Université Bordeaux I
U.F.R. Mathématiques et Informatique

D.E.S.S. de Génie Logiciel
Année 1997-1998

Spécifications et vérifications formelles
Examen de janvier 1998.
(André Arnold & Alain Griffault)

1 Introduction

Cet exercice est inspiré d'un cas test classique en sûreté de fonctionnement. Il consiste, en partant d'une spécification informelle d'un système de régulation de température, d'une part à traduire le fonctionnement nominal de la spécification en un un modèle de système valide et correct vis à vis d'un événement redouté; d'autre part à ajouter les pannes décrites dans la spécification informelle afin d'exhiber les jeux de pannes minimaux qui conduisent inévitablement vers l'événement redouté.

2 HNO3 : un système de régulation de température

Il s'agit d'un système qui maintient la température d'un flux d'acide nitrique dans une plage acceptable. Le système est bien-connu, car il a déjà été choisi à plusieurs reprises dans la littérature pour illustrer l'aptitude de certaines méthodes à determiner l'ensemble de scénarios qui conduisent à l'occurence d'un événement redouté donné :

ER : Température de l'acide nitrique trop élévé en sortie du système.

Le système est représenté à la figure 1. Toutes les liaisons entre les composants sont supposés *parfaites*, alors que ces derniers peuvent connaître des défaillances, mais uniquement celles qui sont listées dans la table 1.

