THE UNIVERSITY OF MELBOURNE
SOFTWARE ENGINEERING METHODS

Project – Evaluating Software Reliability

ED. KAZMIERCZAK

SECOND SEMESTER, 2003

Due Date: 5:00pm Wednesday 29th October, 2003

20% of the Final Mark

Project Aims

The aim of this project is for you to measure and model the reliability growth of a simple program using the basic execution time model. In the process of constructing the model you will be faced with a number of issues concerning the evaluation of reliability. Specifically, the aims are to:

(i) provide you with the means of exploring the practical aspects of reliability engineering and translating theory into practice (which can take some ingenuity);

(ii) expose you to some of the practical issues and limitations of reliability growth modelling;

(iii) provide insight into the ways in which reliability growth modelling can impact projects; and

(iv) provide you with experience in analysing and interpreting reliability results.

At the end of the project you will have an good understanding of how to translate reliability to theory into practice. Further, reliability measurement and growth modelling are statistical methods; you will be able to interpret the results in the context of the programs we are testing.

Note that you are not expected to fix any of the faults in the provided application; in fact, doing so will make it very difficult for you to successfully complete this project.

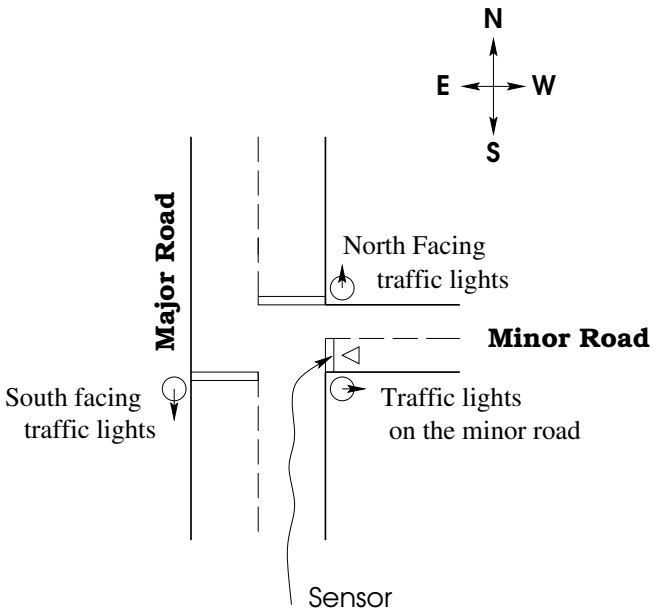

Figure 1: Traffic lights at a T-intersection.

System Specification

A control system must ensure the correct and *safe* functioning of a set of traffic lights at a T-intersection between a major and a minor road. The lights will be green for the major road and red for the minor road *unless* a vehicle is detected by a sensor in the minor road *or* a pedestrian pushes a button to cross the major road.

Note that the sensor is located just behind the lights on the minor road.

If a vehicle or a button push is detected, then the lights will switch from red to green via amber in the standard way and allow traffic to enter the major road from the minor road.

The traffic lights must remain *safe*, that is, the lights in one road must not indicate green until the lights in the other road are *guaranteed* to be red.

As stated, the default state of the intersection is the major road lights showing green and the minor road lights indicating red. When the minor road lights change to green, they should stay green for an interval of four (4) time units. Subsequently, the lights will switch back to the default position in which the major lights are green and the minor lights are red. Again, the lights must be "cycled" so that they ensure the safety of the intersection. Instead of changing green lights directly to red, in order to give approaching cars time to slow down each traffic light must indicate amber for two (2) time units before moving to red.

A time unit is equal to 2.5 seconds.

The traffic lights perform a hardware reset every 24 hours.

Tasks

Reliability Objectives

The project source consists of five (5) builds or versions. Each build represents a (hypothetical) stage in the testing and debugging of the traffic light control system. The goal of the project is to measure the five builds to obtain (simple) estimates of reliability from the five builds.

Reliability Objective – The reliability goal for the traffic light system is less than one failure per 24 hour period.

