Miniprojets - B / Event B / Septembre 2016

Analyse, spécification, conception, codage
(Encadrement : C. Attiogbé)

Note : tous les miniprojets proposés ici sont extraits du cadre du projet ∇ [1]. Ils correspondent à un besoin réel et contribuent par conséquent à votre formation sur des projets opérationnels de difficultés et de tailles moyennes mais réelles.
Un rapport [2] (de préférence en Latex) est demandé pour chaque miniprojet. Le rapport doit mettre en valeur tous les aspects de votre travail : analyse, spécification, développement. Le rapport et le travail sont notés.

Centrale nucléaire

(Cette étude de cas est effectuée dans le cadre du projet ∇.)
Spécification de fonctionnement d'automates programmables par passage d'un modèle logique à une spécification en B
Le système est destiné à refroidir, à l'eau, un fluide circulant à débit constant. L'eau de refroidissement est puisée dans un réservoir à l'aide de la pompe de circulation 001P0 via la vanne 001VN. La pompe d'alimentation OO2P0 assure l'apoint en eau via la vanne 002VN. Deux capteurs de niveau "tout ou rien", 001SN et 002SN, détectent respectivement un niveau bas et un niveau haut dans le réservoir.

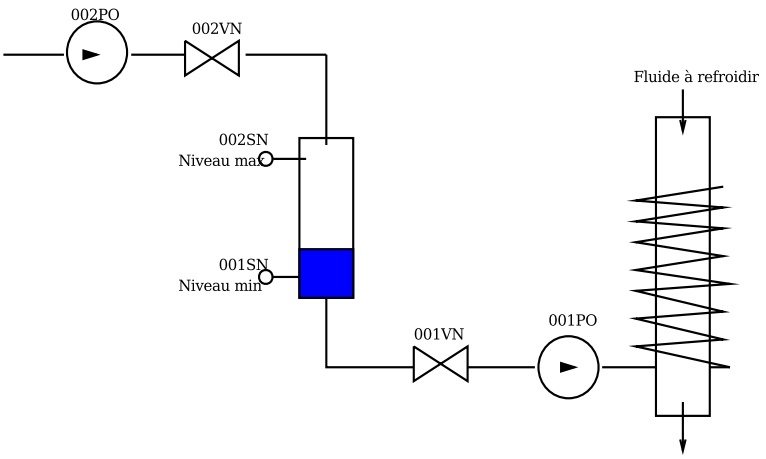

Figure 1 – Schéma de principe

1 Spécification en logique du fonctionnement du système

Il s'agit ici de la construction en logique des propositions, d'un modèle des spécifications de fonctionnement d'automates programmables destinés au système.
Ce modèle est destiné à l'étude formelle de la consistance des spécifications, et ce sous un double aspect : consistance intrinsèque des traitements (existence de solutions pour système booléen représenté par les

1. Nantes B Libraries/Christian Attiogbé
2. Pour les projets aboutis, une version revue et corrigée sera disponible sur le site www du projet.

équations), d'une part ; condition de compatibilité entre le système logique et ses entrées (ou conditions aux limites), d'autre part.
La consistance formelle de ce premier modèle étant acquise, nous pourrons, dans un deuxième temps, l'enrichir de conditions supplémentaires d'exclusion entre événements, liées à la sémantique des variables du modèle. Nous verrons que ces contraintes ont pour effet d'imposer des restrictions sur les donnés en entrée.

1.1 Variables du langage

Le langage propositionnel utilisé pour ce modèle est complètement défini par la donnée des ses variables (ensemble *P*). On distinguera les variables d'entrée (ensemble *F* support des bases de faits à l'initialisation du modèle) des autres variables du modèle. Toutes les variables sont de la forme : "Objet.Attribut", où l'attribut est facultatif.

1.1.1 Variables d'entrée du modèle

La liste ci-dessous regroupe l'ensemble *F* des variables figurant dans les bases de faits initiale.

