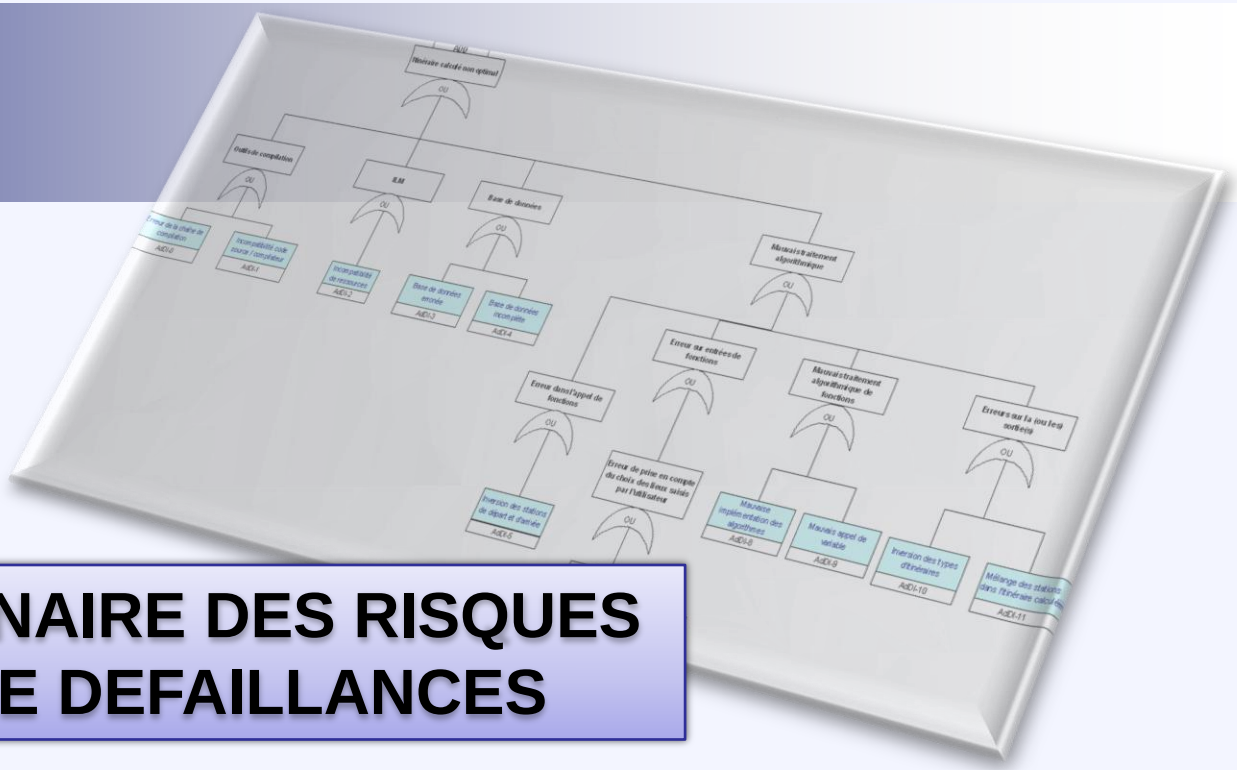
GENIE LOGICIEL



ANALYSE PRELIMINAIRE DES RISQUES
LES ARBRES DE DEFAILLANCES

Soutenu par :
Alain Bureau du Colombier
Hicham Chattou
Vathana Sitthisack
Erwan Cuinet

UNIVERSITE D'ANGERS

Master$_2$ Pro QUASSI
ISTIA – Dpt Qualité &Sûreté de Fonctionnement

INTRODUCTION

- ***Pourquoi le choix de ce sujet ?***

  - Avoir une vision plus proche de la démarche SdF
  - Approfondir nos connaissances

Sommaire

Projet

- *De Novembre 2006 à Février 2007*
- *Mise en application des cours (Génie logiciel, SdF logiciel/matériel)*
- *Outil disponible en salle E13 et bibliothèque de l'ISTIA*
- *Groupe de quatre étudiants.*

Travail à réaliser

- ***Étude générale des outils SdF:***

  → ***Analyse Préliminaire de Risques***

  → ***Arbre de Défaillance***

- ***Analyser et consolider la SdF de l'application POPE***

- ***Proposer des améliorations sous l'angle SdF de l'application.***

Sommaire

Historique APR

- ***développée au début des années 1960***
- ***domaines aéronautiques et militaires***
- ***l'identification des risques au stade préliminaire de la conception***
- ***méthode ne nécessite généralement pas une connaissance approfondie***

- ***2 cas d'application principale***

  - À la conception pour définir le procédé de fabrication
  - Dans le cas d'une installation complexe

Principe

- ***1 : Identification des élément dangereux***
  - Substances, équipements, opérations dangereuses
- ***2 : L'identification de ces éléments dangereux est fonction du type d'installation étudié***
- ***3 : déterminer les causes et les conséquences de chacune des situations de dangers identifiées***
- ***4 : identifier quelles situations nécessitent des propositions d'amélioration***

