

# TD n° 3 : Estimation probabiliste de fiabilité des systèmes

---

*Master Ingénierie du Véhicule Electrique*

*Année 2021-2022*

*B. Monsuez*

## Analyse de la Fiabilité Humaine (HRA – Human Reliability Analysis)

Nous nous intéressons un système de monitoring du système de refroidissement. Ce système fonctionne à partir d'un ensemble de capteurs de technologie différentes et vérifie que la pression de l'eau d'un réacteur reste dans les limites prévues.

Ce système implante trois comparateurs qui doivent être calibrés, le système est en dysfonctionnement si les trois comparateurs sont mal calibrés ou ne fonctionnent pas correctement (OR).

Le système doit être calibré par un opérateur pour que l'ensemble des données retournées par chacun des comparateurs soient conformes.

Si l'opérateur initialise correctement le système de monitoring, il initialise correctement le premier comparateur, la probabilité de ne pas configurer correctement un des deux autres comparateurs est de 0.01, étant donné que les données fournies par le premier comparateur sont correctes.

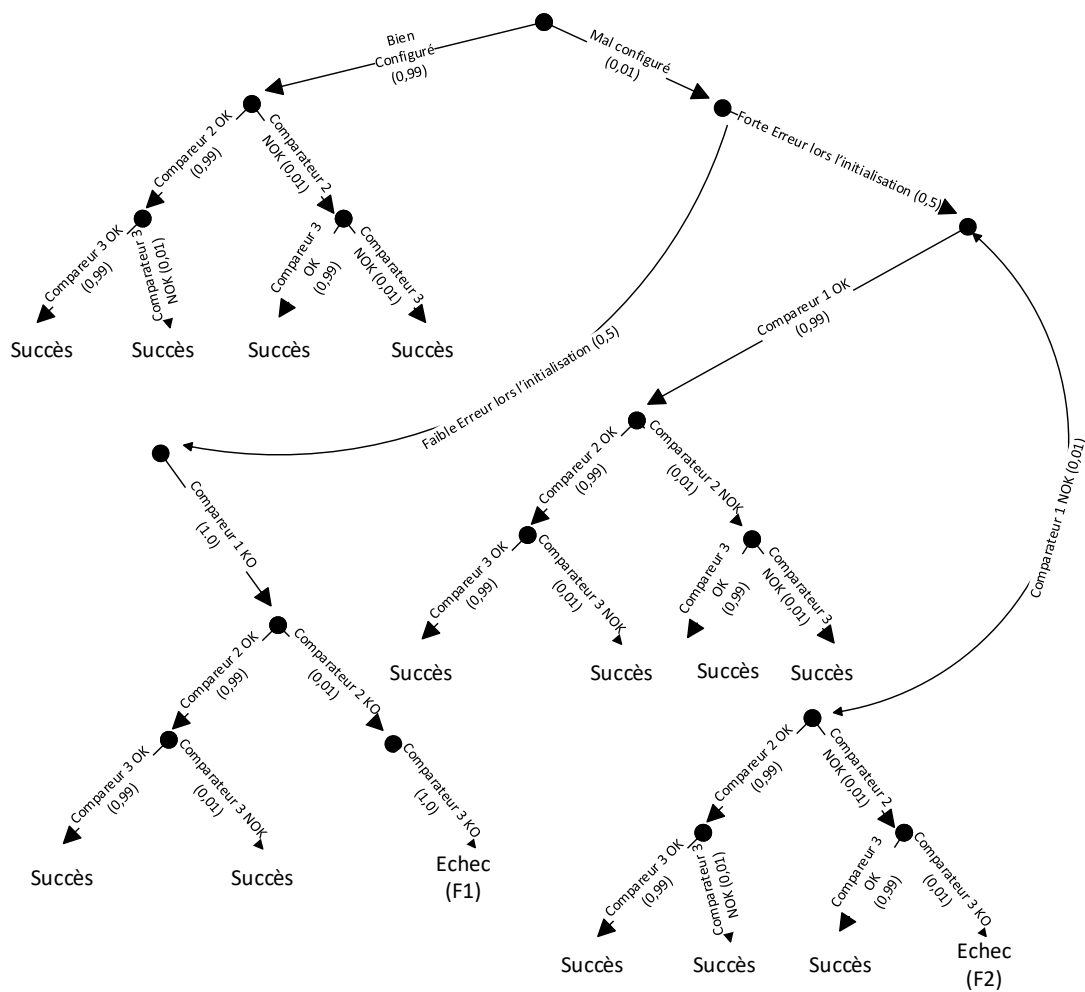
Si l'opérateur n'initialise pas correctement le système de monitoring, ce qui peut arriver avec une probabilité de 0.01, nous distinguons entre deux types d'erreurs d'initialisation qui sont équiprobables et qui ont des conséquences différentes :