The intersection has been estimated to experience cars arriving at an average rate of one (1) every three (5) minutes during off-peak hours and at an average rate of ten (10) per minute during peak times. Pedestrians arrive on average once every four (4) minutes, regardless of the time of day.

Instructions

Task 1

Your first task is to plan out your reliability testing effort by creating a testing plan. To be specific you will need to specify the following:

1. What exactly is a failure of the system, and what potential kinds of failures may occur in practice.

   Create a list of potential system failures. You will need to "experiment" with the first build a little to gain an understanding of its failure behaviour
   BUT...
   However much you're tempted, DON'T FIX ANYTHING!
2. You will need to specify your testing strategy in your report for the project and include:
   - how you will select you test inputs, and whether they reflect the descriptions given of the environment in which the traffic light control system must operate;
   - how each of the failures, or kinds of failures, listed above will be detected;
   - how much operating time should be spent on each build in order that the failure statistics you gather be useful;
   - what stubs, drivers and other tools that you will need; and
   - how and where you will log your results.

Assume an operational profile for the sensor inputs. Discuss how your operational profile might differ from the operational profile of an actual traffic light sensor.

Task 2

The next task is to perform the testing and reliability analysis for Build 1, Build 2, Build 3, and Build 4 according to your plan.

- Plot the failure data as both failure intensity against mean number of failures and failure intensity against time.
- Estimate λ_0 and ν_0 for your data, preferably by linear regression.
- Explain why you think that the data that you have collected is an accurate reflection of the true reliability of the system.
- Interpret your data in terms of the effects of the fault detection and removal process hinted at by your data.
- Estimate how long it will take the current testing and fault correction process to achieve the reliability objectives of the project based on your current data.

Task 3

Extend your reliability model with the data from Build 5 and revise your estimates from the previous task. What, if anything has changed? Interpret your data in the context of the failure detection and fault removal process.

Title Page
1. Summary
2. Testing and Reliability Plan
  1.1 Potential Failures of the System
  1.2 Test Input Selection
  1.3 Failure Detection
2. The Analysis of Builds 1 to 5
3. Findings and Conclusions

Figure 2: Table of Contents for your report

Task 4

Write a report on your findings. A suggested structure for the report is given in Figure 2.

Title Page – YOU MUST INCLUDE THE NAMES OF YOUR TEAM MEMBERS, YOUR LOGINS AND YOUR STUDENT NUMBERS!!!

Summary – is a short introduction to your report, listing the key activities that you did and your key findings. Keep the summary brief – its main aim is to give the reader an overview of your report, the key findings, essential information and where to find it.

Testing and Reliability Plan – should include all of the information from Task 1. You should also discuss your operational profile here and how your operational profile might differ from the operational profile of an actual traffic light sensor.

The Analysis of Builds 1 to 5 – should contain all of the supporting evidence for your findings – graphs, raw reliability data, test oracles, reliability estimates and calculations as well as any observations that can be made from the data.

Findings and Conclusions – should be a summary of your project including a discussion of the questions below.

Discussion Questions

(i) Do the reliability graphs or the reliability data tell us anything about the failure detection and removal process? If so, what do they reveal about the development process?

(ii) The traffic lights need to be safe, that is, a green light should not be simultaneously 'on' on the major road and the minor road – this is a safety property of the intersection! Given the failure rate that you have determined for this traffic light control system, how *safe* do you feel the intersection is? Would you be comfortable driving through? If not, what degree of reliability would you require in order to feel safe, and how much testing effort would be required to achieve it?

(iii) We also want to ensure that the traffic lights maintain the flow of traffic. To this end provide an argument that the system maintains a state in which *not* both sets of lights are simultaneously red, that is, either the lights on the major road are green or the lights on the minor road are green. Comment on whether this is enough to provide appropriate "green" time for the major road, given that the major road can be assumed to experience significantly more traffic than the minor road at all times.

Assessment

The report summarising your findings is the critical piece of assessment. Remember it is only worth 20% of your final mark for this subject. We will be awarding higher marks to good analysis of the program and its reliability and demonstration of your ability to think critically about the system under evaluation. It is therefore important to justify your assertions with references to your reliability data or to the theory.