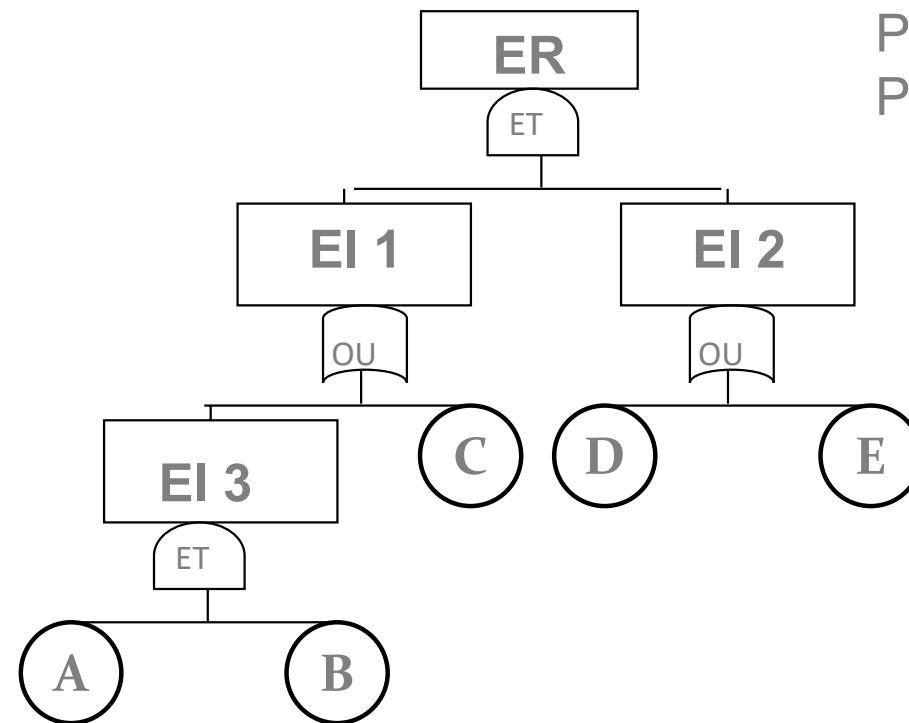
$$P(A) = 0,35$$

$$P(B) = 0,45$$

$$P(C) = 0,25$$

$$P(D) = 0,18$$

$$P(E) = 0,20$$



...particulièrement sensible si mode commun de défaillance

$P(X) = 0,1$
 $P(B) = 0,45$
 $P(C) = 0,25$
 $P(E) = 0,20$

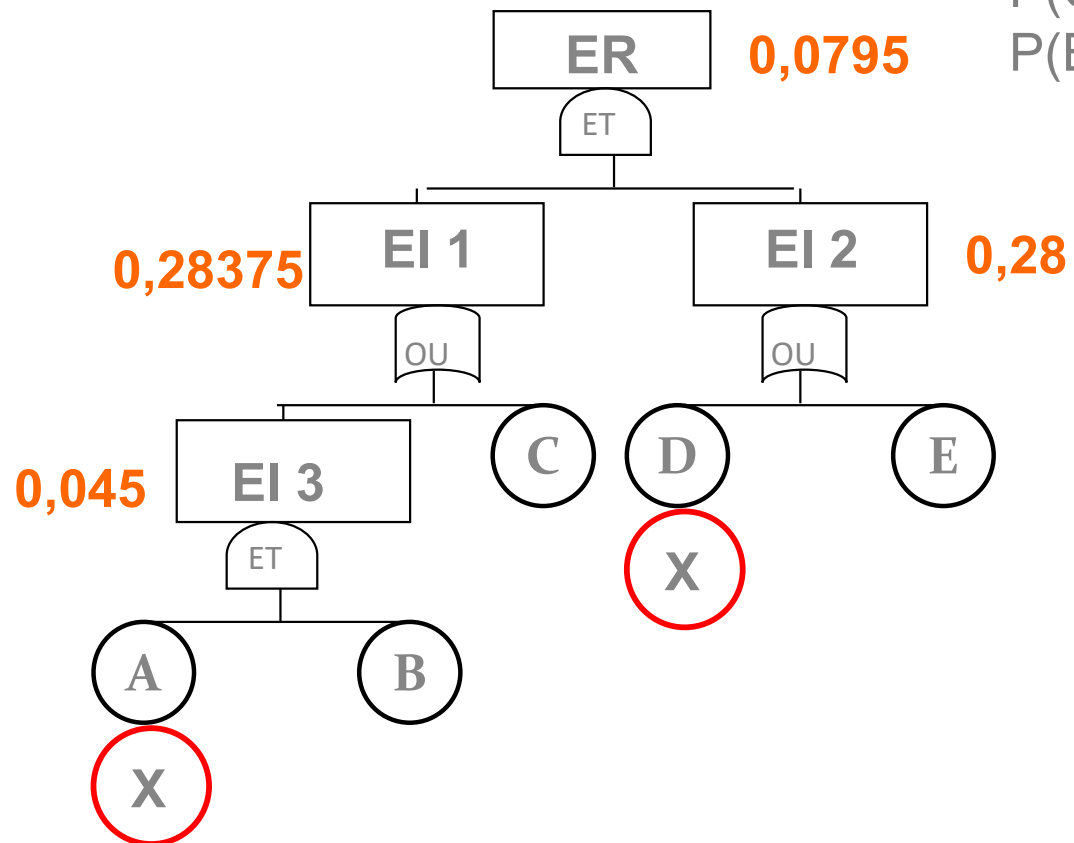
Si A et D sont expliqués par X

Réduction :

