M2 COMASIC
Examen de Sureté de Fonctionnement
30/01/2017

Durée de l'examen 3h.

Consignes particulières : les documents sont interdits à l'exception d'une feuille A4 manuscrite recto verso. Les téléphones portables doivent être rangés. Le présent examen est noté sur 20 pts. Le barème est indiqué devant chaque question.

I Principes de la sûreté de fonctionnement (4 pts)

Question 1) (1 pt) Donnez un exemple, soit d'une exigence non fonctionnelle de sureté de fonctionnement, soit une exigence fonctionnelle de sureté de fonctionnement (vous pouvez par exemple vous servir de l'exemple du distributeur de boisson, ou d'un train).

Question 2) (1,5 pts) Définissez en expliquant la différence entre les deux concepts : l'élimination des fautes et la tolérance aux fautes

Question 3) (1,5 pts) Définissez brièvement ce qu'est une zone de confinement d'erreur dans une description architectural d'un système. Décrivez-les principales caractéristiques.

II Architecture redondantes et modèles de fautes (7 pts)

Question 4) (1 pt) Rappelez ce qu'est une architecture redondante de type réplication passive. (On demande le fonctionnement mais pas l'analyse des états de fiabilité / disponibilité)

Une architecture dite de réplication active est constituée d'un voteur, et d'un certain nombre de calculateurs identiques. Cette architecture repose sur le principe suivant :

- Chaque calculateur possède une version logicielle de la fonction qui doit être redondée.
- Chaque version du logiciel est censée s'exécuter en un temps borné connu T
- Les défaillances de chaque calculateur et de son logiciel sont supposées indépendantes entre calculateurs.
- Au bout d'un temps T, le voteur compare les réponses reçues pour déterminer une réponse majoritaire.

Nous considérons deux modèles de défaillance différents : crash (ou défaillance silencieuse) et byzantin.

Le premier entraine l'arrêt du calculateur : la défaillance ne propage pas de valeur incorrecte. Dans le cas byzantin la défaillance peut propager une valeur incorrecte mais avant tout la manière dont les nœuds défaillent peut être coordonnée.

Question 6) (0,5 pts) Indiquez le nombre de calculateurs devant être considérés pour tolérer deux défaillances (on suppose le voteur totalement fiable) pour chaque modèle, justifiez ?

Il s'avère que le voteur reçoit des valeurs pouvant subir des légère variations dues au calcul numérique. Ainsi par rapport au résultat théorique D chaque réplique peut retourner une valeur X telle que | X- D| < err. (|.| désigne la valeur absolue)

Question 7) (1 pt) indiquez comment procéder coté voteur pour déterminer si les résultats retournées sont valides (sachant que D est inconnue). Indiquez quelle serait l'erreur numérique finale produite par l'architecture de réplication active à 3 répliques ?

Le modèle de reliability bloc diagram est une représentation graphique des conditions qui définissent l'état de fiabilité du système : la formule indiquant sous quelles conditions une architecture reste opérationnelle étant donné que certains de ses composants sont défaillants. Il en existe trois variantes de base : série, parallèle et k parmi n. Vous indiquerez pour le cas « k parmi n » les valeurs de k et n choisies. (cette expression indique la condition de correction k nombre corrects requis sur nombre total de répliques). Nous supposerons dans un premier temps qu'un bloc permet d'identifier : le fonctionnement d'un calculateur avec le logiciel

Question 8) (1pt) Donnez le schéma correspondant à une réplication active avec 3 répliques

On suppose maintenant que l'on dispose calculateurs pouvant chacun exécuter trois répliques et un voteur (si nécessaire). On suppose de plus que la défaillance provient du logiciel seul et ne peut se propager aux répliques exécutées sur le même calculateur.

Question 9) (1 pt) Quelle est la démarche la plus fiable : réaliser un unique vote parmis toutes les répliques ou 3 votes locaux aux calculateur et un vote global entre réponses de calculateur (on suppose toujours les composants de vote parfait).

On souhaite désormais séparer l'impact du logiciel et du matériel, ainsi que l'impact du voteur. On supposera que le voteur ne peut défaillir que par crash, et que l'implémentation logicielle de la fonction, et chaque calculateur peut défaillir selon un modèle byzantin. Cependant, ces défaillances sont indépendantes dans leur occurrence (i.e. chaque nœuds défaille indépendamment mais une fois défaillant, il peuvent se synchroniser pour produire des données fausses).