Déroulement

- ***Sélectionner le système ou la fonction à étudier.***
- ***Choisir un équipement ou produit pour ce système.***
- ***Considérer une première situation de danger.***
- ***Envisager toutes les causes et les conséquences possibles.***
- ***Identifier les barrières de sécurité existantes sur l'installation.***
- ***Si le risque est jugé inacceptable ➔ Amélioration.***
- ***Si tous les enchaînements ont été étudiés, définir une nouvelle situation de danger pour le même équipement.***

Limites et avantages

- ***Avantage :***
  - Permettre un examen rapide des situations dangereuses
  - Économique en terme de temps passé
  - Ne nécessitant pas un niveau de description détaillé du système

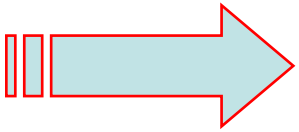
- ***Inconvénients, Limite***
  - Ne permet pas de décrire finement les enchaînement qui conduisent à un accident majeur (système complexe)
  - Nécessite l'utilisation ultérieure d'AMDEC ou Arbre de défaillances

APR sur Pope

Fonction externe	Modes de vie	Modes de défaillance potentielle	Risque global	Commentaires	Gravité	Gravité_num	Proba bilité	Probabilité_num	Moyens de prévention et de détection	Détectabilité	Détectabilité	Criticité	Evt redouté	Evt redouté
Affichage de l'itinéraire optimal	Exploitation	Dégradation de la fonction (sortie erronée)	Fiabilité		Critique	5	Moyen	3	Vérifier via des cas de test que le plan correspond bien à l'itinéraire calculé	Fort	1	15	ER1	Non affichage de l'itinéraire
		Absence de la fonction à la sollicitation (non réponse)	Fiabilité		Critique	5	Faible	1	Vérifier via 1 cas de test que l'on peut bien affiché un plan de l'itinéraire calculé.	Fort	1	5	ER2	Affichage érroné de l'itnéraire
"Cheminement" de l'itinéraire optimal	Exploitation	Absence de la fonction à la sollicitation (non réponse)	Fiabilité		Critique	5	Faible	1	Vérifier via 1 cas de test qu'il est bien possible de calculé un itinéraire	Fort	1	5	ER3	Non calcul de l'itinéraire optimum
		Dégradation de la fonction (sortie erronée)	Fiabilité		Critique	5	Moyen	3		Faible	5	75	ER4	Itinéraire calculé non optimal
Pertubartions sur les lignes	Exploitation	Dégradation de la fonction (sortie erronée)	Fiabilité		Majeure	3	Faible	1	Vérifier via 1 cas de test que si une station sur le chemin optimal est "bloquée" alors elle est contournée	Faible	5	15	ER5	Non possibilité d'ajouter des perturbations
		Absence de la fonction à la sollicitation (non réponse)	Fiabilité		Mineure	1	Moyen	3	Vérifier via 1 cas de test que l'on peut bien saisir des données	Moyen	3	9	ER6	Non prise en compte des pertubations
Chargement des données (stations, rues, …)	Exploitation	Dégradation de la fonction (sortie erronée)	Disponibilité		Critique	5	Faible	1	Vérifier via un auto-test que la liste des stations, rues, … disponible sous le logiciel correspond bien à celle de la base de donnée	Fort	1	5	ER7	Données non chargées ou mal chargées

Exploitation de l'APR

- ***Criticité constaté***
  - 5
  - 5
  - 5
  - 9
  - 15
  - 15
  - 75



Dégradation de la fonction :
Cheminement de l'itinéraire non Optimal

Sommaire

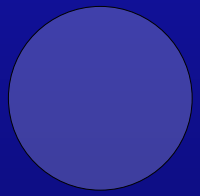
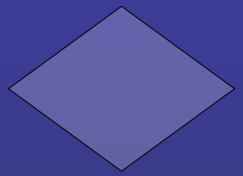
Historique

- ***1ère méthode d'examen des risques***
- ***~ 1960 → Système de tir de missiles***
- ***Déterminer les enchaînements menant à un événement redouté (E.R)***
- ***Aujourd'hui :***
  - aéronautique, le nucléaire, l'industrie chimique, …
  - Analyse d'accident à posteriori

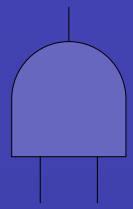
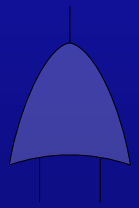
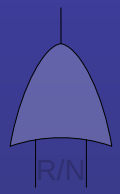
Objectifs et intérêts

- ***Déterminer les faiblesses du système.***
- ***Rechercher les combinaisons d'événements élémentaires qui conduisent à un événement redouté.***
- ***Représenter graphiquement les liaisons entre les ≠ événements.***
- ***Evaluer la probabilité d'apparition de l'E.R.***

Symboles utilisés - Evénements

	Événement redouté ou événement intermédiaire
	Événement élémentaire
	Événement élémentaire non développé