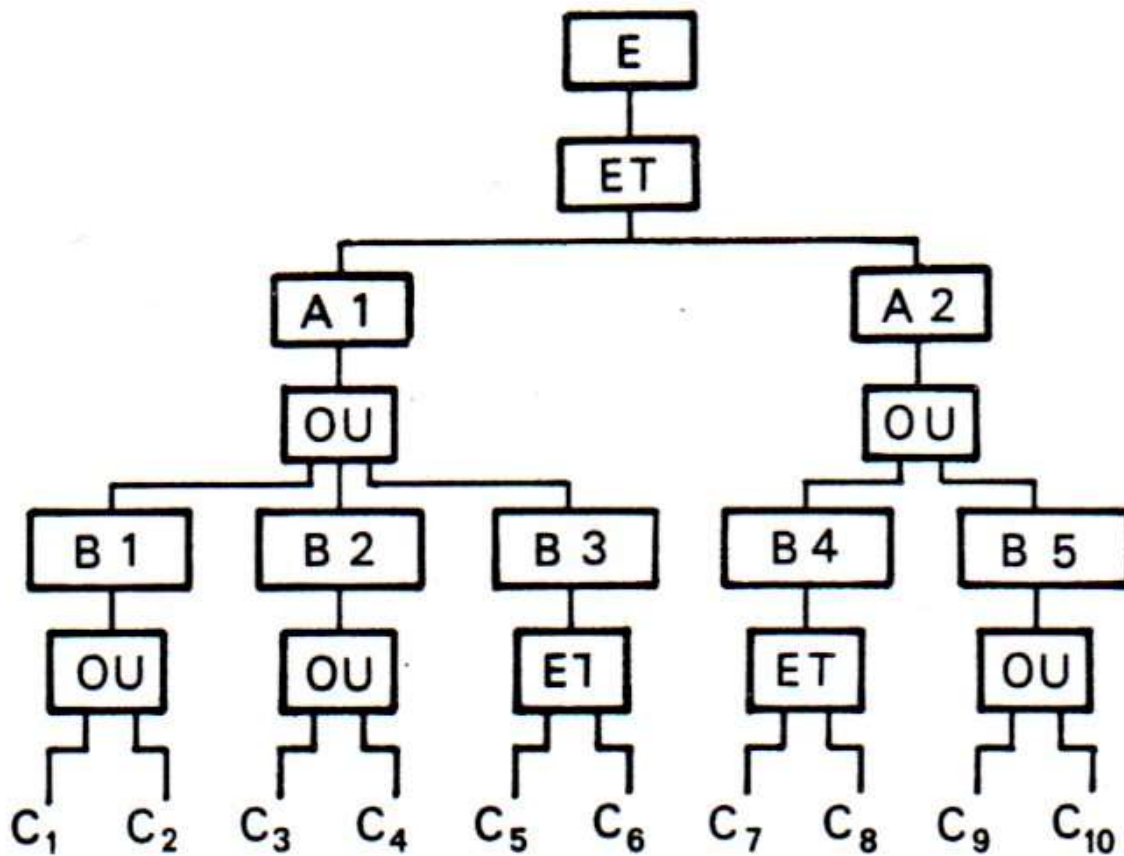
ER=
CX + 0,025
CE + 0,05
BX 0,045

$P(ER) = 0,120$

Calcul précis $P(ER) = 0,115$



RQ : Test de sensibilité

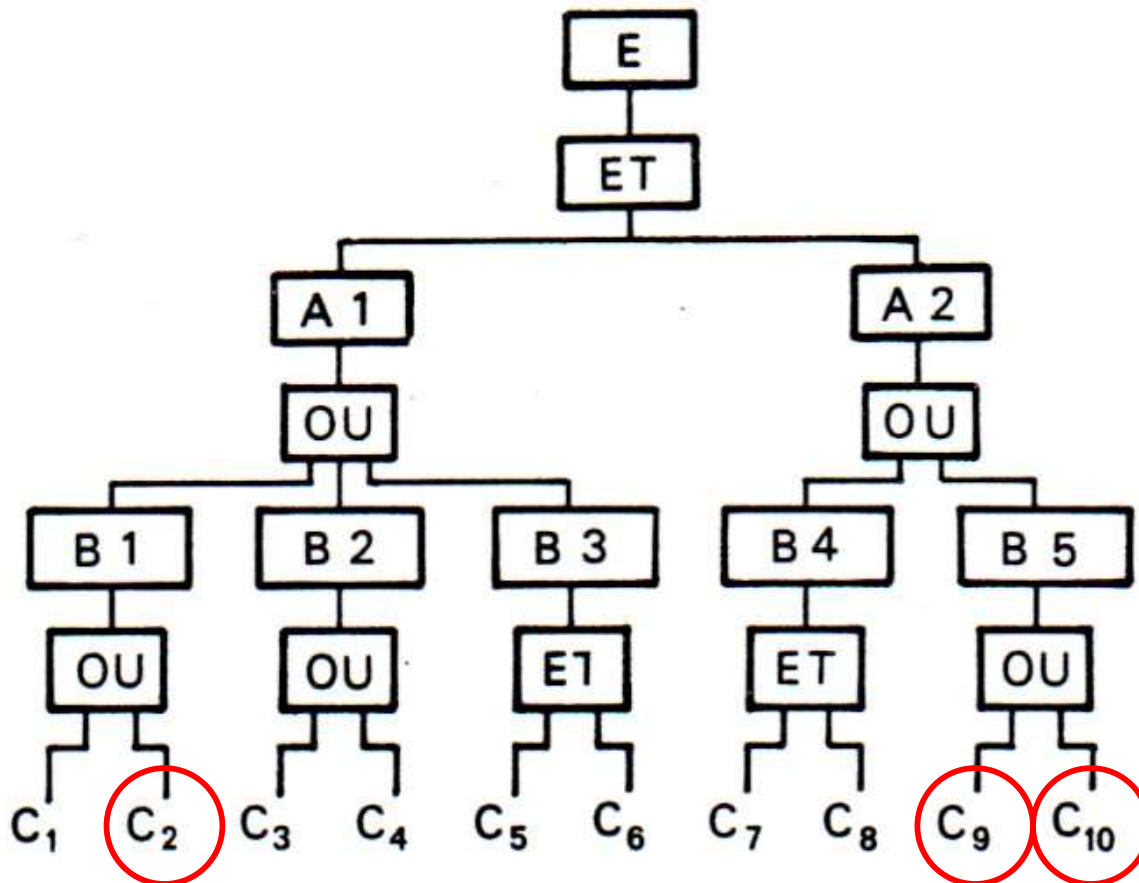


C_1	2×10^{-6}
C_2	3×10^{-3}
C_3	10^{-5}
C_4	10^{-6}
C_5	2×10^{-4}
C_6	10^{-3}
C_7	7×10^{-3}
C_8	9×10^{-6}
C_9	2×10^{-4}
C_{10}	10^{-4}

RQ = Test de sensibilité

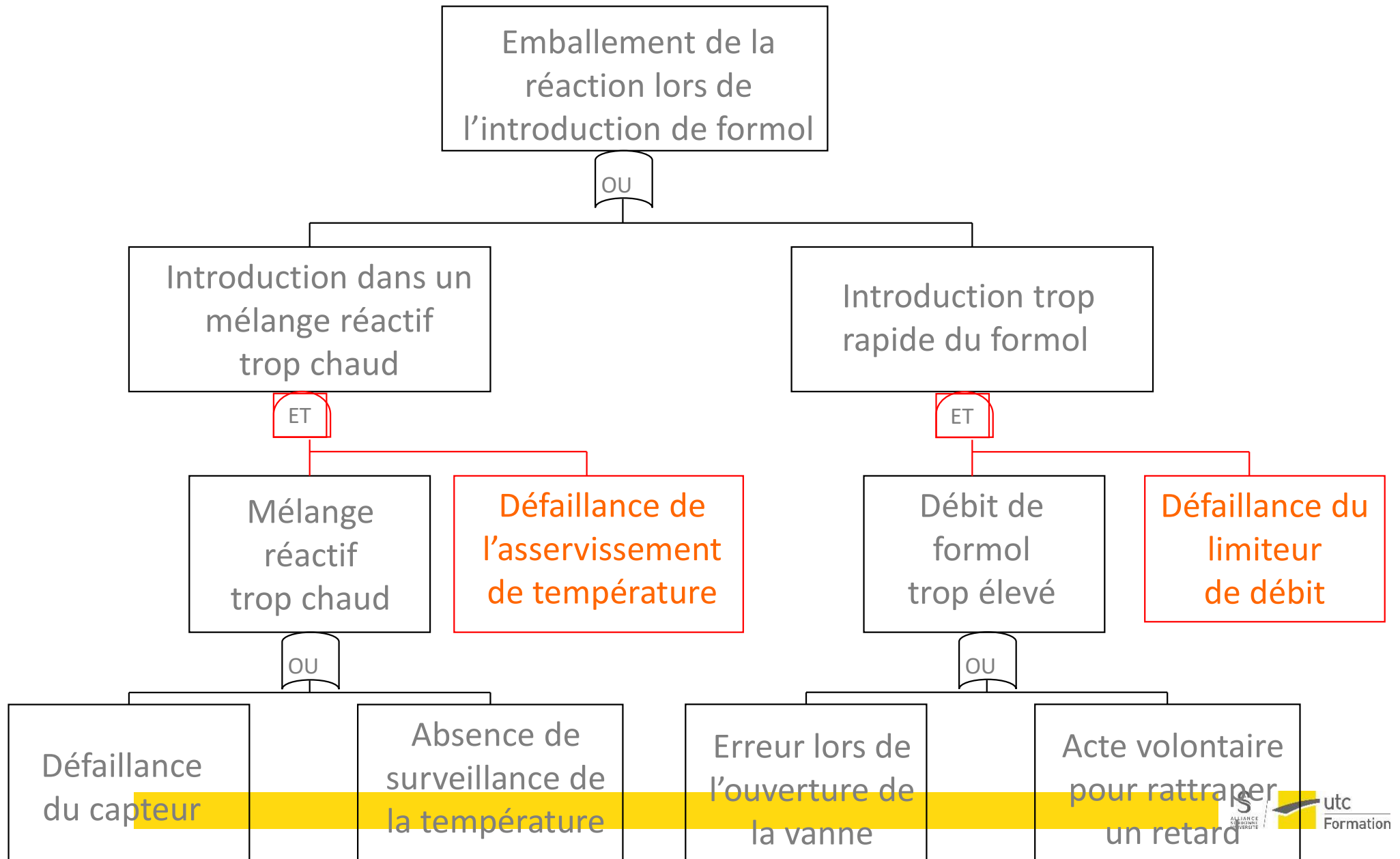
C1	2,00E-06	2,00E-05	2,00E-06	2,00E-06	2,00E-06	2,00E-06	2,00E-06	2,00E-06	2,00E-06	2,00E-06	2,00E-06	2,00E-06
C2	3,00E-03	3,00E-03	3,00E-02	3,00E-03	3,00E-03	3,00E-03	3,00E-03	3,00E-03	3,00E-03	3,00E-03	3,00E-03	3,00E-03
C3	1,00E-05	1,00E-05	1,00E-05	1,00E-04	1,00E-05	1,00E-05	1,00E-05	1,00E-05	1,00E-05	1,00E-05	1,00E-05	1,00E-05
C4	1,00E-06	1,00E-06	1,00E-06	1,00E-06	1,00E-05	1,00E-06	1,00E-06	1,00E-06	1,00E-06	1,00E-06	1,00E-06	1,00E-06
C5	2,00E-04	2,00E-04	2,00E-04	2,00E-04	2,00E-04	2,00E-03	2,00E-04	2,00E-04	2,00E-04	2,00E-04	2,00E-04	2,00E-04
C6	1,00E-03	1,00E-03	1,00E-03	1,00E-03	1,00E-03	1,00E-03	1,00E-02	1,00E-03	1,00E-03	1,00E-03	1,00E-03	1,00E-03
C7	7,00E-03	7,00E-03	7,00E-03	7,00E-03	7,00E-03	7,00E-03	7,00E-03	7,00E-02	7,00E-03	7,00E-03	7,00E-03	7,00E-03
C8	9,00E-06	9,00E-06	9,00E-06	9,00E-06	9,00E-06	9,00E-06	9,00E-06	9,00E-06	9,00E-05	9,00E-06	9,00E-06	9,00E-06
C9	2,00E-04	2,00E-04	2,00E-04	2,00E-04	2,00E-04	2,00E-04	2,00E-04	2,00E-04	2,00E-04	2,00E-03	2,00E-04	2,00E-04
C10	1,00E-04	1,00E-04	1,00E-04	1,00E-04	1,00E-04	1,00E-04	1,00E-04	1,00E-04	1,00E-04	1,00E-04	1,00E-04	1,00E-03
TOP	9,04E-07	9,10E-07	9,01E-06	9,31E-07	9,07E-07	9,05E-07	9,05E-07	9,06E-07	9,06E-07	6,33E-06	3,62E-06	3,62E-06

RQ : Test de sensibilité



C ₁	2×10^{-6}
C ₂	3×10^{-3}
C ₃	10^{-5}
C ₄	10^{-6}
C ₅	2×10^{-4}
C ₆	10^{-3}
C ₇	7×10^{-3}
C ₈	9×10^{-6}
C ₉	2×10^{-4}
C ₁₀	10^{-4}

Maitrise du risque : « barrières »...



