FEUP

Universidade do Porto
Faculdade de Engenharia

Sistemas Críticos

Trabalho Prático Nº 1

Aplicação Tolerante a Falhas

2010/11

1. Introdução e Objectivos

Este primeiro trabalho tem como objectivo familiarizar os alunos com o desenvolvimento de aplicações tolerantes a falhas.

Tendo em conta que a apresentação deste trabalho está ligeiramente adiantada em relação aos assuntos leccionados nas aulas teóricas, sugere-se a utilização de uma arquitectura do tipo *N-Version Programming*. No entanto, fica ao critério dos alunos a escolha do tipo de redundância a implementar (redundância de dados e/ou redundância de concepção), e de ainda a eventual utilização de mecanismos de prevenção de eventuais modos de falhas inerentes à utilização deste tipo de arquitecturas.

Este trabalho está organizado para que a sua realização seja efectuada por grupos de 3 alunos, cabendo a cada aluno a realização de uma variante. Em caso de manifesta necessidade o trabalho poderá ser realizado por alguns grupos de 2 alunos.

2. Contexto

Considere uma central nuclear, onde existe um edifício onde é armazenado o combustível nuclear já utilizado. Este combustível está disposto sob a forma de barras, que consistem numa pilha de elementos radioactivos.

Embora o combustível tenha já sido utilizado, as barras continuam a emitir calor durante bastante tempo devido ao processo de decaimento dos materiais radioactivos. Para arrefecer o combustível as barras são colocadas numa piscina com água. Durante este processo a água vai aquecer e por isso vai ser necessário arrefece-la. Um sistema de bombas vai fazer circular a água através de permutadores de calor, onde a temperatura da água vai ser reduzida, sendo depois injectada de novo na piscina já a uma temperatura mais baixa.

Uma aplicação na sala de comando da central monitoriza a temperatura da água da piscina e controla o caudal das bombas de circulação por forma que a temperatura da água esteja dentro de valores desejados. Para uma operação normal, a temperatura deve estar entre 40º e 50ºC.

Na piscina existem 3 sensores de temperatura que estão ligados a um equipamento de aquisição de dados. Este último envia os valores das medidas dos sensores para a aplicação na sala de comando através de uma rede de comunicações. Os valores são enviados para a aplicação periodicamente, de 1 em 1 minuto. Por sua vez, a aplicação, de 3 em 3 minutos, toma uma decisão sobre qual o caudal a aplicar às bombas.

A tarefa a ser completada pelo grupo consiste em conceber e implementar uma aplicação que, executando num ciclo infinito, define o caudal das bombas que garante que a temperatura da água está dentro dos valores desejados.

3. Requisitos

A cada minuto, o programa deverá efectuar uma leitura da temperatura da água da piscina (i.e do ficheiro de entrada). Como não se dispõe do equipamento de leitura dos sensores, este vai ser simulado através da leitura de um ficheiro que contém os valores (hipotéticos) dos dados recebidos dos sensores.

De preferência, a leitura deverá ser efectuada directamente do **stdin**, o qual poderá ser redireccionado se necessário. O ficheiro de entrada será um ficheiro de texto, em que cada linha terá o seguinte formato:

Si <leitura>

em que **Si** representa sensor **i {i=1,2,3}** e **<leitura>** o valor do sinal do sensor expresso em volts (V). Em cada instante há 3 medidas, cada uma referente a um sensor. Cada sensor pode fornecer uma sinal entre 0.000 e 10.000V. Cada valor é um número em vírgula flutuante, expresso em base 10, sem recurso a expoentes.

Exemplo:

S1 2,213

S2 3,453

S3 2,855

S1 2,246

.....