Symboles utilisés – Portes logiques

	Porte ET
	Porte OU
	Porte R/N

Déroulement

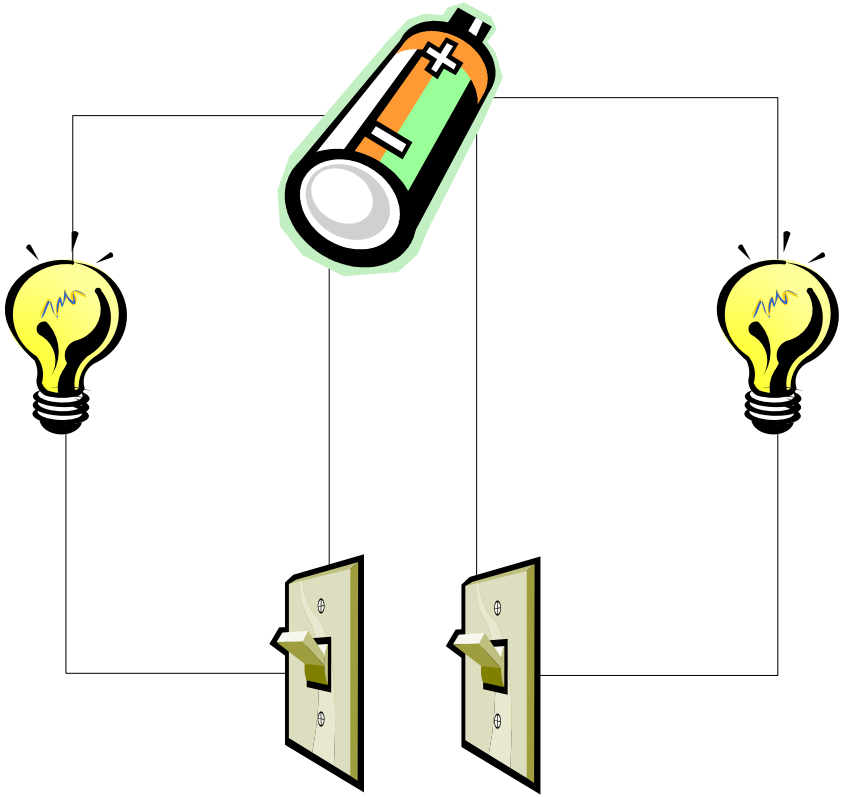
Identification des E.Rs par APR

Décomposition de chaque E.R en sous-événements reliés par des portes logiques

Décomposition des sous-événements jusqu'a obtention d'événements de base

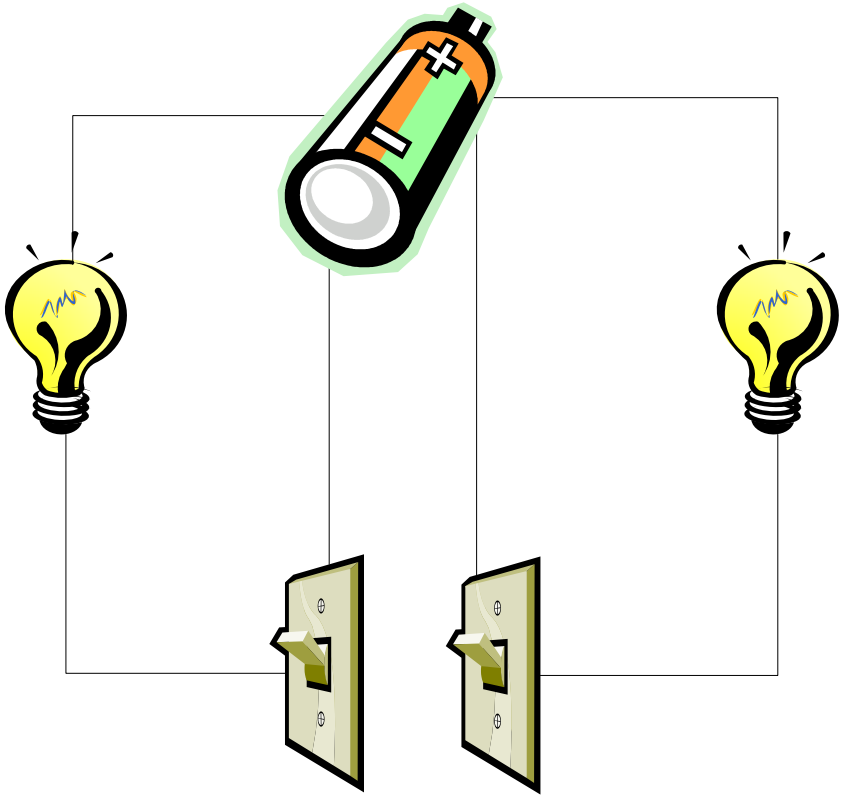
Identification des points faibles du système (coupe minimale, …)