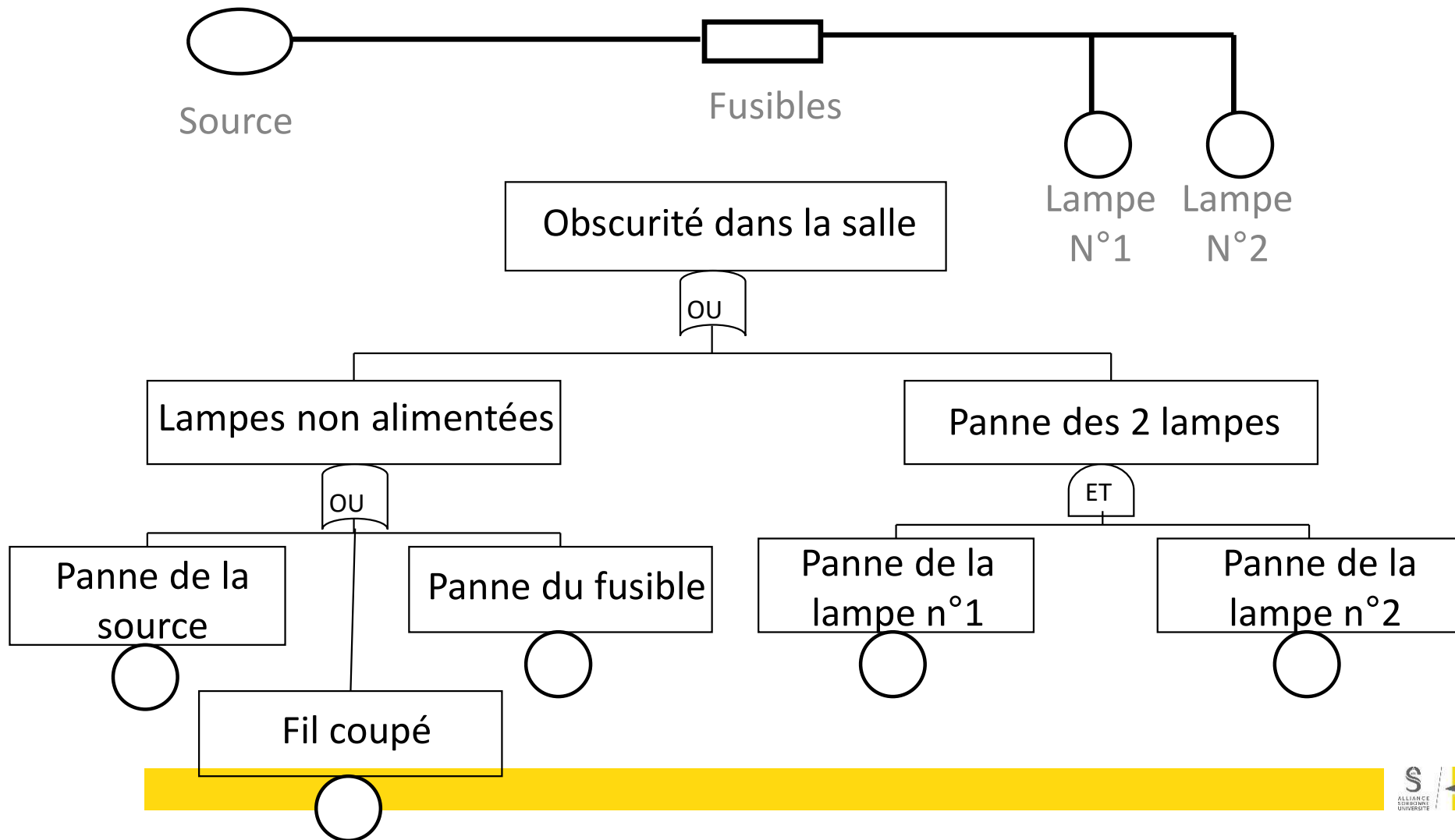


Exemples d'arbres de défaillances

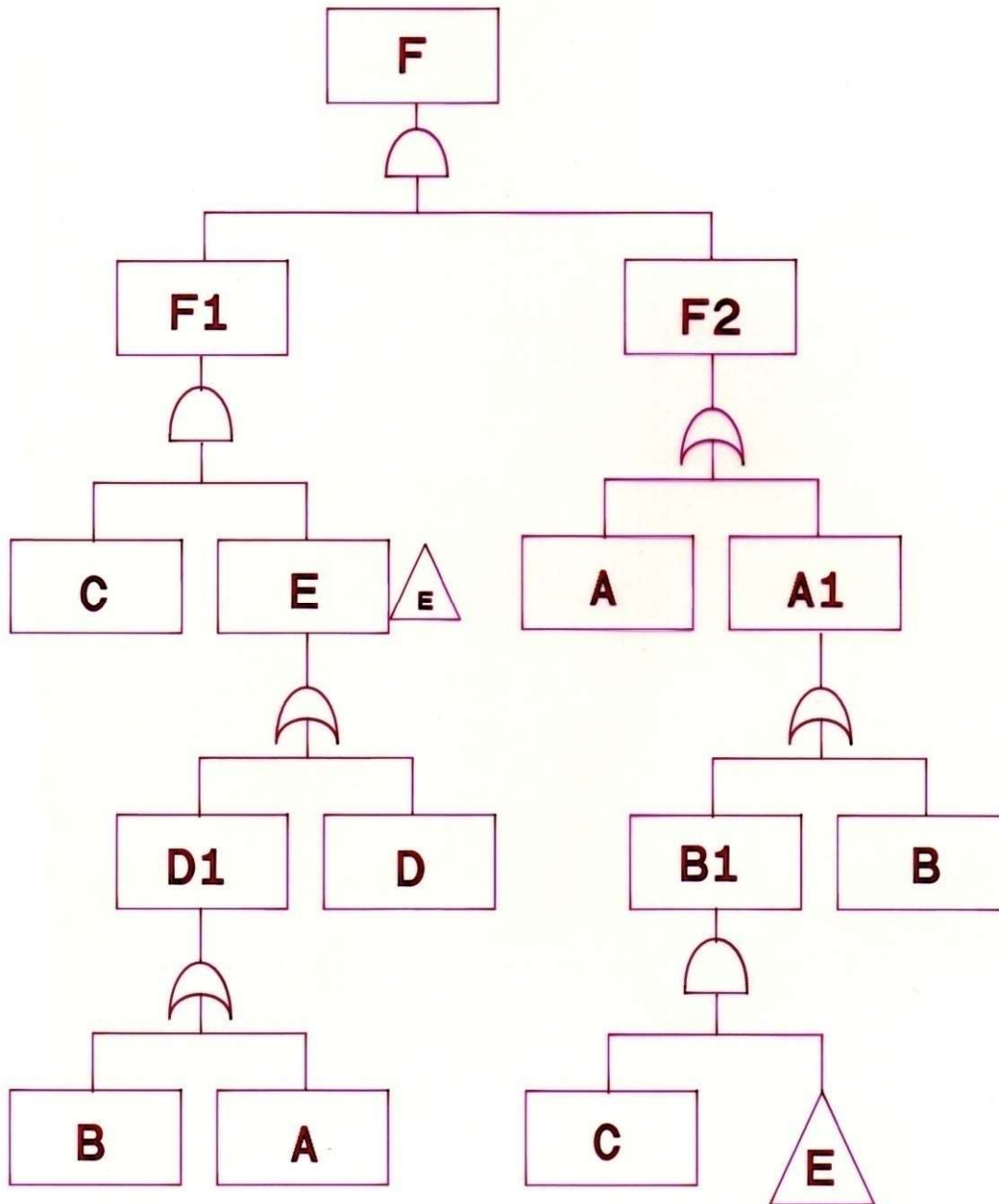
Réduction – construction – « barrières » de prévention

Construire un arbre :

ERC « obscurité dans la pièce »



