Exercise 2.1: Fault Tolerance

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

- What is homogeneous TMR, and which strategy of fault tolerance does TMR use?
- Describe a faulty scenario in which TMR can provide automatic full fault tolerance. How is this achieved?
- Describe a faulty scenario in which TMR can provide fault detection, but no automatic fault tolerance?
- For which faults can TMR provide no fault tolerance at all?

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

Segment i)

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

Segment ii)

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

accept Train_at_Signal; -- train has stopped at signal
Open (Signal);
select
    Train.Proceed;
    Close (Signal);
or
    delay 42.0;
    Close (Signal);
    Controller.Send_Msg ("train not responding");
    raise Unresponsive_Train_Error;
end select;

Exercise 2.2: Recovery Points

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

a. Trace what happens when an error is detected by process P1 at time t, and how this affects the other processes (if at all). Do the same for P2, P3, and P4.

b. With concurrent processes, what is the negative effect called when rolling back recovery points, and what is the cause of this effect?

c. How can this effect be avoided?

d. What are the advantages and disadvantages of recovery points?
**Exercise 2.3: Ariane 5 Case Study**

Read the Ariane 5 case study found at:


and answer the following questions.

a. What were the causes of the Ariane 5 failure?

b. Categorize the *nature of the software fault*, and the *level of fault tolerance* desired from the software component in which the error occurred.

c. Which type of hardware redundancy was used for the SRIs of the Ariane 5?

d. Determine whether forward or backward error recovery would have been appropriate for dealing with the fault. Justify your answers.

e. Who is to blame for the factors that contributed to the failure (keep in mind the roles of the different people involved), and why?

f. How could the failure have been avoided?

g. What are the lessons learned from this case study?