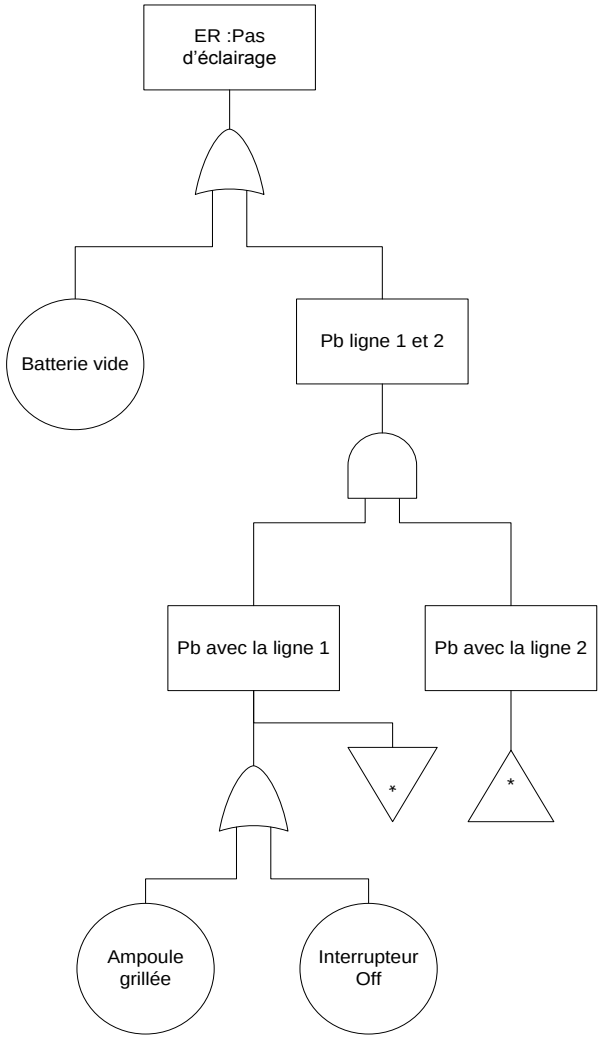
Exemple d'arbre de défaillances



E.R : Pas d'éclairage

Exemple d'Arbre de défaillances

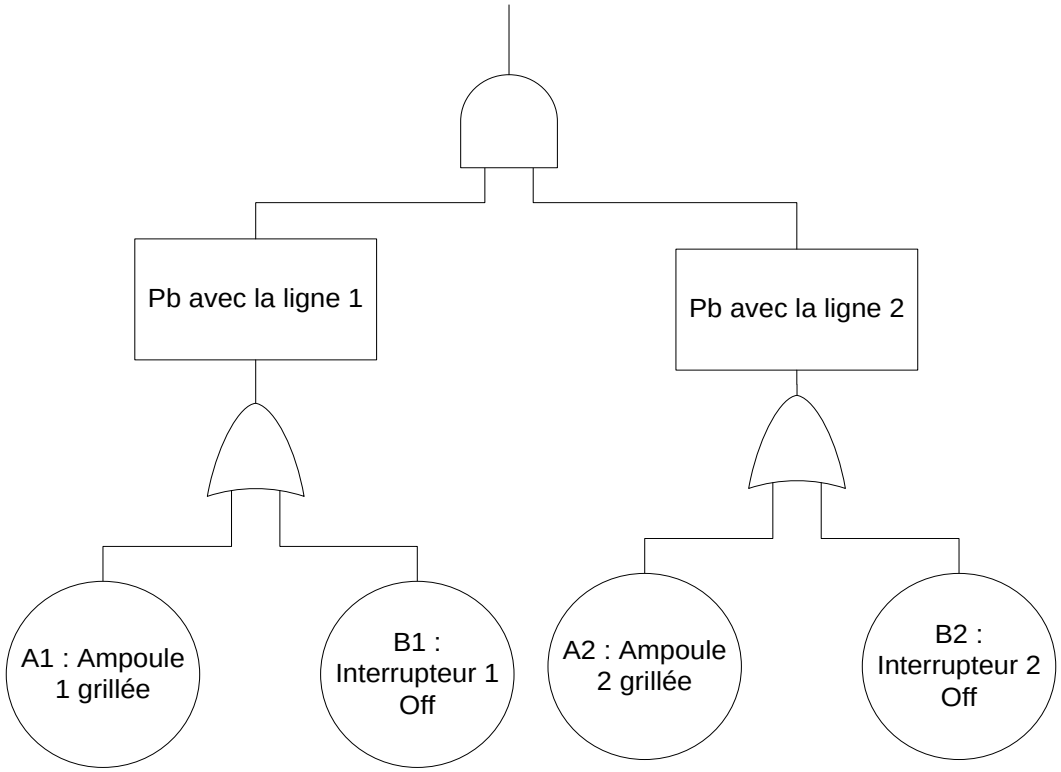




Arbre réduit 1/3

Propriétés	Produit (ET)	Somme (OU)
Commutativité	A . B = B . A	A + B = B + A
Idempotence	A . A = A	A + A = A
Absorption	A . (A + B) = A	A + A . B = A
Associativité	A . (B . C) = (A . B) . C	A + (B + C) = (A + B) + C
Distributivité	A . (B + C) = A . B + A . C	A + B . C = (A + B) . (A + C)