Si le premier cas d'erreur (petite erreur de configuration) se produit, le premier comparateur ne sera pas correctement configuré. Cependant, la probabilité que le second comparateur ne soit pas correctement configuré sera faible parce que dans ce cas, configurer le second comparateur impliquera de reconfigurer le premier comparateur, du fait de la non-cohérence des values. De fait, la probabilité que le second comparateur soit mal configuré n'est que de 0.1. Enfin, si le second comparateur est mal configuré, la probabilité que le troisième comparateur soit mal configuré est de 1, puisque la cohérence sera vérifiée par rapport au deuxième ou au premier comparateur, aucun des deux n'étant bien configuré.

Si le second cas d'erreur se produit (forte erreur de configuration), la probabilité que l'un des comparateurs soit mal configuré est faible, l'opérateur se rendant compte que le calibrage est aberrant en calibrant le comparateur. De fait, nous considérons une probabilité de faute de 0.1 pour les deux premiers comparateurs. Si les deux premiers comparateurs sont mal configurés, par contre, nous sommes certains que l'opérateur configurera mal le dernier comparateur.

**Question n°1** : Etablissement d'un arbre de défaillance humaine et estimation de la probabilité de défaillance liée à l'action humaine.

**Question n°1.1 :** Construisez à partir de la description précédente l'arbre de défaillance des actions humaines.



**Question n°1.2 :** Identifier les états de fautes et calculer la probabilité que suite aux erreurs de calibration, le système ne soit pas en fonctionnel (ie. qu'aucun des comparateurs ne soit correctement configuré).

Il ne s'agit que des chemins amenant à un état de faute.

$$\Pr(F) = \Pr(F_1) + \Pr(F_2) = 0,0005 + 0,00005 = 0,00055$$

**Question n°2** : Prise en compte du stress et du niveau d'expertise.

Les tableaux suivant définissent l'impact du niveau de stress en fonction du niveau d'expertise :

Personnel Expérimenté		
Niveau de Stress	Modification de la probabilité d'erreur lors de l'exécution de la tâche	Impact sur les bornes d'incertitudes
Absence totale de Stress	2 * valeur de référence	2 * valeur de référence
Niveau Optimal	valeur de référence	valeur de référence
Moyennement élevée 1) Processus Séquentiel 2) Processus Dynamique	2 * valeur de référence 5 * valeur de référence	2 * valeur de référence 5 * valeur de référence
Très élevé	0.25	[0,03, 0,75]

Personnel Débutant		
Niveau de Stress	Modification de la probabilité d'erreur lors de l'exécution de la tâche	Impact sur les bornes d'incertitudes
Absence totale de Stress	2 * valeur de référence	2 * valeur de référence
Niveau Optimal 1) Processus Séquentiel 2) Processus Dynamique	valeur de référence 2 * valeur de référence	valeur de référence 2 * valeur de référence
Moyennement élevée 1) Processus Séquentiel 2) Processus Dynamique	4 * valeur de référence 10 * valeur de référence	4 * valeur de référence 10 * valeur de référence
Très élevé	0.25	[0,03, 0,75]

Nous considérons désormais les tâches suivantes qui doivent être réalisées par un opérateur :

- A) Lancement du monitoring de la pression et de la température. (P = 0.01)
- B) Lecture de la pression à partir du capteur de pression, (P = 0.06)
- C) Lecture de la température à partir du capteur de température, (P = 0.001)
- D) Comparaison de l'abaque de saturation avec les valeurs relevées de température et pression (P = 0.01)
- E) Augmente le niveau de refroidissement quand le point se trouve en dessous de la courbe (P = 0.01).

Nous considérons que les tâches A et E sont des tâches séquentielles, les tâches B, C, D des tâches dynamiques.

