Software Engineering   4 mark question

safety-critical

Give an example of redundancy in a computer system.
How does this affect reliability, hazards and
safety?

[4 marks]

SOLUTION

A SAFETY-CRITICAL SYSTEM MIGHT INCLUDE DUPLICATE COMPONENTS
SUCH AS A BACKUP PROCESSOR THAT IS SWITCHED INTO A
CONTROL LOOP IF THE MAIN PROCESSOR FAILS. THIS
IMPROVES RELIABILITY, BECAUSE THE SYSTEM WILL NOT
FAIL UNLESS BOTH PROCESSORS FAIL AT THE SAME
TIME. IT HAS NO EFFECT ON HAZARDS, WHICH
RESULT FROM FACTORS EXTERNAL TO THE
SYSTEM. IT SHOULD RESULT IN INCREASED
SAFETY, ASSUMING THAT THE SOFTWARE CONTROL
OF THE BACKUP SWITCHING CORRECTLY AVOIDS
ACCIDENTS THAT MIGHT RESULT FROM A FAULT
IN ONE PROCESSOR