Arbre réduit 2/3

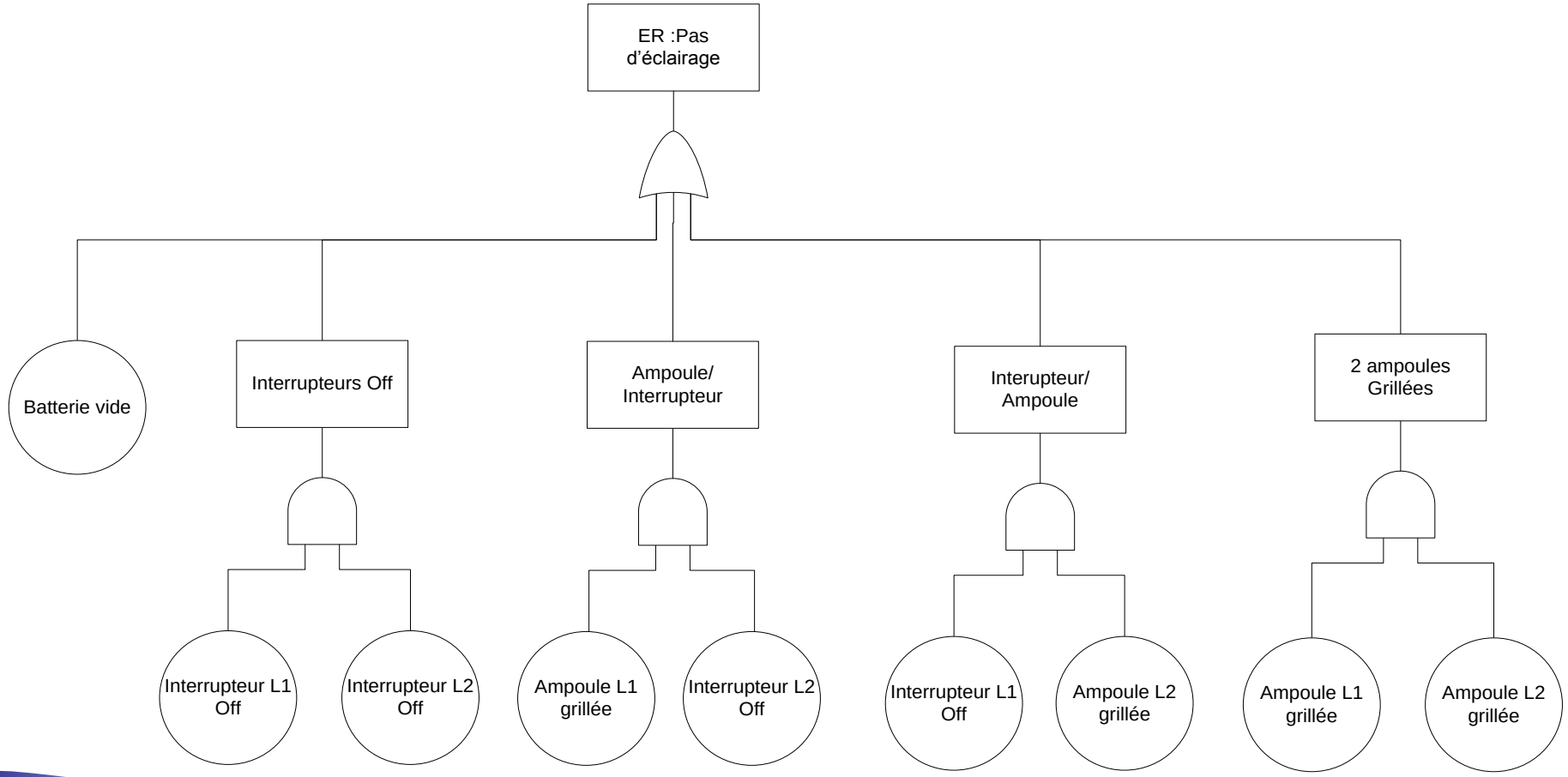


(A1 + B1) . (A2 + B2)