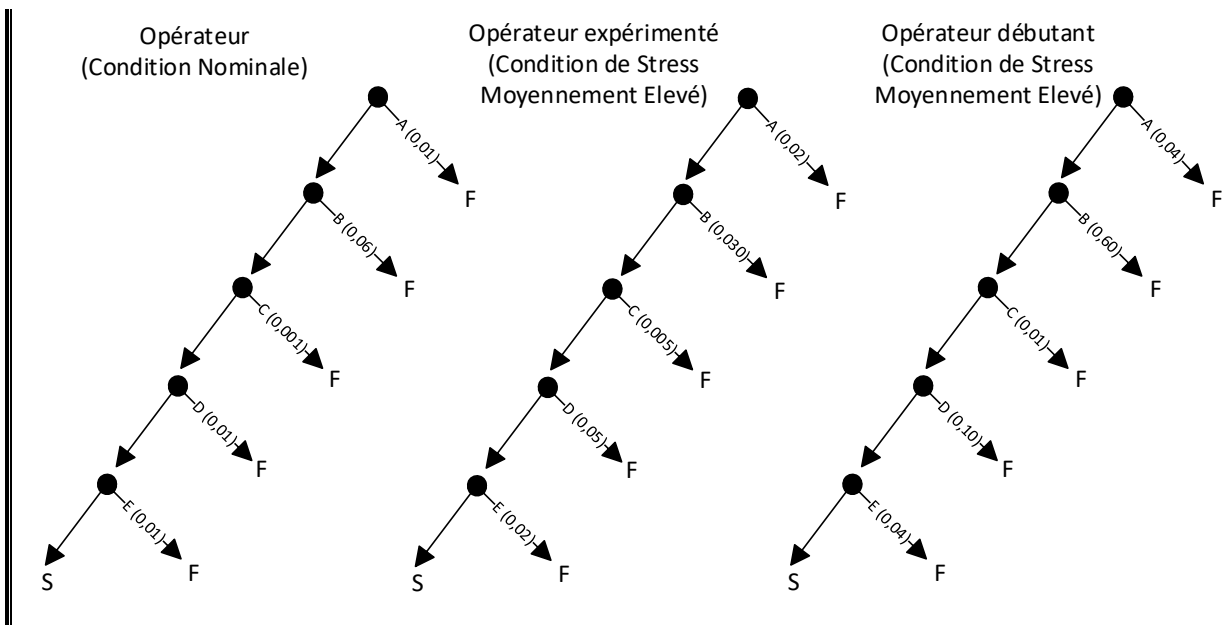
**Question n°2.1** : Caractériser le type d'erreurs possibles sur chacune des actions.

Le tableau suivant récapitule pour chacune des tâches les situations :

Tâche A	Oubli de la tâche Oubli de réaliser la tâche
Tâche B	Erreur de lecture

	Oubli de lire (prendre une valeur imaginaire)
Tâche C	Erreur de lecture Oubli de lire (prendre une valeur imaginaire)
Tâche D	Erreur d'Abaque Mauvais report sur l'Abaque
Tâche E	Oubli de réalisation Mauvaise réalisation

**Question n°2.2 :** Réaliser les différents arbres de défaillances pour des opérateurs en fonction des différentes situations.



Calculer la probabilité de défaillances dans la réalisation de la tâche.

Comme les actions sont séquentielles, l'échec sur une des sous-tâches entraîne un échec de la tâche. La probabilité de défaillance dans la réalisation de la tâche est donc égale à la somme des probabilités de chacune des sous-tâches allant de A à E.

Nous avons donc pour un opérateur dans des conditions nominales une probabilité de faute de :

$$\Pr\{F\} = 0,01 + 0,99 \times \left( 0,06 + 0,94 \times \left( 0,001 + 0,999 \times (0,01 + (0,99 \times 0,01)) \right) \right) = 0,089$$

Pour un opérateur expérimenté dans des conditions de stress moyennement élevé, nous trouvons une probabilité de faute de :

$$\Pr\{F\} = 0,02 + 0,98 \times \left( 0,30 + 0,70 \times \left( 0,005 + 0,995 \times (0,05 + (0,095 \times 0,02)) \right) \right) = 0,3675$$

Pour un opérateur débutant dans ces mêmes conditions de stress moyennement élevé, nous trouvons une probabilité de faute de :

$$\Pr\{F\} = 0,04 + 0,96 \times \left( 0,60 + 0,40 \times \left( 0,010 + 0,99 \times (0,10 + (0,090 \times 0,04)) \right) \right) = 0,6715$$

Si nous considérons les cas de stress très élevé, la probabilité de faute des opérateurs expérimentés ou débutants est de 1, puisque la probabilité de faute pour chacune des tâches est de 0,25.

$$\Pr\{F\} = 0,25 + 0,75 \times (0,60 + 0,40 \times (0,25 + 0,75 \times (0,25 + (0,75 \times 0,25)))) = 0,873$$

Soit une probabilité très proche de 1 en ce qui concerne des opérateurs en très haut niveau de stress.