Question 10) (3,5 pts) Donnez le reliability bloc diagram de l'architecture ou le voteur est dupliqué (deux voteurs), et où l'on dispose de 3 calculateurs exécutant chacun 3 répliques du logiciel. On supposera que le voteur de l'architecture vote sur la réponse majoritaire parmi l'ensemble des répliques logicielles exécutées.

III Mécanismes de tolérance aux fautes (3 pts)

Un ingénieur propose d'implémenter un mécanisme de capture d'état d'exécution de processus Unix (contexte d'exécution d'un programme). Ce mécanisme serait couplé avec un détecteur d'erreur pour pouvoir tolérer fautes liées à des erreurs de développement se manifestant de manière aléatoire. En pratique, il propose donc de déployer un mécanisme de tolérance aux fautes utilisant :

- une sauvegarde régulière d'état associée à un mécanisme de détection d'erreur
- si une erreur est détectée elle déclenche la restauration du dernier état sauvegardé en cas d'erreur.

Question 11) (0,5 pts) Un tel mécanisme porte un nom, donnez le.

Question 12) (1 pt) Quelle caractéristique doit vérifier la faute dont ce mécanisme est censé corriger les erreurs ?

Un recovery block est une manière de munir un code, réalisant un calcul, de capacité de tolérance aux fautes. Le principe de fonctionnement d'un recovery block est d'utiliser ce que l'on appelle un test de vraisemblance pour savoir si le résultat produit est correct. De plus, on dispose d'un certain nombre de versions différentes de logiciels permettant de réaliser la même tâche. On suppose que les calculs sont réalisés sur un volume de données important.

Question 13) (1,5 pt) Dans certaines versions du recovery block, le mécanisme capture une sauvegarde de l'état avant exécution des fonctions de calcul. Donnez une situation dans laquelle ce choix se justifie. Proposez une méthode pour éviter de devoir nécessairement réécrire l'intégralité de l'état du système à chaque chargement.

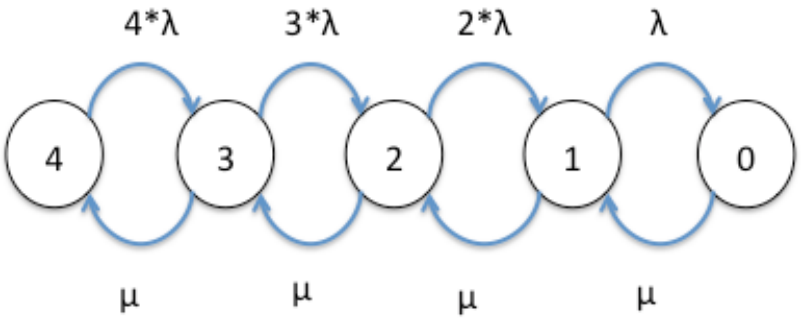
IV Analyse quantitative (4 pts)

Il est dit qu'une architecture de réplication passive permet d'augmenter la disponibilité d'une fonction de calcul si le modèle de défaillance par crash est considéré.

Question 14) (1pt) Peut on dire la même chose pour une réplication active pour le modèle de défaillance byzantin, justifez ?

Nous utilisons la chaine de markov à temps continu page 4 pour modéliser le temps avant défaillance d'une réplication passive à 3 répliques. Nous utilisons le paramètre λ pour identifier le taux de défaillance, et le paramètre μ pour le taux de réparation.

Question 15) (2 pt) Que pouvez vous dire sur ce modèle concernant les hypothèses de défaillance des différentes répliques et le processus de réparation ? (On suppose que l'on dispose de 4 répliques initialement).



Nous souhaitons modélisez le fait jusqu'à 2 répliques défaillances peuvent se réparer en même temps avec le même taux moyen de réparation que dans la question précédente.

Question 15) (1,5 pts) modifiez le modèle pour capturer cette situation.

On suppose que l'on réplique un service implémenté en logiciel qui s'exécute en temps constant. Lors d'une exécution, chaque réplique a la même probabilité de défaillir f (lié au matériel). Les phénomènes de défaillance sont indépendants les un des autres. On suppose que l'on a une architecture de réplication passive ayant une probabilité de défaillance f pour chaque réplique de l'architecture lors de l'exécution d'une instance du service.

Question 16) (1,5 pt) Pensez vous que si l'on prend des composants ayant une chance de défaillir de ½ lors d'une exécution, alors la réplication passive peut améliorer la disponibilité du résultat ? Si oui de combien l'améliore-t-on pour 3 répliques par rapport à une seule.