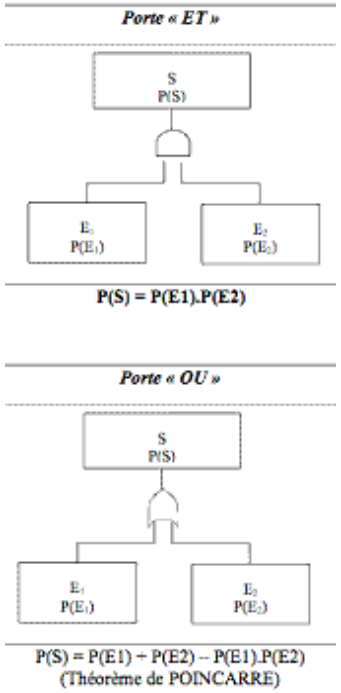
→(A1 + B1) . A2 + (A1 + B1) . B2

→ A1 . A2 + B1 . A2 + A1 . B2 + B1 . B2

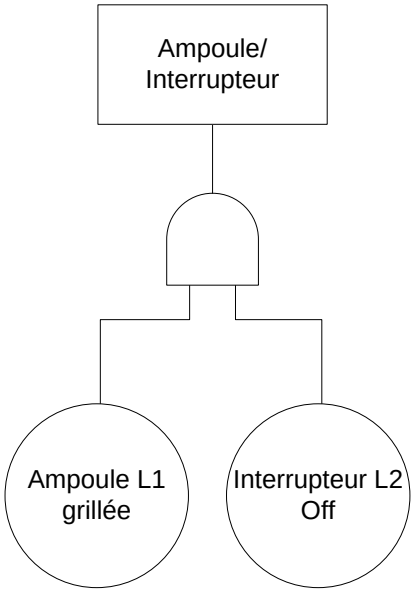
Arbre réduit 3/3



Estimation des probabilités 1/2

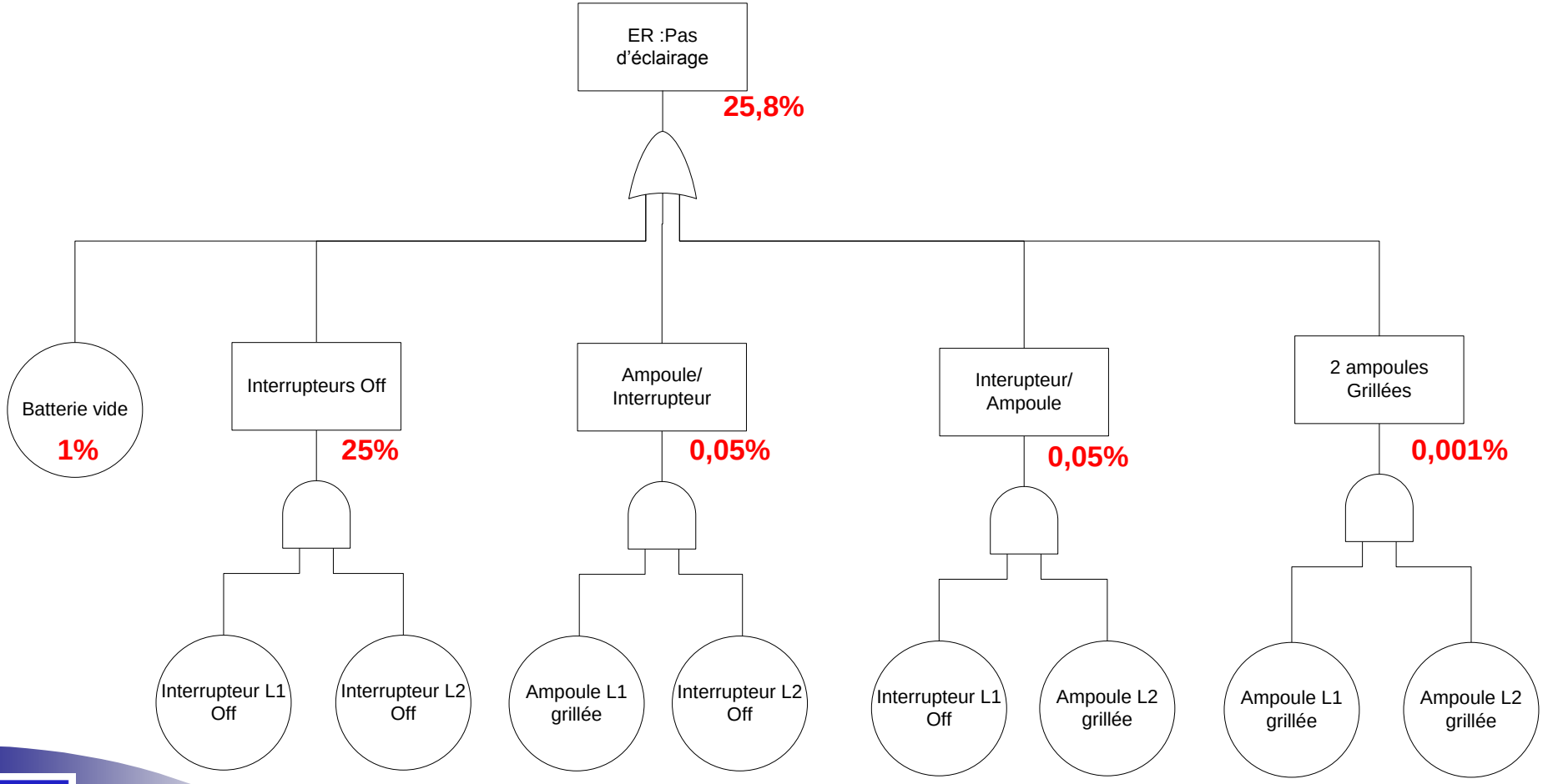


Probabilité :
Interrupteur off = 50%
Ampoule grillée = 1%
Batterie vide = 1%



Ampoule / Interrupteur = 1% * 50% = 0,5%

Estimation des probabilités 1/2



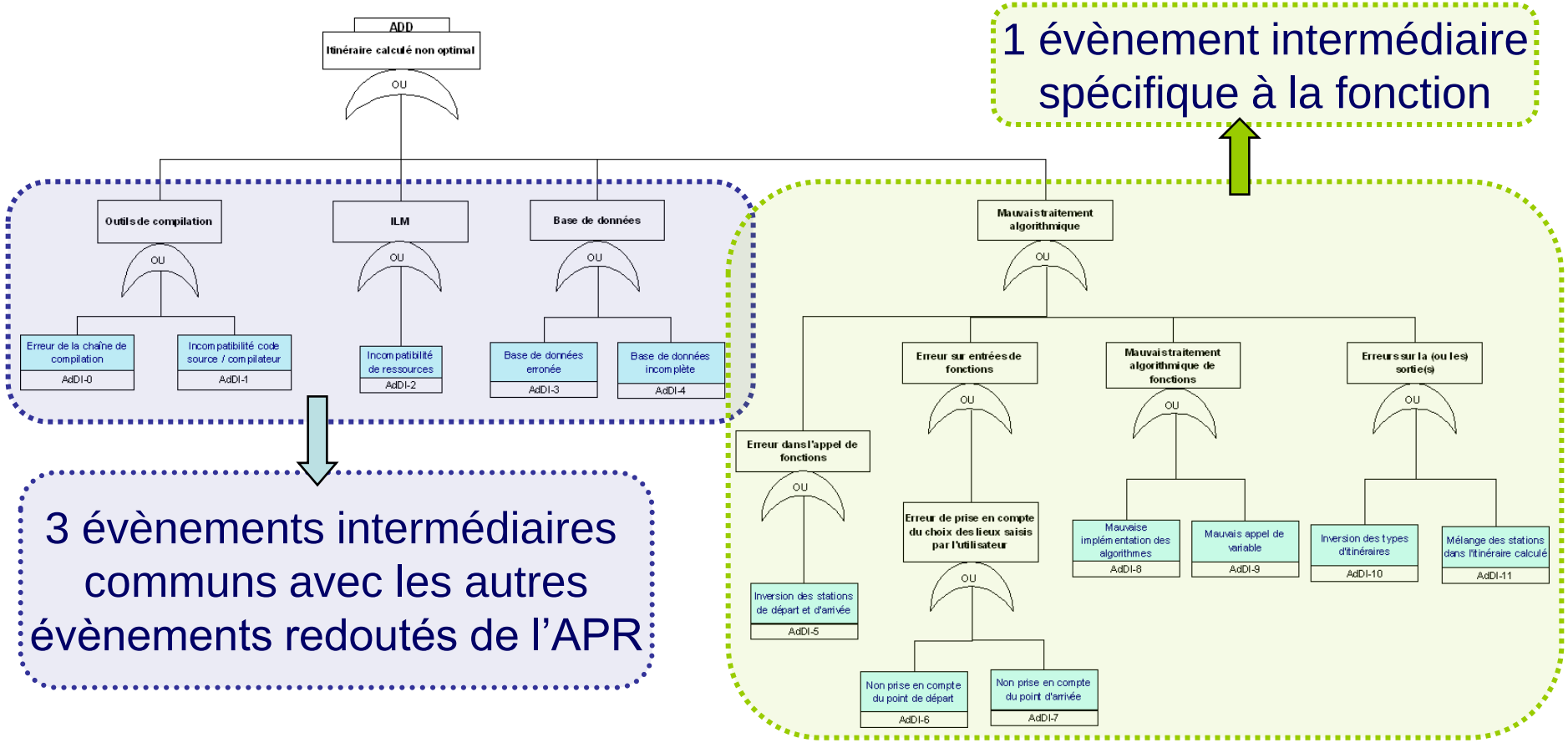
Sommaire

- ***1- Contexte***
- ***2- Analyse Préliminaire des Risques***
  - Théorie
  - Application sur Pope
- ***3- Arbre de Défaillances***
  - Théorie
  - Application sur Pope
- ***4- Améliorations proposées***
- ***5- Conclusion***

Application sur le logiciel Pope

- ***Évènement redouté : le calcul non optimal de l'itinéraire***
  - Fonction externe ayant la plus grande criticité
  - L'itinéraire proposé par le logiciel n'est pas le meilleur
  - 4 évènements intermédiaires indépendants à développer

