

Critical systems requirements 2

Name:

1. What is risk-based requirements analysis?

An approach to requirements analysis that focuses on the risks or threats to a system and what can be done to avoid, tolerate or reduce the impact of these risks..

2. List three risk mitigation strategies?

Risk avoidance
Risk management
Damage reduction.

3. Describe 4 types of asset that may have to be protected?

System operators
People and things in the system's environment
The system itself
Other systems that are controlled or protected by the system being analysed

4. What is top-down and bottom-up hazard identification?

Top down identification – starting with potential risks, identify the states of the system and environment that can cause these

Bottom up identification – start with what might go wrong and work out what incidents that this could cause.

5. Describe 4 hazard classes?

Physical hazards – associated with the physical state of the system
Electrical hazards – associated with the electrical state of the system
Control hazards – associated with the software controlling the system
Data hazards – associated with the system's data

6. What does ALARP mean?

As low as reasonably practical – the system designers must do everything that is reasonable to reduce the risk. However, incurring very high costs may not be justified.

7. What is a fault tree?

A diagrammatic representation with an identified fault at the root of the tree. The tree is used for causal analysis to discover the conditions that can cause that fault to arise.

8. How does a 'safe operating envelope' work?

The operation of the system is constrained by built-in checks so that it always operates between limits that are known to be safe.