Réduction d'arbre



$$F = F1.F2$$

$$F1 = C.E$$

$$E = D + D1$$

$$D1 = A + B$$

$$F1 = C.(A + B + D)$$

$$F2 = A + A1$$

$$A1 = B + B1$$

$$B1 = C.E = F1$$

$$F2 = A + B + F1$$

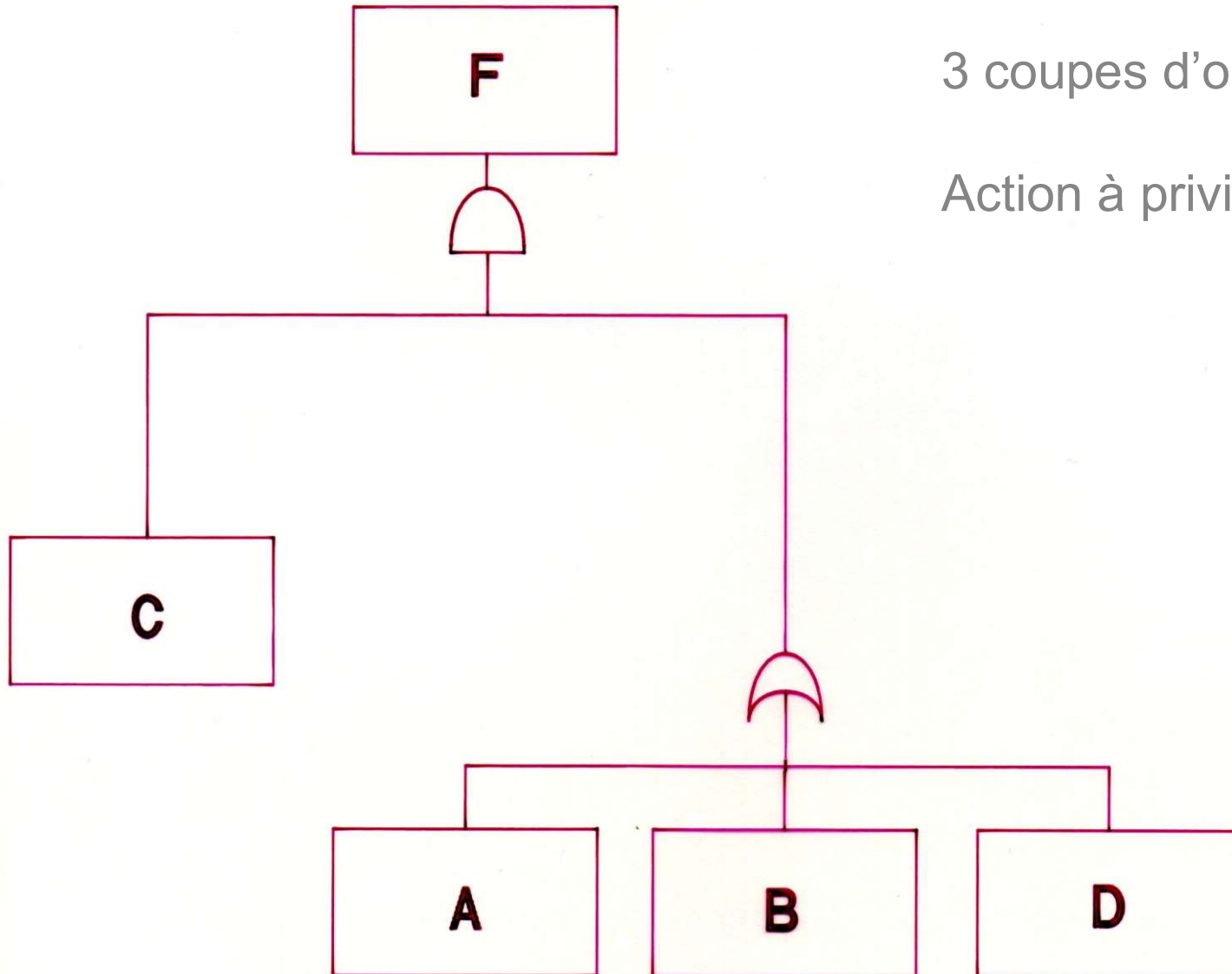
$$F = F1.(A + B + F1)$$

$$F = F1.A + F1.B + F1$$

$$F = F1$$

$$F = C.(A + B + D)$$

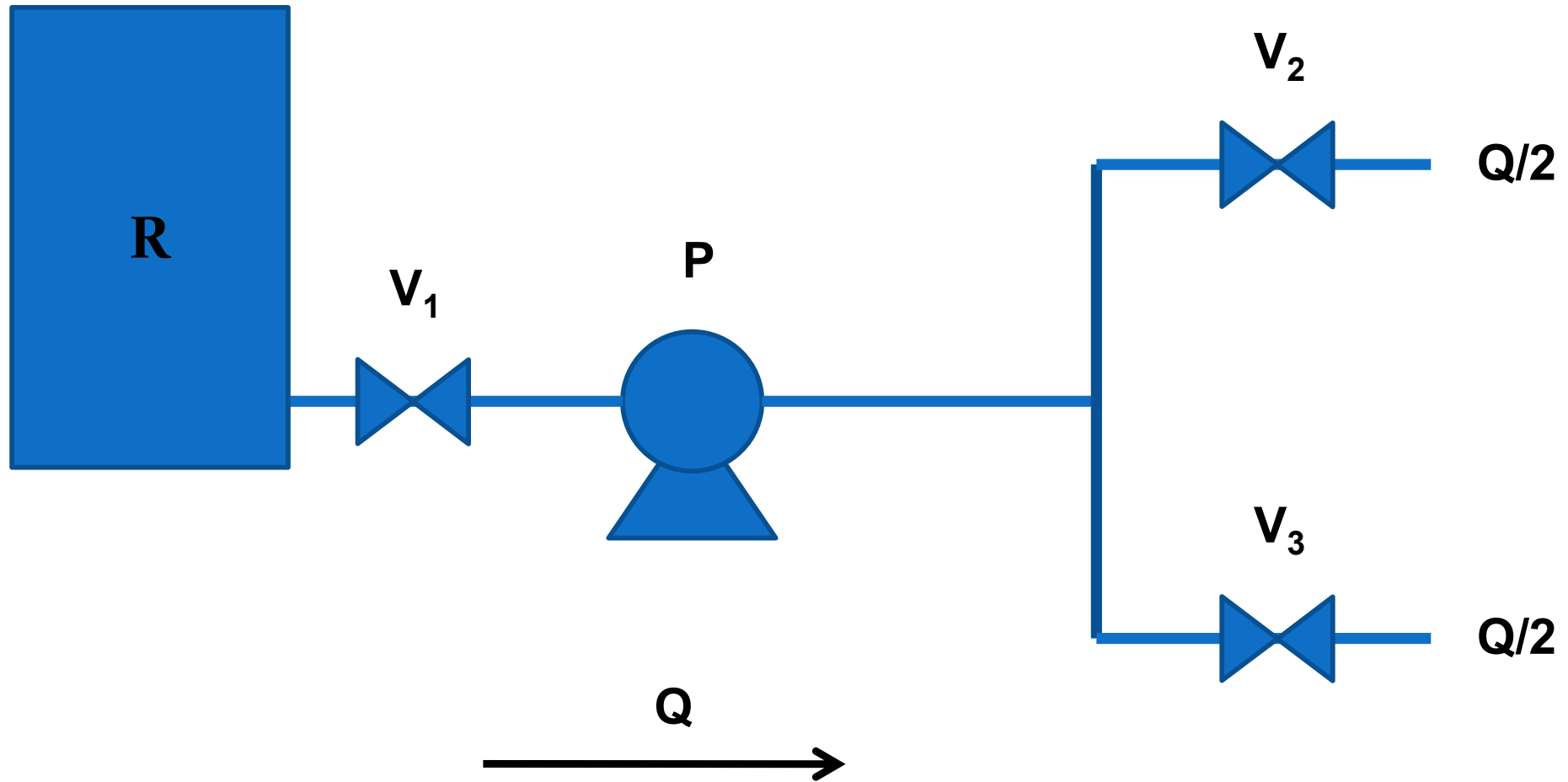
Réduction d'arbre : arbre réduit



3 coupes d'ordre 2

Action à privilégier sur « C »

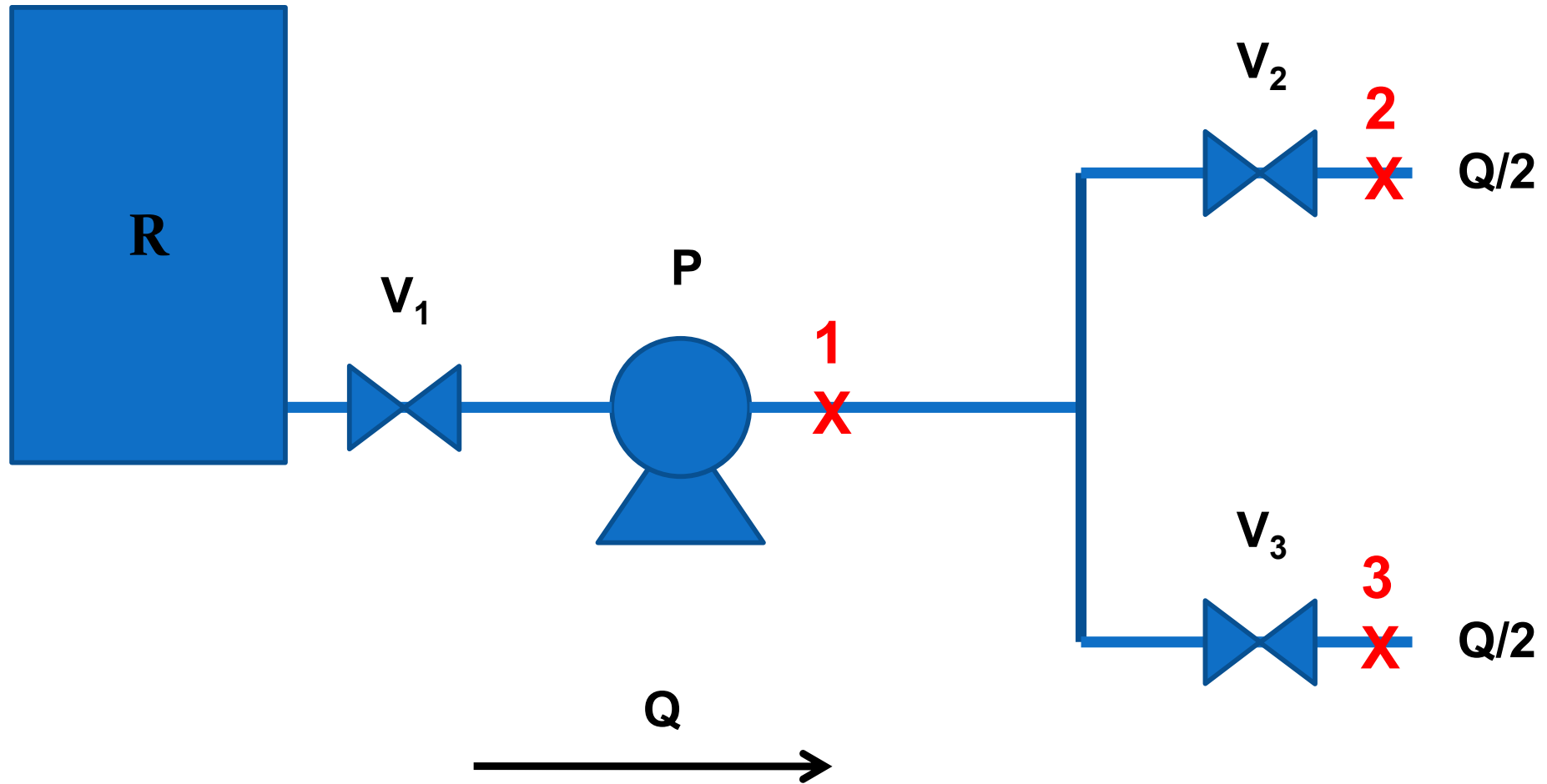
Exemple complet : refroidissement d'urgence



