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

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.*

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

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.*

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`*.*

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.*

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

Question 7 *Decrivez 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.*

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

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.*