Aperçu de l'Arbre de Défaillances



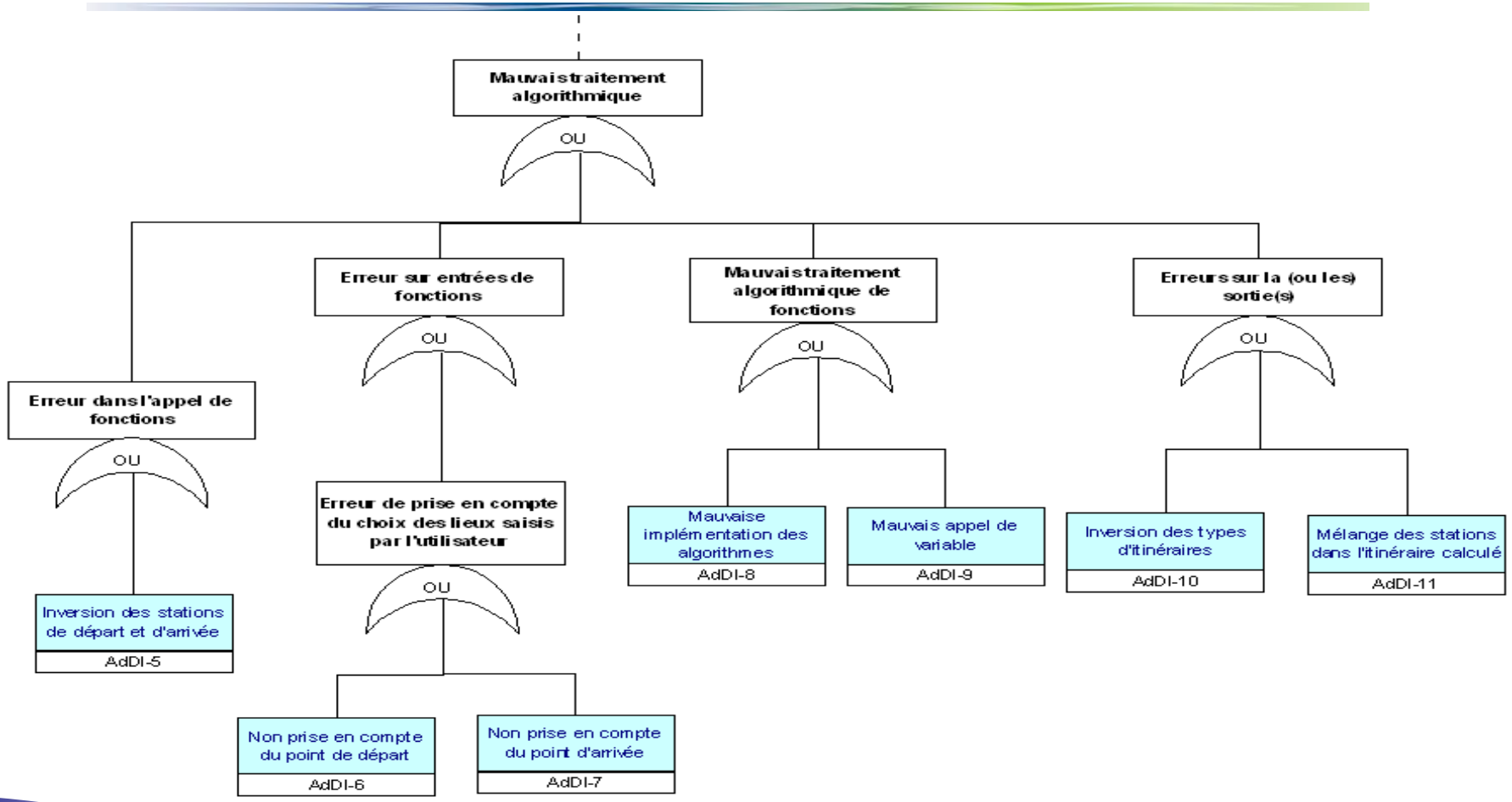
1 évènement intermédiaire spécifique à la fonction

3 évènements intermédiaires communs avec les autres évènements redoutés de l'APR

Les 3 évènements intermédiaires communs

- ***Les outils de compilation***
  - Erreur de la chaîne de compilation
  - Incompatibilité du code source avec le compilateur
- ***L' Interface Logiciel Machine (ILM)***
  - Incompatibilité des ressources
- ***La Base de Données***
  - Base de Données erronée
  - Base de Données incomplète

Mauvais traitement algorithmique



Sommaire

- ***1- Contexte***
- ***2- Analyse Préliminaire des Risques***
  - Théorie
  - Application sur Pope
- ***3- Arbre de Défaillances***
  - Théorie
  - Application sur Pope
- ***4- Améliorations proposées***
- ***5- Conclusion***

4- Améliorations proposées

- ***Ressources***
  - Vérification du matériel avant l'installation.
  - …
- ***Base de données***
  - Vérification des noms des stations par rapport à un plan du métro.
  - …
- ***Interface graphique***
  - E Affichage du nom des stations sur le plan…
  - …

4- Améliorations proposées

- **Fonctionnel**
  - Lors de l'affichage du plan reprendre dans un cadre les informations principales de l'itinéraire (point de départ, d'arrivée, temps, …)
  - …
- **Algorithmique**
  - Mettre en place un temporisateur pour éviter les boucles sans fin lors du calcul de l'itinéraire.
  - …

Sommaire

- ***1- Contexte***
- ***2- Analyse Préliminaire des Risques***
  - Théorie
  - Application sur Pope
- ***3- Arbre de Défaillances***
  - Théorie
  - Application sur Pope
- ***4- Améliorations proposées***
- ***5- Conclusion***

CONCLUSION

- ***Réduction des risques***
- ***Amélioration de la qualité globale***
- ***Optimal si effectué lors de l'analyse***
- ***Investissement « faible » → bénéfice important***

Merci de votre attention