ENSERB
Année 1997-1998

Filière Informatique 3^{eme} année
Option Génie Logiciel

Mardi 17 mars, 14 heures - 16 heures
Tous documents autorisés.

M.F.I.L.
Alain Griffault & Didier Bégay

CORRIGE

Vous vous reporterez au dossier ci-joint, extrait du livre “Safeware” de Nancy Leveson et concernant le cas du Therac 25.

Exercice 1 (10 points) : Etude de risques

Question 1 *Dans un premier temps, vous ferez une analyse des dysfonctionnements et discuterez les points suivants :*

1. *Absence de sécurité.*
2. *Réutilisation abusive de l'existant.*
3. *Absence de découpage modulaire du programme.*

Réponse 1(5 points)

Question 2 *Vous proposerez en conséquence des éléments méthodologiques permettant d'éviter les inconvénients observés.*

Réponse 2(5 points)

Exercice 2 (10 points) : Modélisation et vérification

Le but de l'exercice est de construire un modèle formel d'un des problèmes du Therac-25, afin de calculer le ou les scénarios critiques.

La partie étudiée correspond à la section **Specific Design Errors** comprise entre les pages 534 et 537 du document joint.

Question 3 *Donnez la liste des composants de ce sous-système, suffisante afin de pouvoir étudier le phénomène. Justifiez brièvement vos choix.*

Réponse 3(1 points) Les composants sont de divers types :

les variables partagées : Elles sont au nombre de trois, MEOS, DataEntry, MEOSChanged.

les tâches : Elles sont au nombre de trois, Datent, Magnet, Ptime ; et éventuellement l'ordonnanceur Treat.

l'environnement : Il n'est pas obligatoire, mais modéliser un composant Keyboard qui permet la modification des variables partagés est pratique.

Pour une analyse plus fine, il sera peut-être nécessaire de distingués plusieurs composants à l'intérieur de certaines tâches, notamment faire apparaître leurs variables locales.

Question 4 *En utilisant les préfixes* `To` *(resp.* `Is`*) pour indiquer une affectation (resp. une lecture de la valeur), donnez le système de transition qui représente le* comportement *de la variable partagée* `MEOS`*.*

Réponse 4(1,5 points) Pour notre étude, la variable MEOS peut être assimilée à une variable pouvant prendre quatre valeurs distinctes : PhotonHigh, PhotonLow, ElectronHigh et ElectronLow. Le mode et l'énergie peuvent être modifiés séparément, mais la sélection du mode Photon met par défaut l'énergie à une position basse. Le système de transition est alors représenté par la figure 1.

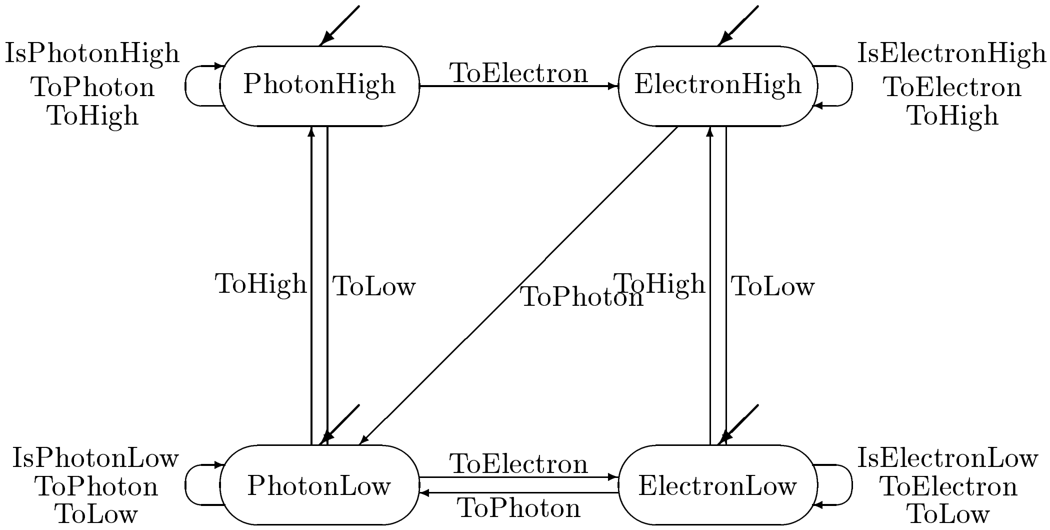

Figure 1: La variable MEOS.

Question 5 *Donnez une abstraction du comportement (ie. un système de transition) de la tâche* `keyboard`*, dans laquelle seules subsistent les modifications de certaines variables partagées.*

Réponse 5(1 points) D'après le texte, il est possible de modifier les variables partagées dans n'importe quel ordre. Il semble en effet que l'on peut changer les valeurs de MEOS à tout instant, donc celle de MEOSChanged, et que la variable DataEntry est modifiée des que le curseur est sur la dernière ligne de l'écran. Cela donne le système de transition de la figure 2.

