Fault tolerance is a specialized kind of planning for change.An example of successful fault tolerance occurred when the Cassini spacecraft, currently on an extended mission to Saturn, unexpectedly ceased communication with ground operations on Nov. 2, 2010.Communication was restored within the hour, at which point human operators began a slow and careful check of the spacecraft followed by recovery activities such as clearing error log files and turning science instruments back on. Recovery actions were completed on November 24, and the Cassini spacecraft continues to be healthy at the time of this writing.Software is growing to handle not just failures (e.g., the Cassini bit flip), but also a range of other unexpected situations (e.g., novel usage scenarios) and contingencies (e.g., debris temporarily blinding the spacecraft camera).However, as Dvorak et al. note, extending the techniques of onboard fault protection to cover a wider range of software failures can also increase algorithmic complexity, which makes the software harder to verify [2]Developing robust software that can handle failures and other conditions that threaten the mission begins with a thorough systems and software hazards analysis.Software requirements to protect the spacecraft from mission-critical failures are derived from these hazards analyses.As described at the Cassini website, the onboard fault-protection software quickly switched to a backup computer and shut off non essential power loads.It is not surprising, given the long life and hostile environments encountered by spacecraft, that failures occur.As spacecraft and their missions become more complicated, the number of unwanted scenarios that the software must handle increases.The software had been designed to configure the spacecraft to a safe but degraded state when communication was lost.It switched to an alternate (low-gain) antenna, pointing it toward the sun to improve the chances of communicating with operators.The fault protection software on spacecraft continually monitors for deviations between the expected spacecraft state and the actual spacecraft state.Fault recovery software is especially important because it is usually invoked when something has .already gone wrong on the spacecraft.It was later determined that this was caused by a flipped bit