Book Questions
Chapters 11
Devayan Mandal

11.3 A train protection system automatically applies the brakes of a train if the speed limit for a segment of track is exceeded, or if the train enters a track segment that is currently signaled with a red light (i.e., the segment should not be entered). Giving reasons for your answer, explain which reliability metric you would use to specify the required reliability for such a system.

Ans: The given scenario of a train outside it's speed limit or in a track segment which has a red light can have serious consequences. The POFOD - probability of failure on demand system fits the train protection system requirements more appropriately because if the service request is not met in a timely manner, a serious system failure could occur. The frequency of service requests is not frequent in the POFOD system and this further fits the train protection system because frequent cases of train speeds exceeding the safe limit or speeding in a red light track segment is not expected.

11.4 What is the common characteristic of all architectural styles that are geared to supporting software fault tolerance?

Ans: A common scenario for a fault report in a software system will be the presence of a bug. The bug can be a single error or multiple errors in the software or malfunctioning of a certain hardware component of group of hardware components. In all probability, the system's technical support team will be capable of addressing the area concerning hardware failure. But for architectural styles specifically geared towards fault tolerance, inbuilt software needs to be written, executed and dedicated towards detecting bugs. The architectural style will ensure that software components within the system will be fully capable of internally addressing a software bug or have a course of action set in place if external aide is required.

11.6 You are responsible for the design of a communications switch that has to provide 24/7 availability but that is not safety-critical. Giving reasons for your answer, suggest an architectural style that might be used for this system.

Ans: An architectural style which might be appropriate for this case is N version programming. N version programing offers self-monitoring functionality and this coincidences with the primary requirement of the communications switch i.e. to provide 24/7 availability. This will be made possible because N version programming offers multiversion programming. If

a fault is detected, the architectural style can provide the output through a different version present in the system. A protection based system like POFOD is not required in this case because the system is not safety critical.