Os valores da temperatura (no ficheiro) devem em primeiro lugar ser convertidos para ºC. Como os sensores não são lineares (têm maior sensibilidade para certas gamas de temperatura), a conversão efectua-se de acordo com a seguinte expressão:

$$T = -W * \ln(1 - (S * Y - Z)/K)$$

em que:

S : valor medido pelo sensor, em Volt

K= 5,21

W= 456

Y= 0,104

Z= 0,01

T : temperatura, em ºC

O caudal a aplicar às bombas é definido através do seguinte procedimento:

1. Calcular a média pesada, TS, das 3 últimas leituras de temperatura

$$TS = [T(i-2) * 0.978 + T(i-1) * 1.013 + T(i) * 1.023]/3.014$$

em que:

T(i) : temperatura neste instante

T(i-1): temperatura há 1 minuto atrás

T(i-1): temperatura há 2 minutos atrás

2. O caudal a aplicar às bombas é dado pelas seguintes expressões:

$$E = 45 - TS$$

$$C = 500 * KC * [E + 1/TI * \int_0^t E(i)di]$$

em que:

KC: 0,495

TI: 117

E(i) = 45-TS(i), em que TS(i) representa o valor da média pesada medida no instante i.

C : caudal das bomba, em L/m

Tendo em conta a forma com as bombas operam, a saída, representando o caudal das bombas em L/min, deve ser expressa por um valor inteiro. O caudal das bombas não pode ser negativo, nem ultrapassar 1000L/min. Se algum destes casos ocorrer, a saída deve ser colocada a 0 no primeiro caso, e no segundo caso a 1000.

De três em três minutos, o programa deverá actualizar o caudal das bombas. O caudal deverá ser escrito para o terminal, ou seja o 'stdout'.

Deseja-se que este programa seja tolerante a falhas, sendo para tal imposto como requisito que o programa deverá ter tantas variantes como elementos do grupo. Por exemplo, um grupo com 3 elementos deverá implementar um programa com 3 variantes.

Deverá ter ainda em atenção que pode ainda ocorrer a falha dos sensores de temperatura, bem como haver falha na comunicação com a sala de comando. No primeiro caso, o sensor avariado pode limitar-se a produzir sempre o mesmo valor (modelo de falhas do tipo 'stuck-at'), ou produzir valores aleatórios que estejam sempre a mudar. No segundo caso, a falha de comunicação será representada por uma entrada sem qualquer valor (i.e. linha em branco no ficheiro). Além disso, como os sensores não estão colocados no mesmo local da piscina é possível que forneçam valores ligeiramente diferentes. Sugere-se a utilização de um algoritmo de *votação maioritária dinâmico* para definir o valor da temperatura na piscina.

Em caso de detecção de mais falhas do que aquelas que o programa consegue tolerar, o programa deverá falhar. A indicação da falha será através da escrita do texto 'FAIL' no terminal, em substituição do valor de saída que deveria ser produzido em situação de funcionamento normal.

Por forma a reduzir o tempo de teste e validação do programa, este último não necessita de executar em tempo real. Ou seja, poderá executar os ciclos sem recorrer a qualquer relógio e sem considerações de tempo.

Os valores de saída, i.e. o caudal das bombas, deverão ser armazenados num segundo ficheiro.

O programa não necessita de ter qualquer interface gráfica. Deverá ser capaz de executar na linha de comandos, tendo como primeiro e único parâmetro o nome do ficheiro onde se encontram guardados os dados de entrada. Os valores de saída deverão ser impressos para o

terminal em formato semelhante ao dos dados de entrada: uma linha por ciclo, um único número por linha, cada número expresso em formato textual e em base decimal.

Cabe a cada grupo definir qual o tipo de diversidade a utilizar em cada variante, a arquitectura a utilizar, o mecanismo de decisão a adoptar, e a forma de organizar o programa.

A linguagem de programação é de escolha livre.

4. Apresentação

O trabalho deverá ser entregue por email (pportugal@fe.up.pt) até dia 30 de Abril. Neste email deverá ser enviado:

- o código fonte
- o código já compilado (sendo indicado no email o ambiente para o qual foi compilado)
- dois ficheiros, um com a entrada e outro com o resultado de uma execução do programa
- um relatório, com máximo de 3 folhas A4, onde deverá ser expresso as opções tomadas para o desenvolvimento do projecto, as razões que fundamentam essas opções, comentários à capacidade de tolerância a falhas e à fiabilidade do programa, bem como eventuais sugestões de como se poderia melhorar o programa.