Etude de cas Sureté de Fonctionnement COMASIC 2016-2017

Consignes et critères d'évaluation :

Le sujet étant communiqué une semaine à l'avance, les réponses devront être rendues le jour de la séance prévue pour réaliser le TD étude de cas. Certaines questions nécessitent une réponse rédigées, d'autres reposent sur la création de fichiers (modèles prism, courbes). Vous pouvez rédiger les réponses sur papier ou au format électronique (rendu sous forme de fichier pdf si possible).

Les rendus sont individuels, il n'est cependant pas interdits de discuter du sujet en séance (un copier pur et simple des réponses n'est pas accepté).

Thèmes couverts par l'étude de cas : le cours sur l'analyse quantitative et les mécanismes de tolérance aux fautes lors de la comparaison de différentes architectures en fonction des modèles de défaillances choisis.

Nous supposons le TP prism précédant terminé. La précision des réponses rédigées sera évaluée (nous serons indulgents sur l'expression mais pas sur les arguments).

I. Disponibilité fiabilité d'une calculateur embarqué

Dans cet exercice, nous allons évaluer la fiabilité et la disponibilité d'une architecture primaire-secondaire (ou primary backup).

Nous étudions une fonction implémentée par un unique composant logiciel qu'il est possible de répliquer. Nous souhaitons implémenter une réplication passive reposant sur l'hypothèse que le logiciel n'a qu'un mode de défaillance : défaillance silencieuse.

Cette défaillance est de plus réparable via un redémarrage du calculateur sur lequel le logiciel est exécuté, et un chargement d'une configuration valide précédente. Cependant, le redémarrage peut pendre un temps variable (en fonction des éléments devant être restaurés). Nous supposerons dans un premier temps que le matériel est parfait.

Modélisation :

- le temps moyen jusqu'à la première défaillance d'une réplique est connue et correspond à 1500 s. Le temps jusqu'à une première défaillance sera modélisé par une variable de loi exponentielle
- le temps moyen d'un redémarrage est de 30 secondes : ce temps sera modélisé par une variable de loi exponentielle.

L'exécution d'une instance du service rendu par la fonction répliquée nécessite au pire trois quarts d'heure.

Question 1 (modélisation) Réalisez un modèle pour une architecture composée de deux répliques représentées par une unique chaine de Markov à temps continue. On supposera que seul le primaire peut défaillir mais que les nœuds ayant défaillis redémarrent de manière indépendantes (i.e. leur taux s'additionnent)

Correction possible (déjà généralisée)

```
ctmc
const double lambda =1/1500;
const double mu=1/30;
const int N=4;
// s : nombre de nœuds fonctionnels 0 => défaillants
module primarybackup
  s: [0..N] init N;
  [] s>0 -> lambda:(s'=s-1); // seul le primaire defaille
  [] s<N -> (N-s)*mu:(s'=s+1); // chaque défaillant peut se réparer
endmodule
```

Vous allez maintenant généraliser votre modèle afin de répondre à une question concrète d'ingénierie.

Question 2 (Expliquez comment vous procédez en indiquant les formules/ modèles utilisés) Trouvez le plus petit nombre de répliques assurant que si toutes les répliques sont fonctionnelles alors la probabilité que le système deviennent défaillant lors de l'exécution d'une instance du service est inférieure à 10^{-5}.

Correction :

La généralisation repose sur le fait que PRISM énumère les états et collecte l'ensemble des transitions par état : ici pour 0<s <N il y aura donc 2 transitions de sortie : 1 pour la défaillance et une pour la réparation.

Une instance dure 2700 secondes. Si l'état 0 est atteint entre 0 et 2700, cela signifie que plus aucune réplique ne conserve l'état du service courant => défaillance. La propriété à évaluer pour trouver ceci est : P<= 0.00001 [F[0,2700] s=0]. La plus petite valeur de N rendant cette formule vraie est 4.

Question 3 (réflexion) Que faut il calculer pour déterminer la proportion du temps moyenne pendant lequel le système serait défaillant (en faisant l'hypothèse d'un intervalle de temps très grand)?

Correction :

la probabilité stationnaire de la chaine.

Donnez la valeur trouvée pour l'architecture correspond à la question 2.

Supposons maintenant que chaque réplique lors d'une défaillance à une probabilité $p=10^{-3}$ d'être définitivement défaillante.

Question 4 Tracez la courbe représentant la probabilité que l'architecture ne soit pas capable de rendre le service à la date T (on prend toujours le pire cas e.g. le service dure 2700 s, et le service n'est pas rendu dès qu'aucune réplique n'est plus disponible).

Trouvez la valeur de T telle que cette probabilité devienne égale à 10^{-3}

Correction : la valeur en soit importe moins que la méthode de détermination. Pour trouver la valeur, il faut fixer la propriété P= ? [F[0,T] s=0]., avec T une constante non initialisée. Puis vous réalisez une expérience avec T variant de 1000 à 80000 avec un pas de 50 (cela devrait suffire). La valeur se trouve sur l'intervalle.

II. Exercice 2

Nous allons dans cet exercice évaluer une architecture mélangeant réplication active et calculateur de backup (dits spares). C'est une architecture classique d'une commande de vol civile. Cet exemple est volontaire irréaliste sur les durées.

On suppose un modèle de faute byzantin avec une probabilité instantanée de défaillance constante égale à 0.00001 (pour des unités de temps en ms). Ceci modélise un processeur réalisant des erreurs de calcul de temps en temps (indépendamment de la correction du code exécuté). Une tâche périodique est un modèle d'exécution supposant qu'une même séquence de code, appelée le corps de la tâche, est répétée non pas dans une simple boucle mais de telle sorte que chaque itération soit exécutée dans un intervalle de durée fixe T (la période de la tâche). Ainsi, une tâche de période 10 ms verra son corps exécuté une première fois entre 0 et 10 ms, puis une autre fois entre 10 et 20 ms

Question 1 Expliquez pourquoi le modèle de taux de défaillance constant peut être interprété efficacement pour calculer la probabilité de défaillance d'une tâche lors de l'exécution de son corps (1 fois), quelle information est nécessaire ?

Question 2 Construisez le modèle d'une réplique, utilisez ce modèle pour déterminer la probabilité de défaillance d'une tâche de période 500 ms ayant une durée d'exécution 100 ms fixe (pour son corps).

Question 3 Déterminer la probabilité que l'architecture TMR puisse être défaillante 3 périodes d'affilées (on supposera que chaque réplique se répare automatiquement après une exécution. (donnez la valeur). Vous choisissez le modèle adéquat pour exploiter l'information précédente.

Hypothèse : on va supposer maintenant que le processeur peut de plus défaillir définitivement avec une probabilité instantanée 0.0000001

Question 4 Déterminez combien de composant de rechange faut il pour assurer que le TMR sera fonctionnel 10h d'affilées avec une probabilité $1\text{-}10^{-3}$