1 Fault Tolerance

a) A well-known fault tolerance mechanism is homogeneous Triple Modular Redundancy (TMR).

- What is homogeneous TMR?
- For which faults can homogeneous TMR provide automatic full fault tolerance and how is this done?
- For which faults can TMR provide no fault tolerance?
- For which faults can TMR provide fault detection, but no automatic fault tolerance?

b) For each of the following code segments, characterise the fault against which protection is attempted, and the level of fault tolerance achieved. Use established terminology for this characterisation.

Hint: Reread section 4.5.1 of the lecture notes.

Segment a)

```
loop
  begin
    Get (Sensor, Data);
    exit;
  exception
    when SENSOR_INPUT_ERROR =>
      Reset (Sensor); -- restoring state
  end;
end loop;
```

Segment b)

```
begin
  Find_Very_Accurate_Solution;
exception
  when Numeric_Instability | Not_Enough_Time =>
    Find_Coarse_Approximation_to_Solution;
end;
```
Segment c)

accept Train_at_Signal; -- train has stopped at signal
Open (Signal);
select
    Train.Proceed;
    Close (Signal);
or
    delay 60.0;
    Close (Signal);
    Controller.Send_Msg ("train not responding");
    raise Unresponsive_Train_Error;
end select;

2 Recovery Points

The following diagram illustrates the concurrent execution of four communicating processes and their associated recovery points (for example, R11 is the first recovery point for process P1).

Explain what happens when an error is detected by P1 at time t. Do the same for P2, P3, and P4.
3 Questions

Are the following statements true or false? Please also provide the reason.

a. Knuth’s Law states that in steady state on average about 33% of the available heap memory is wasted due to fragmentation.

b. If several execution sequences of the same statement are allowed, it is possible that some of those lead to runtime errors while others do not.

c. Forward error recovery is generally much easier to implement than backward recovery.

d. For a language, in which all variables are statically sized (e.g., C or Java), the size of an activation record can be statically determined.

e. A specific parameter evaluation order is prescribed by every programming language.

f. When writing a program, one should define exception handlers only when necessary because they cause a significant run-time overhead during program execution.

4 Case Study

Please read the case study of the Ariane 5 failure available at


and discuss your findings according to the following aspects.

• What was the cause behind the Ariane 5 failure?

• Who is to blame for the reasons which triggered the failure (keep in mind the roles of the involved people)?

• How could this failure have been avoided?

• What do we learn from this case study?