Ali Mojibi

Therac-25 Reading Report

The unfortunate accidents of Therac-25 that cost human lives were mainly due to implementation flaws in the device operating system. Lack of a single core to manage hardware access and division of regulatory tasks into an array of subroutines made synchronization and error checking much too difficult. While such excessive software complexity took away any small room for error, extensive and incorrect usage of shared variables as the means to control the device operation and to maintain its proper state was more than enough to cause deadly accidents.

In one case, for example, lack of synchronization between Datent, Ptime, and Magnet subroutines caused a change in data entry to remain undetected to the device: sharing memory space among subroutines, uncontrolled and unprotected access to that space, and synchronization errors are clearly flaws of the device operating system implementation. In another case, a similar type of problem in updating the "data-entry completion" variable in Datent would lead to a race condition, revealing another major flaw in implementation of the Therac-25 operating system.

The excessive complexity of Therac-25 software did not only affect its operation; it also made it that much more difficult to test the device. In fact, failure in proper and adequate testing is perhaps the second most significant cause of the overdose accidents trailing after the implementation flaws. Lack of a clear test plan and failing to adequately test the device software on its own let important programming errors go unnoticed by the AECL engineers.

Testing software independently of the entire system is crucial in debugging complex machines since it may not always be possible to produce all test case scenarios for a variety of software subroutines at a system level. In the Tyler accident case, for example, an update in data entry needed to be performed in less than 8 seconds to trigger a specific fault. While a system-level simulation and testing of such a scenario would have been almost impossible without hindsight, a thorough analysis of the software using clear test routines could have possibly manipulated and detected the programming error.

AECL's incapability to test the device became quite apparent when the company engineers failed to detect the main cause of the first reported problem for a significant while after the accident had taken place. In fact, as the investigation report indicates, the micro-switch bit-error that was initially announced to be the cause of that accident was likely not to have been a major factor at all. Since like many other modern-day systems, safety interlocks of Therac-25 were heavily dependent on software, a thorough and independent testing of the software was paramount to safety of the device. Yet, AECL failed to administrate sufficient testing and death and suffering were administrated to some unlucky patients instead.