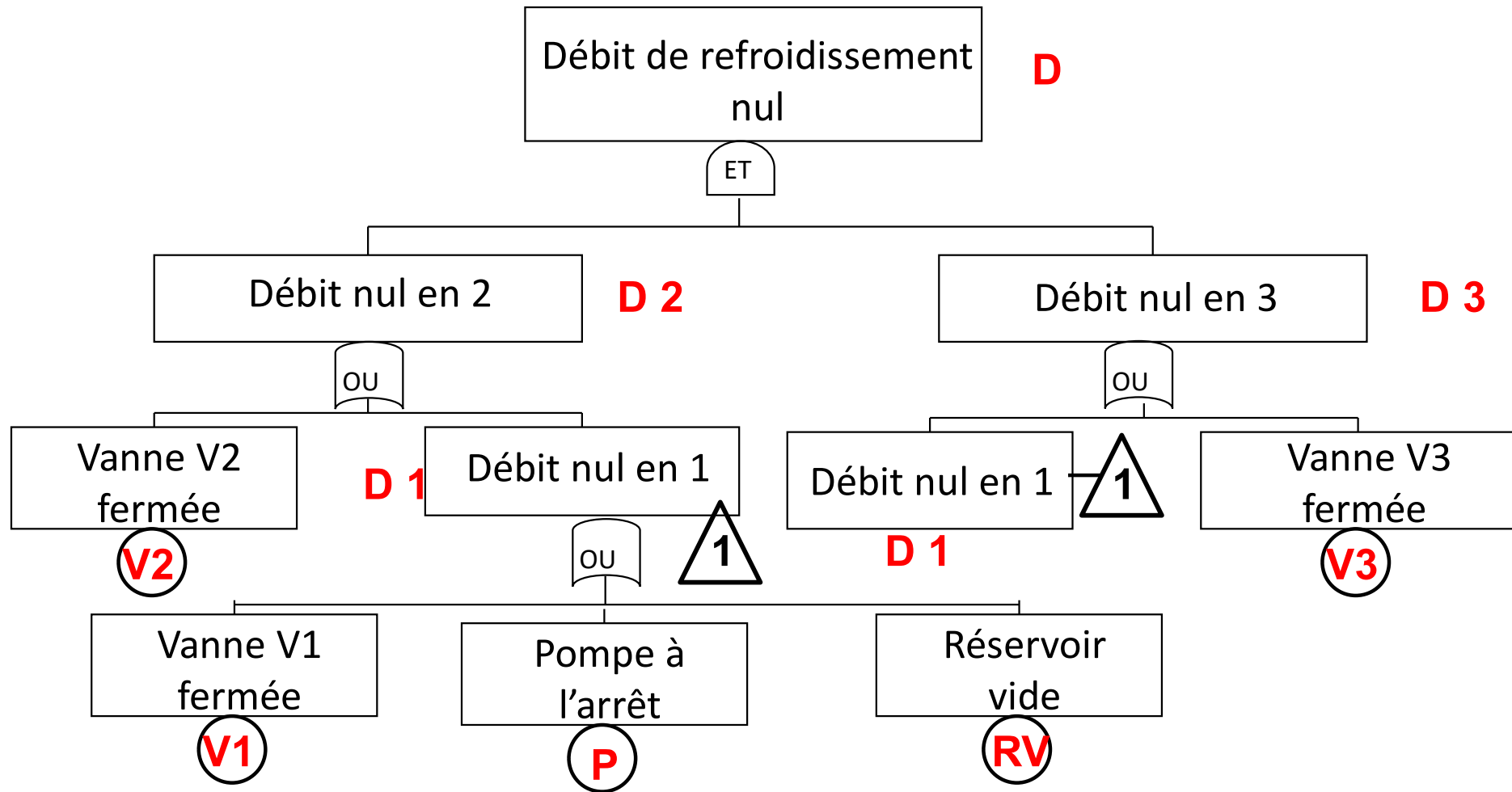
Circuit de refroidissement d'urgence

- ERC : les situations possibles = >
 - Débit de refroidissement nul : catastrophique
 - Débit de refroidissement = $Q/2$: critique
 - Débit de refroidissement = Q : normal
- Construire l'arbre complet
- Le réduire
- Reconstruire l'arbre réduit