**Question n°2.3 :** Supposons que nous n'avons pas un opérateur mais deux opérateurs.

Calculer la probabilité de faute en supposant que les actions des opérateurs sont indépendantes.

Si les actions des deux opérateurs sont indépendantes, pour qu'il y ait faute, il faut que les deux opérateurs commettent la même faute :

$$\Pr\{F\} = \Pr\{F_{Opérateur A}\} \Pr\{F_{Opérateur B}\}$$

Dans ce cas, nous avons pour les combinaisons d'opérateurs dans des conditions de stress moyennement élevé :

Opérateur	Opérateur A	Opérateur B	Défaillance combiné
Débutant + Débutant	0,672	0,672	0,451
Expérimenté + Débutant	0,365	0,672	0,245
Expérimenté + Expérimenté	0,365	0,365	0,133

**Question n°2.4 :** Supposons désormais que l'action consistant à oublier de lancer l'opération de monitoring de la pression de de la température est fortement dépendante (l'opérateur 2 surveille l'opérateur 1), calculer la probabilité de défaillance de l'opération.

Si les actions des deux opérateurs sont indépendantes, pour qu'il y ait faute, il faut que les deux opérateurs commettent la même faute :

$$\Pr\{F\} = \Pr\{F_{Opérateur A}\} \left( \frac{1 + \Pr\{F_{Opérateur B}\}}{2} \right)$$

Dans ce cas, nous avons pour les combinaisons d'opérateurs dans des conditions de stress moyennement élevé :

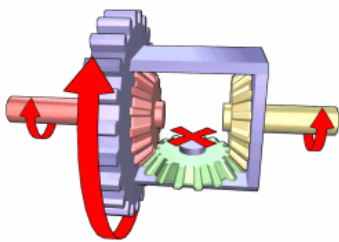
Opérateur	Opérateur A	Opérateur B	Défaillance combiné
Débutant + Débutant	0,672	0,672	0,561
Expérimenté + Débutant	0,365	0,672	0,305
Débutant + Expérimenté	0,672	0,365	0,458
Expérimenté + Expérimenté	0,365	0,365	0,133

## Définition d'un différentiel électronique

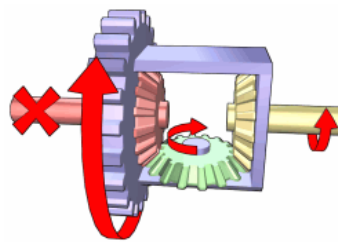
Nous considérons un robot à quatre roues dont les moteurs électriques sont des moteurs roues. Dans ce cas, il est nécessaire de contrôler les moteurs de manière indépendante afin de pouvoir modifier la vitesse de rotation dans les courbes à l'instar de ce que fait un différentiel mécanique, tout en fournissant en plus l'effort de traction.

**Question n°0 :** Expliquer schématiquement le fonctionnement d'un tel différentiel électronique.

Le différentiel mécanique a pour objet de répartir les vitesses de rotation sur chacune des roues, la roue intérieure tournant plus vite que la roue extérieure.



Les deux roues tournent à même vitesse, les engrenages rouges et jaunes tournent donc à la même vitesse, la roue verte ne tourne donc pas.



La roue gauche ne tourne pas, seule la roue droite tourne, l'engrenage vert tourne à la même vitesse que la roue jaune, permettant à la roue droite de ne pas tourner.

