

Software Design (F28SD2):
Exercises in Dynamic Analysis 2
Possible Solutions

Andrew Ireland
School of Mathematical and Computer Sciences
Heriot-Watt University
Edinburgh

Exercise 1

The key safety invariant is: “*The signals associated with the north and west bound roads should never simultaneously display green aspects.*” The program `Controller.java` as it stands violates this invariant, *i.e.*

```
cycle = 0 north = Green west = Red  
cycle = 1 north = Green west = Green  
cycle = 2 north = Green west = Green  
...
```

This violation can be detected if a class invariant is used, *i.e.*

```
assert north != west;
```

The complete code for a “safe” version of the controller can be found in

```
http://www.macs.hw.ac.uk/~air/swdesign/SafeController.java
```