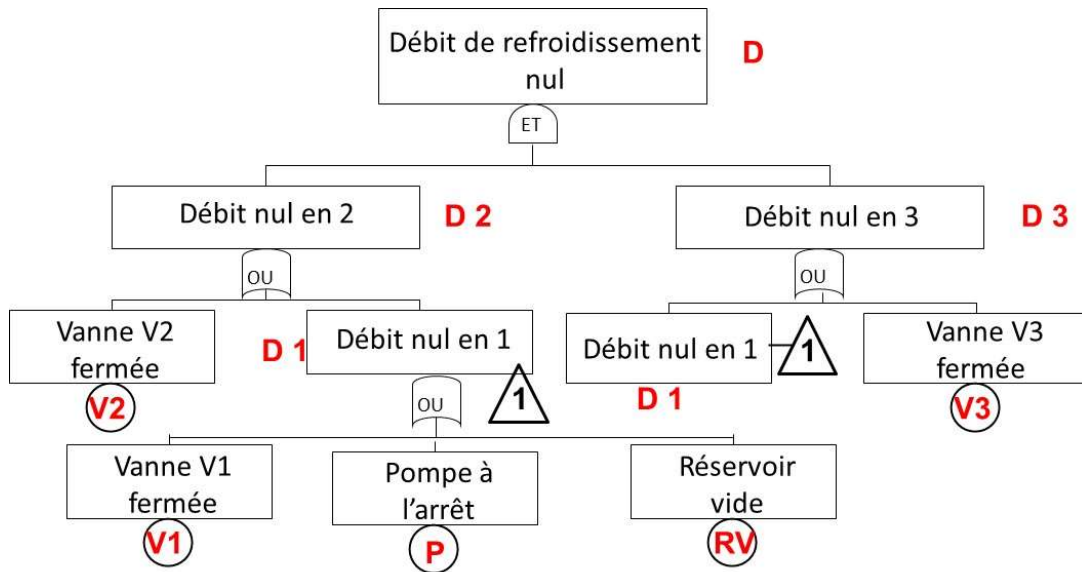
Circuit de refroidissement d'urgence



L'arbre complet



Réduction de l'arbre



$$D = D2.D3$$

$$D2 = V2 + D1$$

$$D3 = V3 + D1$$

$$D1 = V1 + P + RV$$

$$D = (V2 + D1).(V3 + D1)$$

$$D = V2.V3 + V2.D1 + D1.V3 + D1.D1$$

$$D = V2.V3 + V2.D1 + D1.V3 + \mathbf{D1.D1}$$

$$D = V2.V3 + V2.D1 + D1.V3 + D1$$

$$D = V2.V3 + V2.\mathbf{D1} + \mathbf{D1}.V3 + \mathbf{D1}$$

$$D = V2.V3 + D1$$

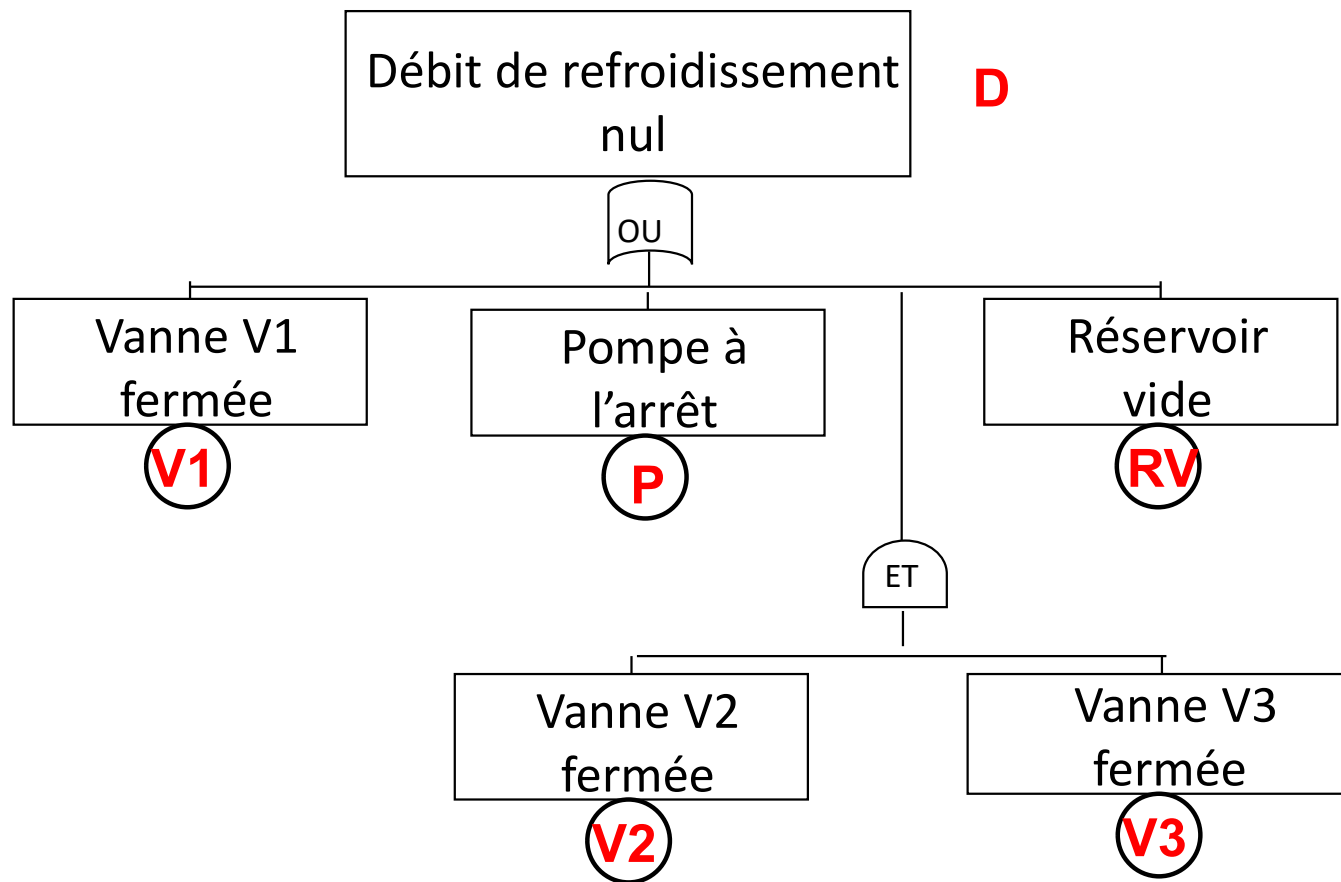
$$D1 = V1 + P + RV$$

$$D = V2.V3 + V1 + P + RV$$

Reconstruction de l'arbre réduit

$$D = V2.V3 + V1 + P + RV$$

3 coupes d'ordre 1
1 coupe d'ordre 2





L 'arbre « d'événements »

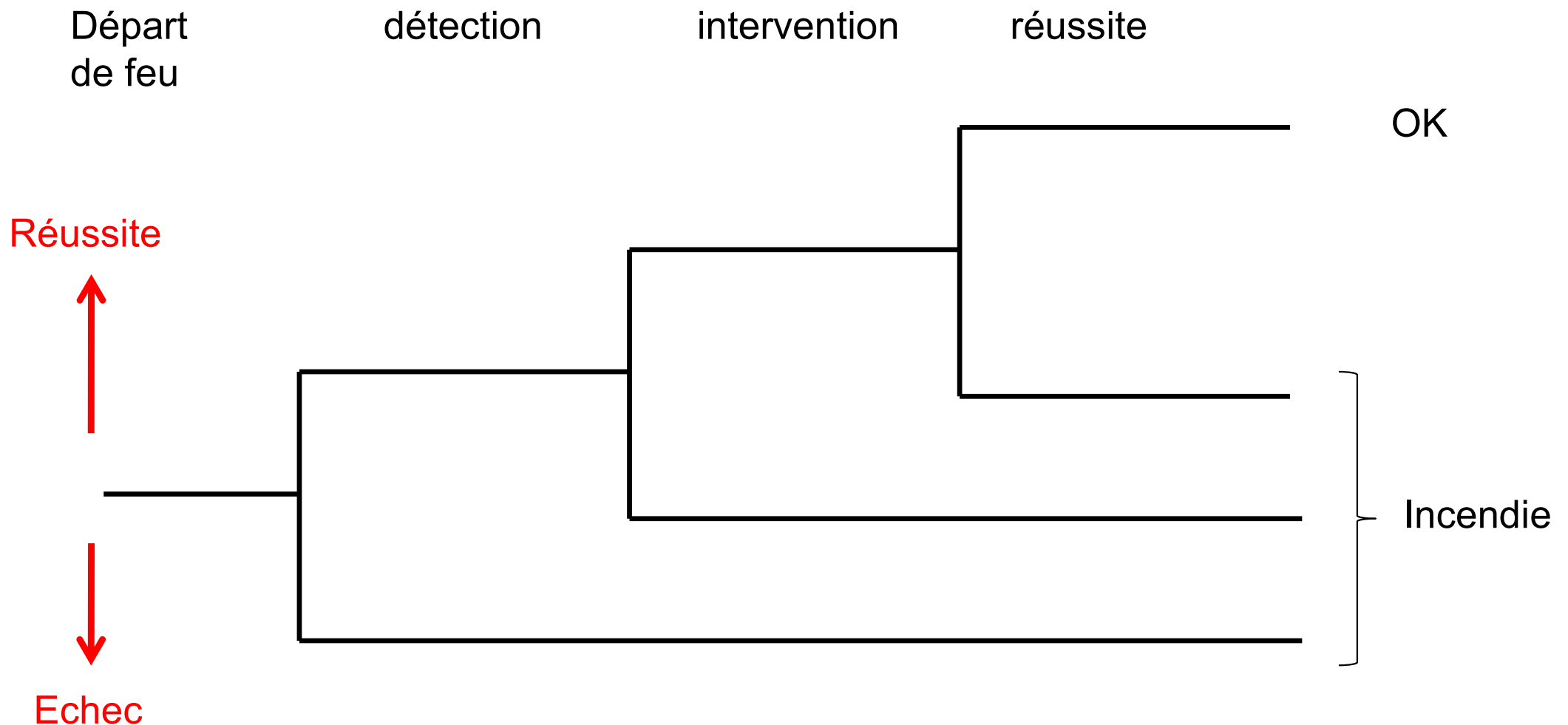
ICI

Décrire l'inéluctable pour définir des stratégies de lutttes contre les effets (« barrières » de protection)

Présentation

- Méthode élaborée début des années 70
(Rapport Rasmussen Wash-1400 (1975))
- Méthode inductive permettant une quantification
- Elaboration de scénarios à partir d'un événement initiateur et d'une cascade de réussites ou d'échec de moyen de sauvegarde

Intervention sur départ de feu



Mise en œuvre

1. Définir l'événement initiateur
2. Recenser les moyens de sauvegarde (matériels, humains, organisationnels)
3. Etablir la chronologie des interventions
4. Construire l'arbre
5. Eliminer les incohérences
6. Faire le calcul de probabilité