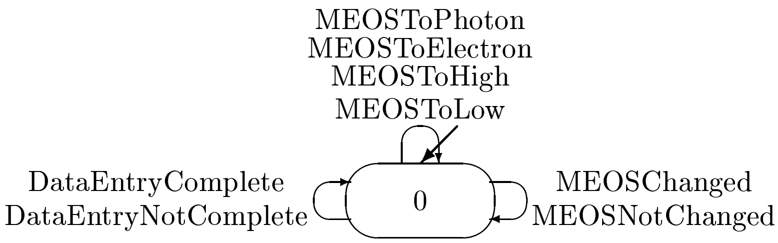

Figure 2: L'environnement.

Question 6 *Donnez une abstraction du comportement de la tâche* `Datent` *(ie du code de la page 536).*

Réponse 6(1,5 points) Dans notre modèle, la variable MEOS est toujours spécifiée. Le premier test du code est donc supprimé dans l'abstraction représentée par la figure 3.

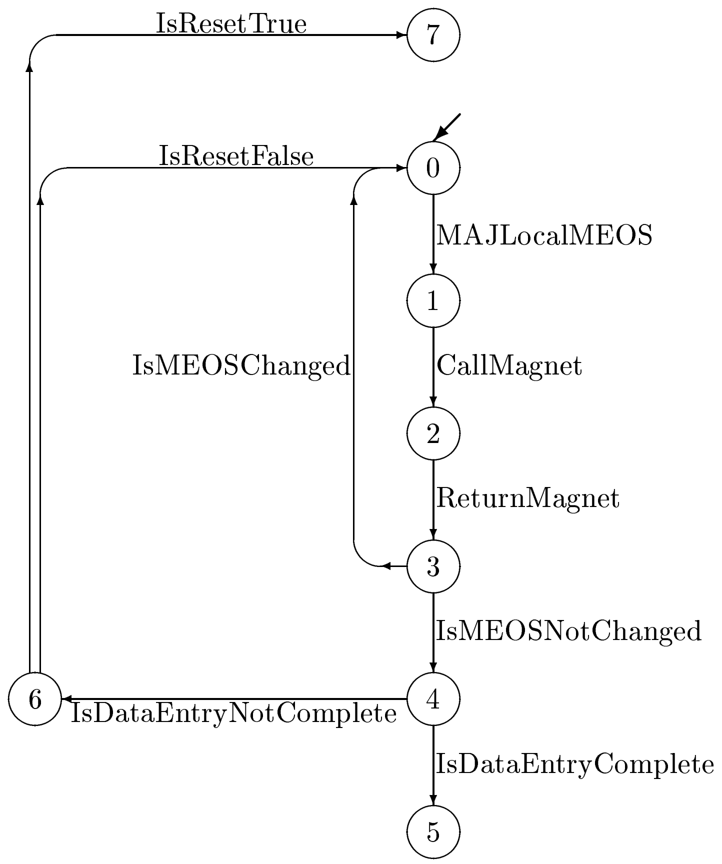

Figure 3: La tâche Datent.

Question 7 *Décrivez le système de synchronisation (ie. l'ensemble des interactions) de ce système en fournissant :*

1. *Exactement les vecteurs de synchronisations reliant les composants* `MEOS`*,* `keyboard` *et* `Datent`*.*
2. *Des indications sur la nature des vecteurs de synchronisations reliant les autres composants.*

Réponse 7(2 points) Pour décrire les intéractions entre les composants `MEOS`, `keyboard` et `Datent`, il est pratique d'introduire un composant supplémentaire qui représente la variable locale MEOS.

Keyboard	MEOS	Datent	LocalMEOS
MEOSToPhoton	ToPhoton		
MEOSToElectron	ToElectron		
MEOSToHigh	ToHigh		
MEOSToLow	ToLow		
	IsPhotonHigh	MAJLocalMEOS	ToPhotonHigh
	IsPhotonLow	MAJLocalMEOS	ToPhotonLow
	IsElectronHigh	MAJLocalMEOS	ToElectronHigh
	IsElectronLow	MAJLocalMEOS	ToElectronLow

Les autres intéractions du système sont les suivantes :

- Pour chacune des variables partagées, le composant Keyboard les modifie, et elles sont lues par une tâche, qui éventuellement sauvegarde leurs valeurs dans des variables locales.
- Les appels entre les tâches sont représentés par deux vecteurs de synchronisation. Le premier est du type (CallX,run) et le second du type (ReturnX, return).

Question 8 *Donnez une expression logique, évaluable par un outil de vérification tel que Mec, montrant l'existence de situations anormales.*

Réponse 8(1,5 points) L'anomalie du Therac 25 est la possibilité d'émettre des photons avec une grande énergie. Cela est possible si la variable partagée MEOS et la variable locale sont différentes au moment où la tâche Datent termine normalement.

Avec un outil de vérification, il suffit de regarder si le résultat du calcul suivant est l'ensemble vide ou non.

Anomalie := !state[Datent]='5' and (!state[MEOS] # !state[LocalMEOS]) ;

Question 9 *Donnez une expression, calculable par un outil de vérification tel que Mec, dont le résultat pourra être interprété comme une exécution conduisant à la situation anormale précédente.*

Réponse 9(1,5 points) L'outil de vérification Mec possède une fonctionnalité dont le résultat est l'ensemble des transitions appartenant à un chemin de longueur minimale entre deux ensembles d'états en n'utilisant que des transitions dans un ensemble donné.

Il suffit donc d'interprèter comme une exécution le résultat du calcul suivant :

ManipulationCritique := trace(initial,*,Anomalie) ;