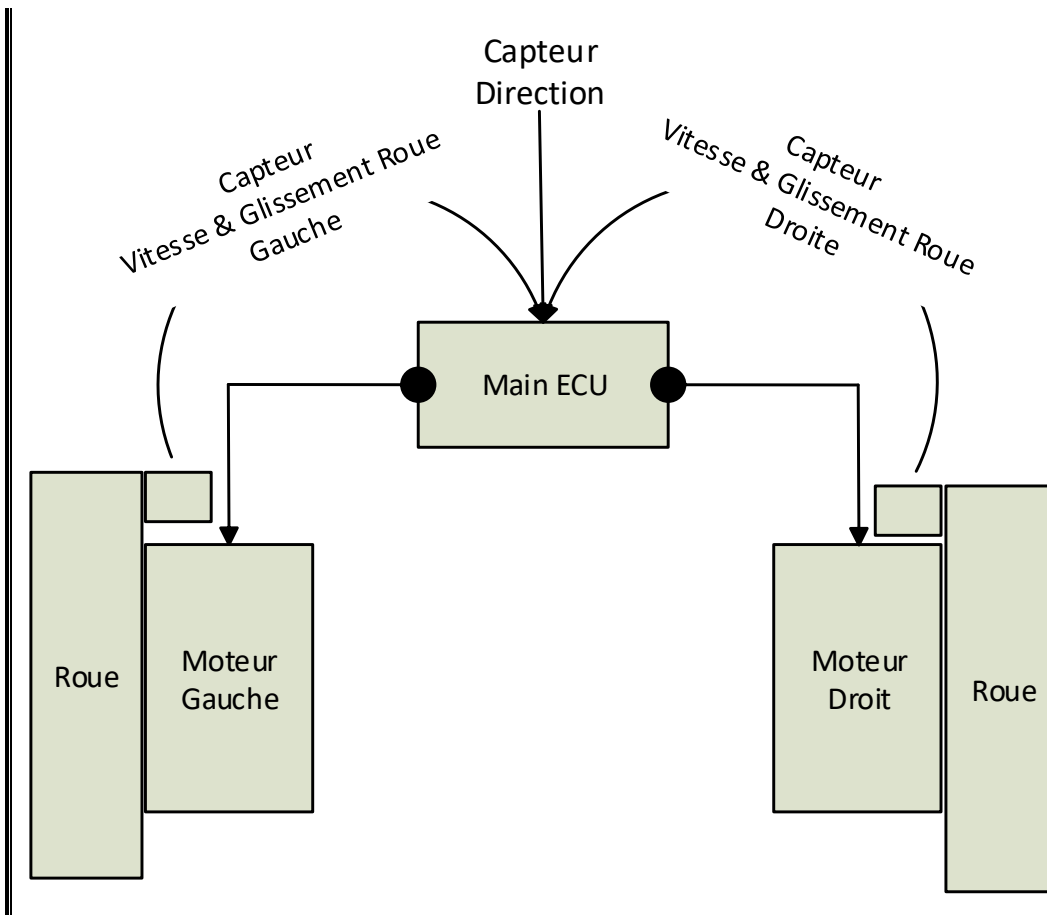
Le différentiel électronique a pour caractéristique de devoir effectuer cette même tâche, c'est-à-dire d'adapter la vitesse de chacun des moteurs roues à la vitesse que la roue doit avoir pour suivre la courbe.

Un défaut du différentiel mécanique est que même si les vitesses de rotation sont différentes, le même couple est appliqué sur les deux roues. Un différentiel électronique permettrait de moduler le couple en fonction de l'adhérence de la roue.



Figure 1: Différentiel Central de la Porsche Cayenne

**Question n°1 :** Proposer une architecture fonctionnelle pour un tel différentiel électronique.



**Question n°2 :** Quelle est la contrainte la plus forte sur un tel système ? Essayer de la quantifier ?

Le temps de réponse qui doit être suffisamment faible pour éviter que le robot se retrouve en tête à queue ou fasse une embardée, du fait d'une répartition inadéquate des vitesses de rotation sur chacune des roues.

Typiquement, le temps de réponse devra être de quelques ms à comparer aux  $\mu\text{s}$  qui sont typiques pour un différentiel mécanique.

**Question n°3 :** Quels sont les événements redoutés ? Déterminer leur gravité au regard de la grille normale de lecture.

Non-respect de la trajectoire

Grave ou Catastrophique

Perte de la motricité

Majeure

**Question n°4 :** Comment rendre un telle architecture robuste ?

Il est nécessaire de dupliquer complètement les chaînes de calcul et de traitement pour pouvoir assurer un niveau de fiabilité convenable, éviter les situations graves et catastrophiques.