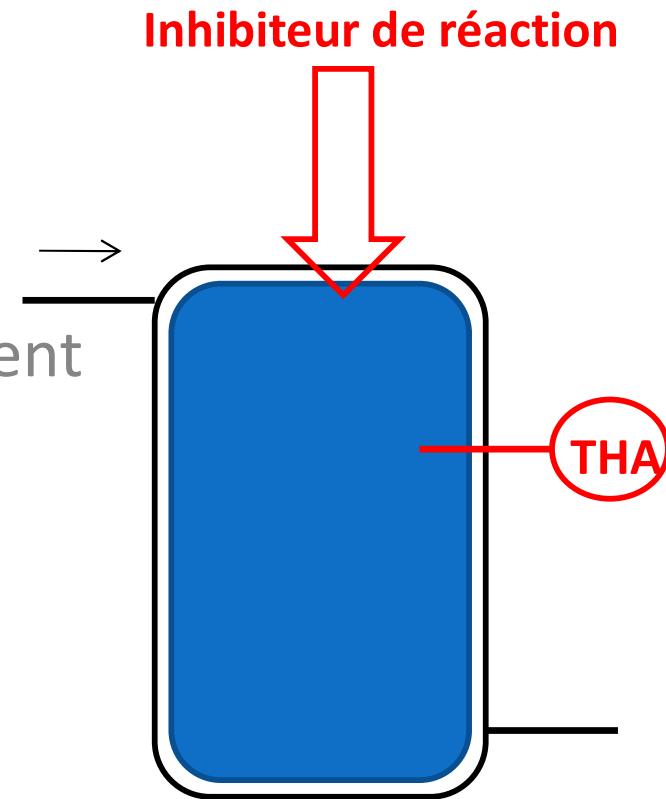


Exemple

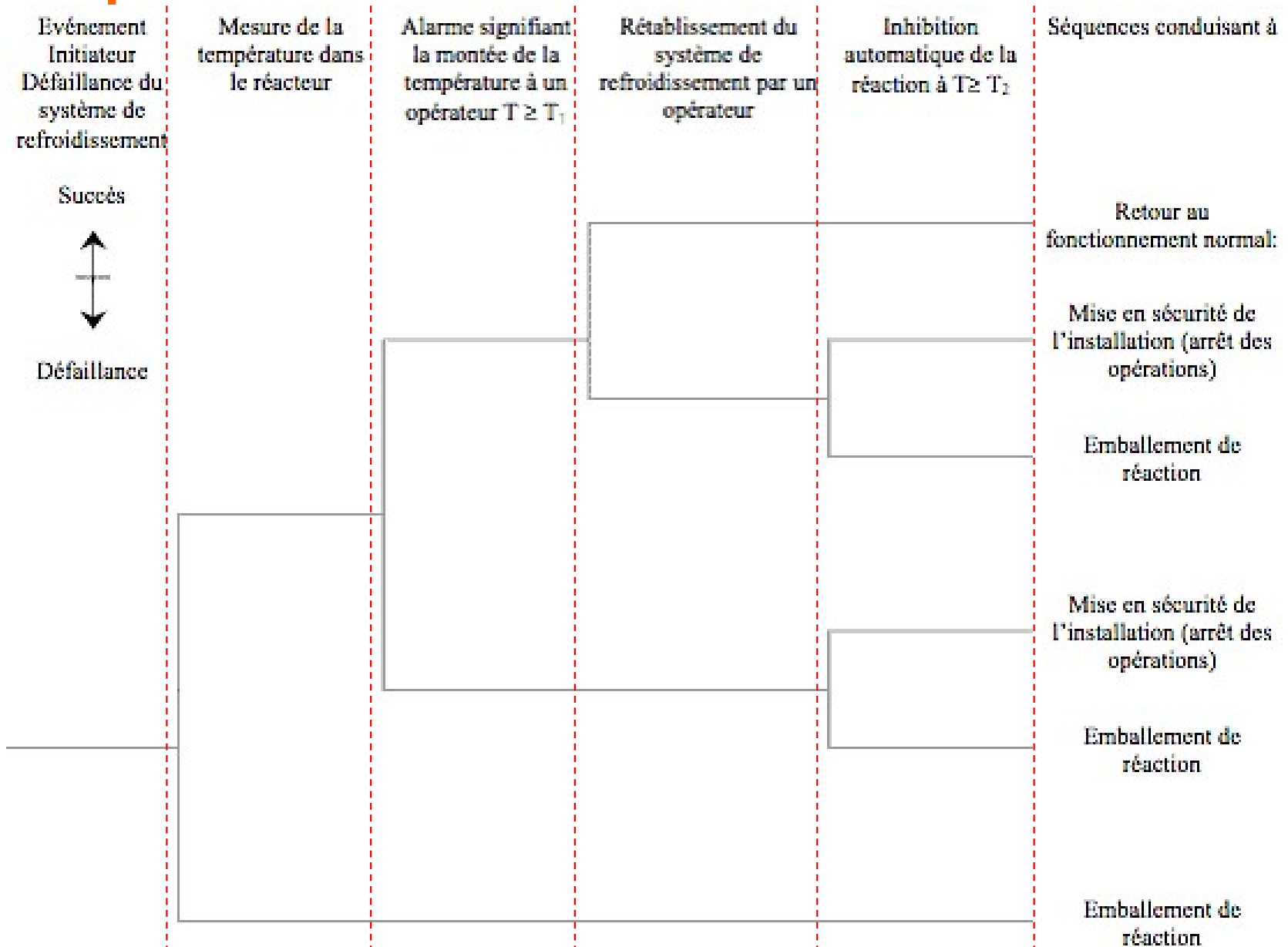
En cas d'arrêt du refroidissement, il y a une alarme de T° haute.

L'opérateur doit rétablir le refroidissement

S'il tarde ou échoue, le capteur déclenche une injection (en dernier recours) d'un inhibiteur de réaction



Exemple

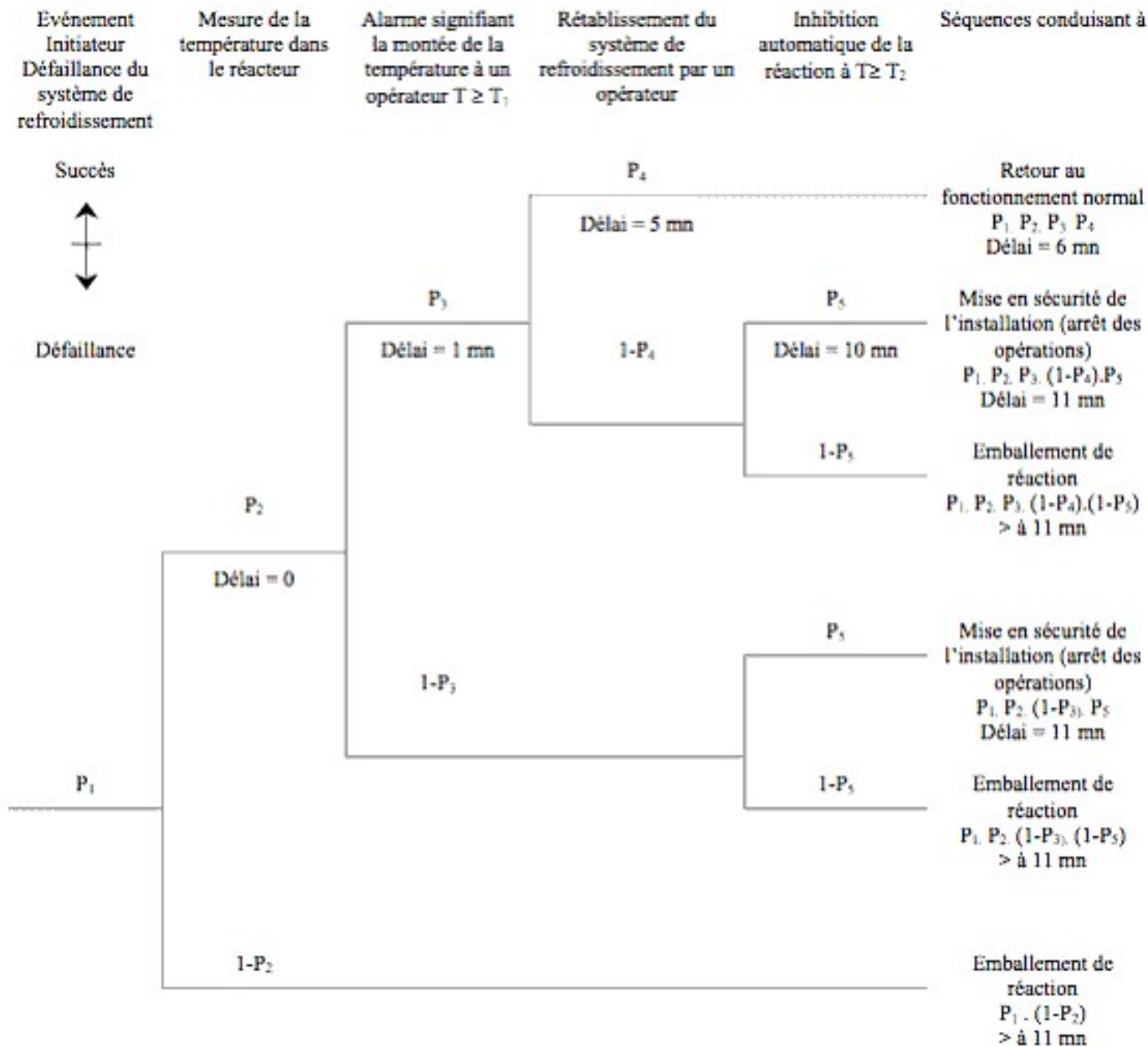


Principes à respecter

- Une fonction dépendant d'une autre
 - doit être considérée après celle-ci
 - Si échec de $f_1 \Rightarrow$ échec f_2 , le succès de f_2 n'est pas à étudier
- De même, une réussite interrompt une branche où d'autres éléments devaient intervenir
- Attention au défaillance de mode commun



Exemple quantifié



En conclusion

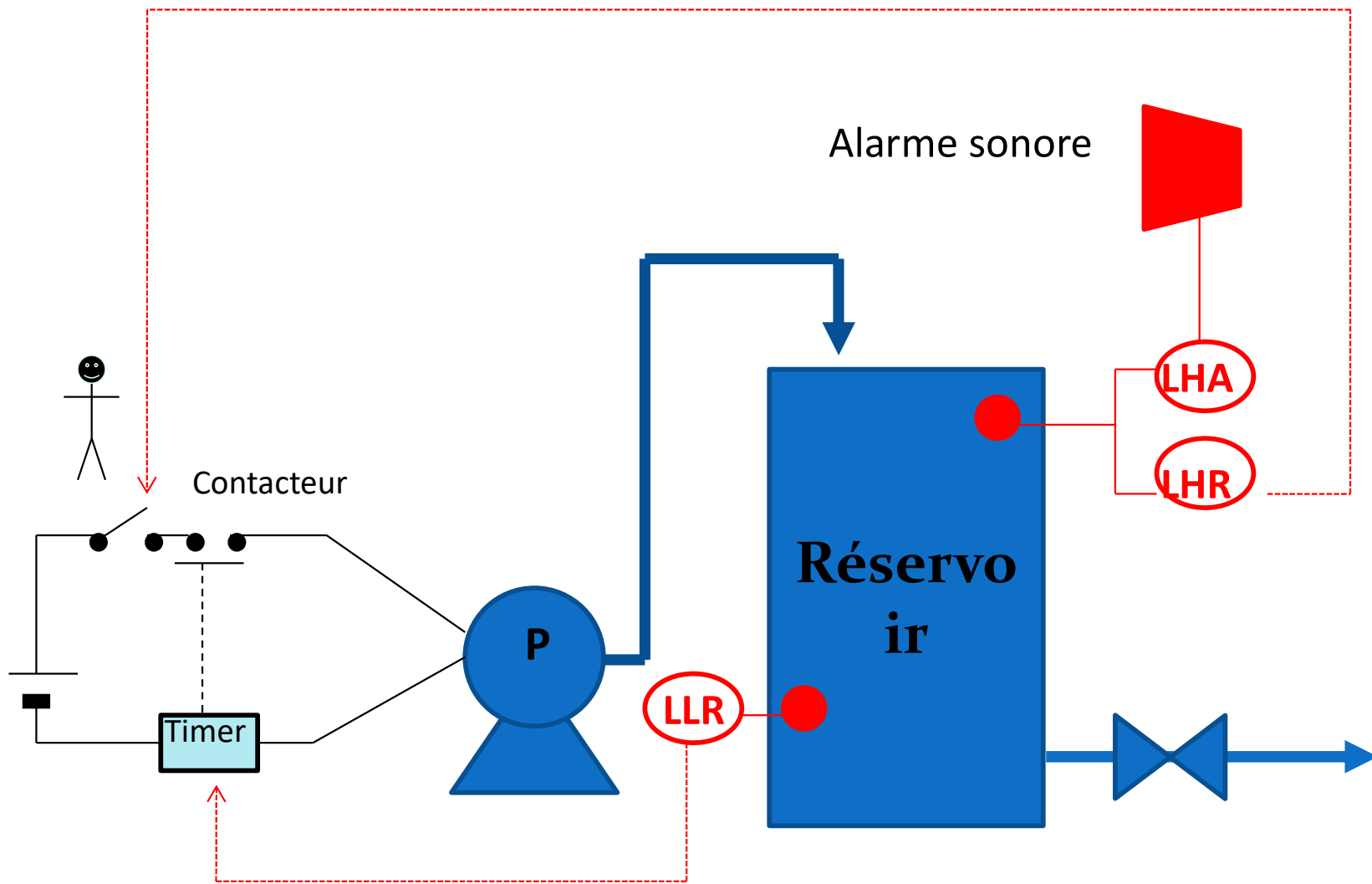
- Méthode pertinente pour formaliser des scénarios (et les « quantifier »)
- Usage fréquent lors d'analyse d'accident
- Attention : démarche rapidement lourde => bien cerner (et limiter) l'objet de l'étude.