Variables	Attributs	Description
DC380HT		Défaut d'alimentation (380 V)
		Sans attribut
OO4MT		Température fluide réfrigéré
		(amont échangeur)
	1	Seuil basse température
	2	Seuil haute température
001PO		Pompe de circulation
	1	Pompe enclenchée
	2	Pompe indisponible
001SN		Bâche : niveau bas
	0	Niveau minimum
002SN		Bâche : niveau haut
	0	Niveau maximum
202TL		"Tourner-lumineux" de pompe d'alim.
	E	Position "pompe enclenchée"
	D	Position "pompe déclenchée"
001VN		Vanne de circulation
	0	Vanne fermée, fin de course
002VN		Vanne d'alimentation de la bâche
	0	Vanne fermée, fin de course
001PO		Pompe de circulation
	D.PP	Ordre PP de déclenchement
	D.PR	Ordre PR de déclenchement
	E.PP	Ordre PP d'enclenchement
	E.PR	Ordre PR d'enclenchement

Tourner-lumineux : désigne les boutons de commande sur les pupitres des salles de commandes dans les centrales nucléaires de conception classique. Ces boutons lumineux s'allument tant que l'état du matériel commandé est en discordance avec la commande affichée.
pp : Panneau principal de commandes (calculateur de conduite)
PR : Panneau de repli.

1.1.2 Autres variables du modèle

Variables	Attributs	Description
001PO		Pompe de circulation
	D	Ordre global de déclenchement
	E	Ordre global d'enclenchement
	V1	Verrouillage à l'enclenchement par perte du 380 V
	V2	Verrouillage à l'enclenchement par perte du fluide
002PO		Pompe d'alimentation
	D	Ordre global de déclenchement
	E	Ordre global d'enclenchement
003KA		Circulation indisponible
		Sans attribut
905KA		Haute température fluide et circulation indisponible
		Sans attribut
901KA		Excès de circulation
		Sans attribut

1.2 Modèle des spécifications de fonctionnement des automates

1.2.1 Modèle sous la forme d'implications logiques

[L1] $(001PO2 \vee 001SN0) \wedge 004MT2 \rightarrow 905KA$

Haute température du fluide réfrigéré, associé à l'indisponibilté de la circulation : bas niveau du réservoir ou pompe indisponible (conditions de l'alarme 003KA).

[L2] $001PO2 \wedge 001SN0 \rightarrow 003KA$

Indisponiblité de la circulation (bas niveau du réservoir ou pompe indisponible).

[L3] $001PO1 \wedge 004MT1 \rightarrow 901KA$

Excès de circulation : pompe de circulation enclenchée et seuil bas de température du fluide réfrigéré.

[L4] $202TL.E \vee \neg 002VN0 \rightarrow 002PO.E$

Ordre d'**enclenchement de la pompe d'alimentation** : position enclenchée du tourner-lumineux, ou vanne d'alimentation non fermée.

[L5] $202TL.D \vee 002VN0 \rightarrow 002PO.D$

Ordre de **déclenchement de la pompe d'alimentation** : position déclenchée du tourner-lumineux, ou vanne d'alimentation fermée.

[L6] $001SN0 \vee 001VN0 \rightarrow 001PO.E.V2$

Verrouillage à l'enclenchement de la pompe de circulation : niveau minimum au réservoir, ou vanne de circulation fermée.

[L7] $(001PO.E.PP \vee 001PO.E.PR) \wedge \neg DC380HT$
$\wedge \neg(001PO.D.PP \vee 001PO.D.PR \vee 001VN0 \vee 001SN0)$
$\rightarrow 001PO.E$

Ordre d'**enclenchement de la pompe de circulation**. Conditions :
- existence d'une commande d'enclenchement (soit PP, soit PR),
- 380V disponible,
- pas de commande de déclenchement (ni PP, ni PR),
- vanne de circulation ouverte et réservoir non vide. C'est la négation des conditions du verrouillage à l'enclenchement $001PO.E.V2$ dans [L6].

[L8] $(001PO.D.PP \vee 001PO.D.PR) \vee (001VN0 \vee 001SN0) \rightarrow 001PO.D$

Ordre de **déclenchement de la pompe de circulation**. Conditions :
- existence d'une commande d'enclenchement (soit PP, soit PR),
- vanne de circulation fermée ou réservoir vide. Ce sont les conditions du verrouillage à l'enclenchement $001PO.E.V2$ dans [L6].

[L9] $\neg 001PO1 \wedge DC380HT \rightarrow 001PO.E.V1$

Verrouillage à l'enclenchement de la pompe de circulation par manque de tension 380V : DC380HT et pompe non enclenchée.

Référence

M. Gondran, J-F. Héry, J-C. Laleuf, *Logique et modéliation*, Eyrolles, 1995