TD n° 3 : Estimation probabiliste de fiabilité des systèmes

Cours «Sûreté de Fonctionnement des Systèmes à Autonomie Décisionnelle »
Année 2020-2021

9 octobre 2020

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).

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.

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.

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.

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.

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.

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 ?

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

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

Question n°5 Torque Vectoring (A faire en dehors du TD): De fait, nous pouvons au contraire contrôler la différence de vitesse entre les roues pour soit amplifier le mouvement de rotation.

Expliquer comment il est possible de déclencher un mouvement de rotation du véhicule en ne jouant que sur la vitesse des roues.

Déterminer dans ce cas les évènements redoutés ? Déterminer aussi leur gravité au regard de la grille normale de lecture.

Question n°5 : Prise en compte du pilotage de l'humain.

Expliquer quel est l'interaction entre le système différentiel et les commandes initiées par l'humain.

Déterminer les risques pouvant naître de la latence de réaction du différentiel par rapport à la commande ?