

L'arbre des défaillances (FTA)

Source : <https://www.strategik.net/blog-iso-9001/arbre-des-defaillances/>

Définition

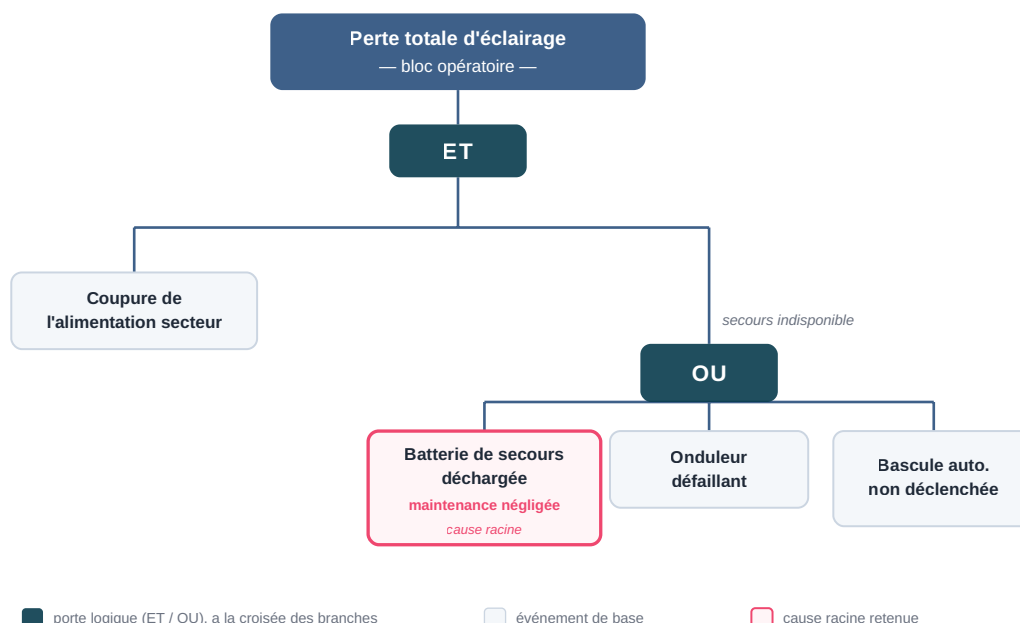
L'**arbre des défaillances** (ou *Fault Tree Analysis*, FTA) est une méthode **déductive** d'analyse de la sûreté de fonctionnement. On part d'un **événement redouté** placé au sommet, puis on descend pas à pas — via des **portes logiques ET / OU** — jusqu'aux **causes élémentaires**, appelées événements de base. C'est le pendant déductif (du haut vers le bas) de l'AMDEC, qui procède à l'inverse, de façon inductive (des causes vers les effets).

Finalités & valeurs ajoutées

- Mettre en évidence **toutes les combinaisons de causes** qui conduisent à un événement critique.
- Isoler les **coupes minimales** (les scénarios les plus courts menant à la défaillance) pour cibler les barrières les plus efficaces.
- **Quantifier** la probabilité de l'événement redouté lorsque les probabilités de base sont connues.
- Éclairer les décisions de **maîtrise des risques** : prévention, redondance ou surveillance.
- Fournir une analyse **visuelle et auditable**, exploitable dès la conception.

Exemple illustré

Événement redouté : la **perte totale d'éclairage d'un bloc opératoire**. Elle ne survient que si l'alimentation principale et l'alimentation de secours défontent en même temps (porte **ET**) ; le secours, lui, peut être indisponible pour plusieurs raisons (porte **OU**).



Lecture — la coupe minimale critique associe « coupure secteur » et « batterie déchargée ». Ce dernier événement, le plus probable et le plus évitable, désigne la **cause racine** : une maintenance de la batterie de secours négligée. **Action retenue** : test de décharge trimestriel + alarme d'état de la batterie.

Limites

- **Vision statique** : l'arbre capture mal les séquences temporelles et les dépendances dynamiques entre défaillances.
- Le résultat dépend de l'**exhaustivité des événements de base** : tout oubli le fausse.
- Les **défaillances de cause commune** (un même facteur touchant plusieurs branches) sont délicates à modéliser.
- La **quantification** exige des données de fiabilité souvent indisponibles ou incertaines.
- Un arbre = **un seul événement redouté** : couvrir un système complet en demande plusieurs.

À retenir

➔ **Déductive** (du sommet vers les causes), la FTA complète naturellement l'AMDEC, qui est inductive. Les **portes ET / OU** posent la logique ; les **coupes minimales** révèlent les points faibles à traiter en priorité. Un outil de maîtrise des risques rigoureux et auditable, d'autant plus utile qu'il est mobilisé **dès la conception**.