Exemples


Plus proche d'une exploitation systématique
d'arbre des causes





Identifier :

- l'événement initiateur
- Les fonctions de sécurité

- 
- Événement initiateur : surremplissage
 - Fonctions de sécurité :
 - Détecteur
 - Régulateur
 - Interrupteur
 - Alarme
 - Opérateur

Construire l'arbre



Surremplissage

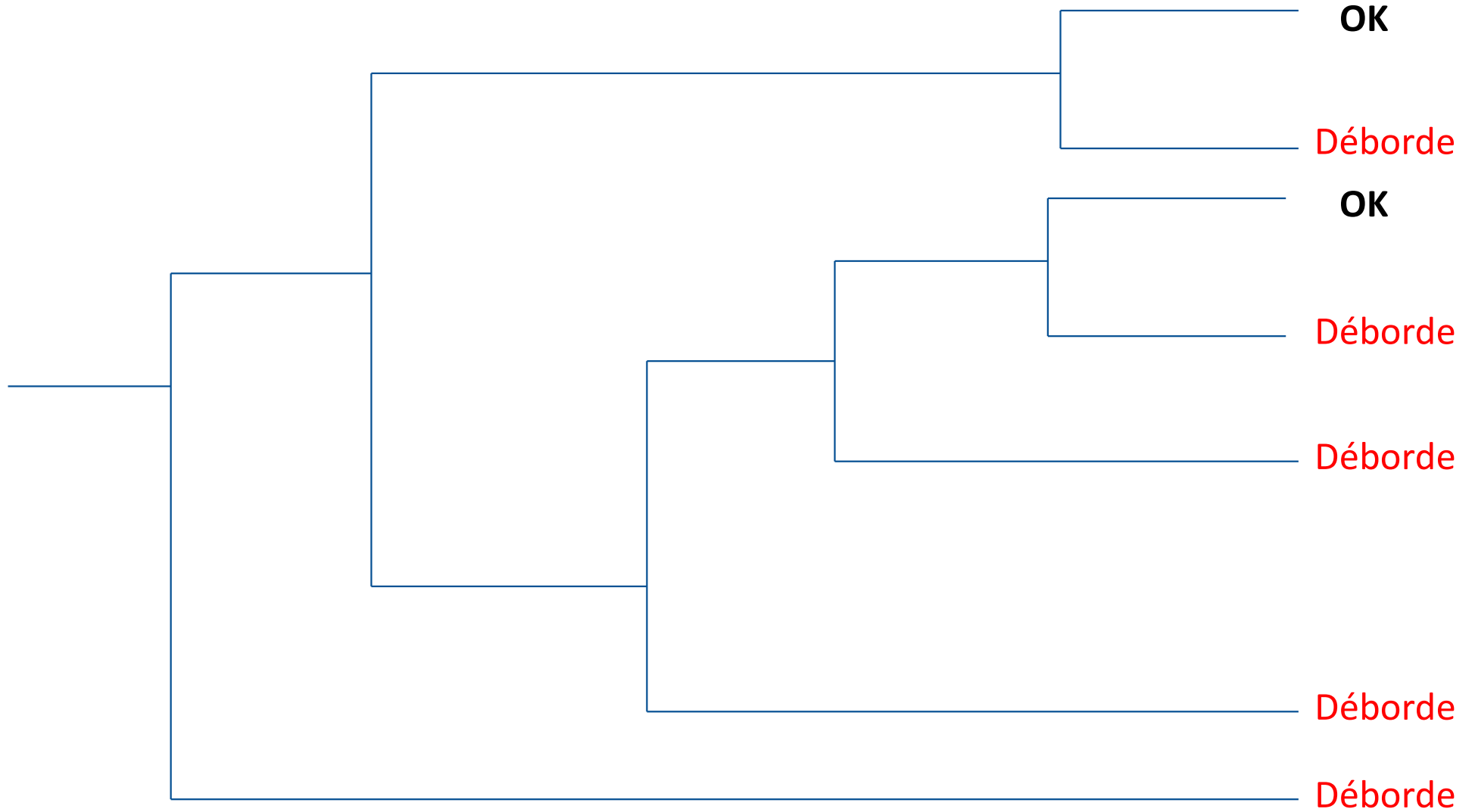
détection

régulateur

alarme

opérateur

interrupteur



calcul de probabilité

Défaillance détecteurs de niveau : 10^{-2}

Défaillance régulateur : $5 \cdot 10^{-3}$

Défaillance chaîne d'alarme : 10^{-2}

Interrupteur collé : 10^{-2}

Défaillance opérateur : 10^{-2}



Surremplissage

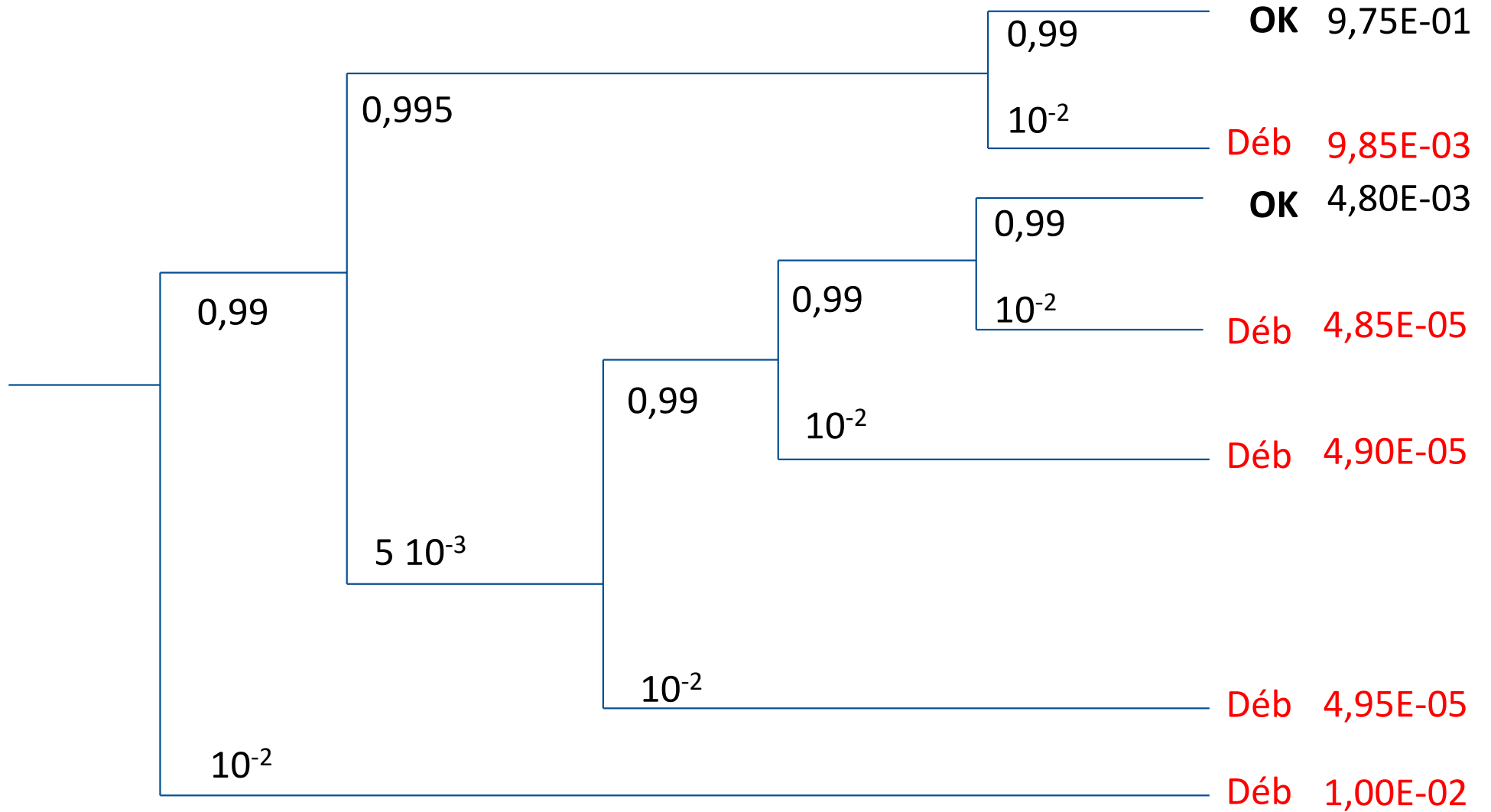
détection

régulateur

alarme

opérateur

interrupteur



P(OK) = 9,80E-01 P(Débordement) = 2,00E-02

(2,01E-02)