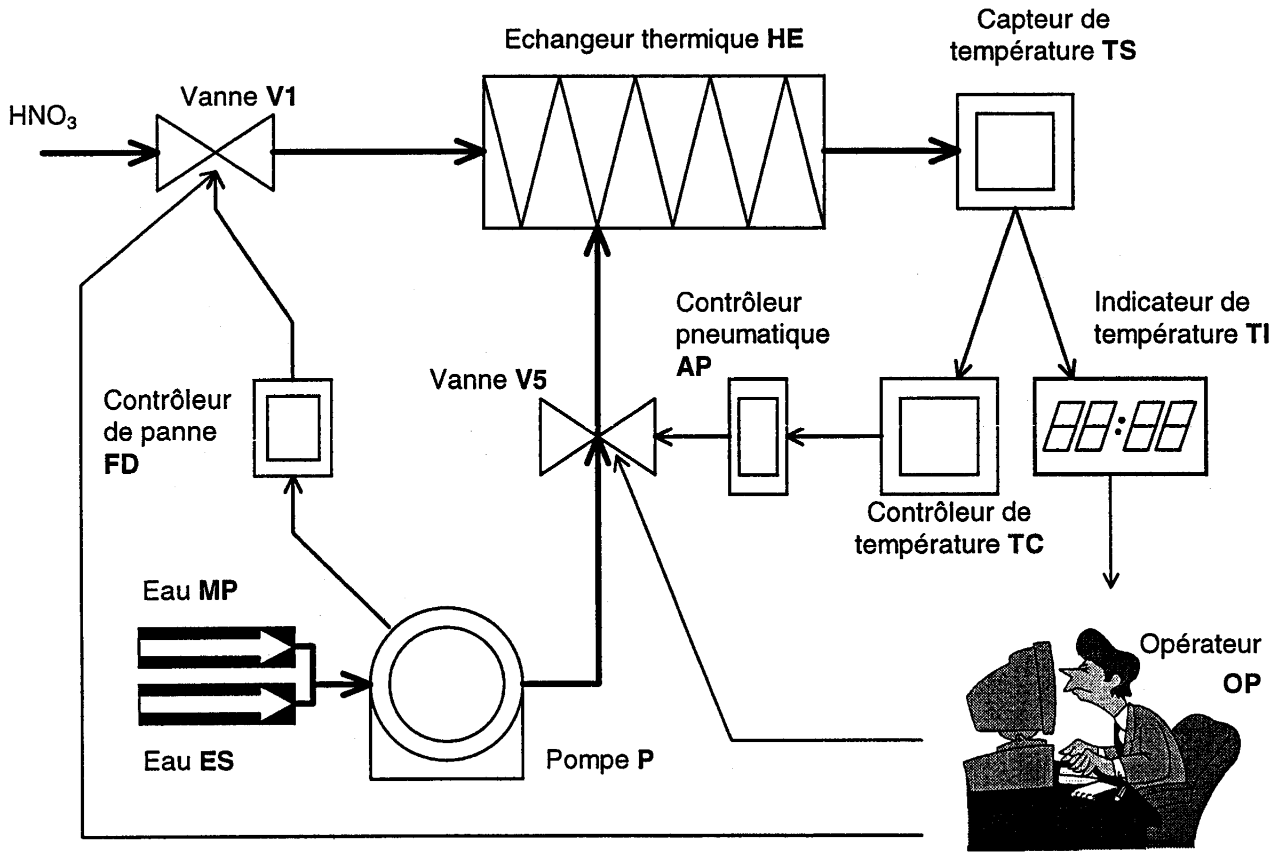

Figure 1: Description du système

Composants	Fonctions	Modes de défaillances
V1	Vanne de régulation du débit d'acide nitrique et de sécurité. Sa fonction de régulation est réalisée par action manuelle de l'opérateur. Sa fonction de sécurité résulte de FD ou de l'action de l'opérateur.	V1S : bloquée en position, V1 ne réagit pas aux sollicitations de FD ni à celles de l'opérateur.
HE	Echangeur. Il est supposé "parfait".	Aucune, si ce n'est que c'est ici que se produit l'explosion.
TS	Capteur de température. Il mesure la température T3 du flux de HNO3 en sortie de l'échangeur et transmet l'information T6 à TC et TI.	TSS : bloqué en position. TSFL : le capteur envoie une information érronée par défaut $T6 < T3$ réelle.
TC	Contrôleur de température. Il compare la valeur de T6 à celle de Tc et, quand il détecte une dérive, modifie en conséquen,ce le débit de V5 par l'intermédiaire d'une commande pneumatique AP.	TCS : bloqué en position, TC n'envoie aucun ordre à V5.
V5	Vanne de régulation, contrôlée par AP. Elle contrôle elle-même le débit d'eau de refroidissement destiné à HE. Elle peut être actionnée manuellement par l'opérateur après que celui-ci ai déconnecté l'automatisme. Elle se ferme par manque d'air comprimé.	V5S : bloquée en position, V5 ne réagit ni aux sollicitations de TC via AP, ni à celles de l'opérateur. V5R : suite à une erreur de remontage après une opération de maintenance, V5 réagit à l'inverse des ordre reçus.
AP	Air comprimé, commande l'ouverture de V5.	LAP : perte d'air comprimé.
MP	Alimentation principale en eau de refroidissement.	LMP : perte de l'alimentation principale.
ES	Alimentation de secours en eau de refroidissement.	NES : perte de l'alimentation de secours.
P	Pompe, elle assure le débit nécessaire en eau de refroidissement.	PF : pompe défaillante (arretée).
TI	Indicateur de température. Il constitue la seule source d'information sur la température de sortie de HNO3, pour l'opérateur.	TIS : bloqué en position.
FD	Détecteur de panne de la pompe P. Lorsqu'il détecte une panne de P, il envoie un signal de fermeture à V1.	FDB : bloqué, il n'envoie aucun signal à V1.
OP	Opérateur. Il supplée les défaillances (ou supposées telles) de la régulation automatique en agissant sur V5 et, si nécessaire sur V1.	OPA : opérateur absent.

Table 1: Les composants

La mission du système consiste à refroidir un flux d'acide nitrique et à maintenir sa température dans une plage acceptable. Ceci est obtenu par l'action de l'une des trois séquences (interruptibles) décrites ci-après dans l'ordre chronologique de leur intervention :

- automatique : TS → TC → AP → V5 → HE
- manuelle : TS → TI → OP → V5 → HE
- manuelle : TS → TI → OP → V1 → HE

L'opérateur n'a qu'une seule source d'information : TI. Il n'agit pas tant que la température T6 lui apparaît égale à la température de consigne Tc, ou lui apparaît y être ramenée par la régulation automatique. Dans le cas contraire, il déconnecte l'automatisme de la commande de V5 par le contrôleur pneumatique AP, afin de pouvoir agir sur V5, puis sur V1 si ses actions s'avèrent inefficaces.

De même, toute défaillance de la pompe doit être détectée par FD, qui commande immédiatement la fermeture de V1.

A partir de l'état initial, deux évolutions possibles de la température de l'acide nitrique doivent être envisagées :

- un accroissement transitoire, dT, de cette température, trop bref pour pouvoir conduire, seul, à l'événement redouté.
- un accroissement persistant, DT, de cette température, qui, s'il n'est pas compensé par les régulations, conduit à l'événement.

3 Modalités

- Vous pouvez utiliser les sources disponibles dans `~griffaul/Demos/HNO3`. Le répertoire `Version_1` contient deux versions du système sans panne, et le répertoire `Version_2` correspond à l'injection d'une première panne.

  Le travail demandé comprend donc quelques questions et un travail de modélisation.

  1. Le modèle hno3_v11 vous parait-il valide ?
     Si oui, modifiez simplement le calcul portant sur les l'événements incontrôlables, afin que les résultats soient toujours l'ensemble vide.
  2. Expliquez la différence entre hno3_v11 et hno3_v12 ?
  3. Le modèle hno3_v21 vous parait-il valide ?
  4. Pour chacun des modèles, dites si l'événement redouté ER est :
     – impossible,
     – impossible si l'opérateur fait "correctement" son travail.
     – possible si l'opérateur fait non "correctement" son travail. Vous donnerez une trace d'éxécution comme justificatif.
     – inévitable. Vous donnerez la combinaison minimale de pannes conduisant à cette situation.

- Date limite de remise des rapports : Mercredi 14 janvier à 9 heures du matin. Le rapport devra être déposé dans le répertoire `~griffaul/VF/` avec un nom permettant d'identifier le propriétaire. Le répertoire sera accessible en écriture du vendredi 9 janvier au matin jusqu'à la date limite.
- Le rapport doit comprendre les fichiers "sources" et un texte explicatif (non nécessairement long).
- Les binômes sont acceptés.