Computer Science Tripos Part IA and IB

2019-2020
Exam Question
Cover sheet

Student BGN2023A**…..……**

Paper2**……**

Question number6**……**

How did you answer this question?

Timed	☐	Open Book	☑
Untimed	☑	Closed Book	☐

Questions

List all the questions you have answered for this paper here. 1,4,6,7,8

Computer Science Tripos Honour Code

1. We take it as a principle that maintaining the integrity and fairness of examinations should be regarded as a collaboration between students and the Department.
2. The students undertake that they will not help others in examinations and will not receive any help from others (students or non-students).
3. Students will actively contribute to ensuring that all students adhere to the code.
4. Students will keep to the conditions of the assessment and will accurately report those conditions when asked.
5. The Department will not make any attempt at remote invigilation of online examinations.

I **undertake to respect the Computer Science Tripos honour code**

Tick the box to confirm ☑

6a) Fault tree analysis is a top-down method of failure analysis, in which each system failure is traced back to its contributing component failures, so that measures can be put in place to avoid those. This is done using a fault tree, and may be used to assign probabilities to types of failure. It is most effective when only a few system failures are possible, but many component failures can contribute to them.

b) Failure modes and effects analysis is a bottom-up method of failure analysis in which each component or subsystem is examined for what failures it may produce, and those are then related to their effects on the rest of the system. It is most effective when there are only a few components in the system.

c) In the Therac-25 accidents, failure modes and effects analysis (FMEA) may have fallen short in various ways:

- The particular issue with the Therac-25 machine was due to the interaction of multiple components - the turntable was not in place when the beam fired - which may not be picked up on by FMEA, which primarily inspects individual components.
- The process of FMEA is based on examination of known failures (not necessarily all possible, but improbable failures), which may not always be testable.
- Similarly, FMEA may only examine the intended use of an interface, but in the case of Therac-25 the specific operation which led to accident was unanticipated by the manufacturers.
- FMEA relies heavily on the experience of engineers to identify common failures of particular components, but in this case, many of the components had already seen use in the Therac-20 predecessor, so may have been assumed reliable.
- Particularly since the design of the machine was taken from a previous version, the application of FMEA after the design was mostly complete was probably too late, and these methods should have been used before then.

d) In the case of the Therac-25, fault tree analysis (FTA) may have prevented the accidents:

- Since the malfunction in the machine was due to a fairly obvious unwanted outcome, it is likely that FTA could have identified it.
- In particular, this specific malfunction was already considered by the manufacturers, since in a previous version there was a mechanical interlock to prevent its occurence.
- Since the fault tree looks at the combined results of individual component failures, this may have been suited to spotting the result of the joint causes for the accidents.
- However, the exact conditions resulting in the accident were a little more subtle, so they may have been difficult to deduce.
- Also, like FMEA, the FTA would have likely been applied too late to a project for which the blueprints were already in place from a previous version.

- In fact, fault tree analysis was used to examine the Therac-25 machine, but it was used improperly to estimate likelihood of this kind of accident, assigning a random probability.