Étude de cas Sûreté de Fonctionnement COMASIC/SLR 2019-2020

Ce sujet correspond au contrôle continu mis en place dans le cadre de l'évaluation de l'unité d'enseignement. Il compte pour 1/3 de la note totale.

Les réponses devront être rendues au plus tard mardi 21/01/2020 au soir (23h59 GMT+1) pour vous permettre d'obtenir un retour sur vos rendus avant l'examen.

Utilisez le lien suivant pour vous connecter au moodle : https://moodle.r2.enst.fr/moodle/mod/assign/view.php?id=824

Clés d'inscription : 2020

Le rendu se compose de texte et de modèles PRISM a priori.

I. Disponibilité d'un réseau en anneau (9 pts)

Dans cet exercice nous allons étudier la topologie réseau en anneau. On parle ici de topologie physique et donc de « câblage ».

Le but de cet exercice est de vous amener à utiliser les outils découverts en TD pour analyser et résoudre un problème.

Le modèle du système et ses défaillances.

Le principe d'une topologie en anneau est la suivante. Pour un ensemble de N machines nommées m_0,… m_{N-1}. Chaque machine m_i est connectée à m_{i-1} et m_{i+1} modulo N (ceci est la version simple qui fait abstraction de certains détails dans la constitution d'un tel réseau). En l'absence de connexions défaillantes (câbles rompus), les données circulent de machine en machine par le chemin le plus court. Ce modèle suppose que les câbles permettent des communications bi-directionnnelles. La pile réseau en charge du transport est munie de moyens de détection pour la perte de connexions entre un nœud et ses voisins directs. En cas de perte de connexion chaque nœud met à jour une table indiquant pour le nœud en question le prochain nœuds sur le plus court chemin pour chaque destination. On supposera que cette table se met à jour instantanément et sans erreur. Le réseau est déclaré défaillant pour les nœuds (m_i, m_j) si il est impossible d'établir un chemin de i à j. **Pour tout ce problème, nous supposerons que N=10.**

Question II.1 (1 pts)

Combien de câbles peuvent être rompus sans empêcher la transmission de donnée de la machine 0 vers la machine 4

- dans le pire cas (du point de vue de l'ingénieur en sûreté de fonctionnement)
- dans le meilleur des cas

Question II.2 (1 pts)

En supposant que le phénomène de rupture est indépendant de l'usage des câble :

- la date de rupture d'un câble dans cette architecture suit une loi exponentielle de paramètre L=0.00001 (pour une unité de temps correspondant à 1h),
- la rupture de chaque câble doit être vue comme un événement indépendant

Calculez la probabilité que les nœuds 0 et 4 restent connectés pendant 5 mois à partir d'un système totalement fonctionnel.

Processus de maintenance (modèles alternatifs)

Le processus de maintenance est modélisé de la manière suivante. Le temps nécessaire pour la réparation d'un câble rompu suit une loi exponentielle de paramètre m=0,0005 (même unité temps qu'auparavant). La détection de défaillance étant instantanée, le processus de maintenance est engagé dès qu'un câble se rompt. On supposera qu'il y a au moins autant d'équipes de maintenance que de câbles. Une connexion entre deux machines (mi, mj) est jugée défaillante si aucun des deux chemins possibles pour communiquer entre ces machine n'est fonctionnel. Le système est défaillant à partir du moment où il existe une connexion défaillante dans le système.

Question II.3 (3 pts)

Quelle est la probabilité maximale que le système soit défaillant pour un couple de machines durant 24h d'affilées. (Lors du rendu, donnez en même temps que la valeur, les éléments permettant de refaire le calcul : modèle et propriétés, pas les données...).

Question II.4 (3 pts)

Calculez la probabilité que l'indisponibilité d'une connexion entre deux machines soit inférieure dans le pire cas à 2h. Est ce la même pour tout couple de machines ? (Vous pouvez vous contenter d'échantillonner cette probabilité par tranche de 10 minutes et non en chaque instant.…). Donnez la valeur maximum de cette probabilité pour chaque paire de machine envisageable (un argument de symétrie peut être envisager pour rendre la réponse plus concise).

Question II.5 (1,5 pt)

Modifiez le paramétrage de votre modèle afin d'exprimer m en fonction de L et d'un ration multiplicateur r (caractérisant le rapport entre le taux de réparation et le taux de défaillance). Calculez le rapport minimal r permettant de garantir pour toute paire de nœuds qu'une indisponibilité supérieure à 2h a une probabilité inférieure à 0.001 pour un temps moyens de rupture de câble de 10000 heures.

Question II.6 (1,5 pt)

Si l'on augmente L d'un ordre de grandeur, comment évolue r ?

II. Raisonner sur plusieurs modèles (6 pts)

Nous souhaitons modéliser le temps d'exécution d'un système puis réutiliser cette modélisation dans un modèle d'étude de la fiabilité à la demande. Supposons que l'on souhaite modéliser le comportement d'une méthode d'analyse de modèle connue pour ne pas avoir de preuve de terminaison. Cette application repose sur l'exécution séquentielle de trois fonctions qui ont des temps d'exécutions caractérisé par une loi exponentielle de temps moyens de terminaison T1=100min, T2=50min et T3=50min dans le cas où le calcul peut se terminer. On estime que la fonction a rencontré une défaillance lorsque le temps d'exécution de chaque étapes est 5 fois supérieur à son temps moyen.

Question I.1 (2pts) Utilisez un modèle à temps continu pour évaluer la probabilité pour chaque fonction que sur une exécution, son comportement soit jugé défaillant ?

Question I.2 Supposez maintenant que la fonction a un comportement en partie aléatoire qui garantit que même ré-exécutée sur les mêmes données les temps d'exécution sont indépendants. Fournissez un modèle qui permette

1. (2 pts) D'évaluer la probabilité que l'application s'exécute sans ré-exécution des fonctions sur défaillances (i.e. l'application défaille si une fonction défaille)

2. (5 pts) D’évaluer la probabilité que le temps d’exécution de l’application soit inférieure à une borne temporelle exprimée en multiples de 50 min supérieure à 1000 min.