Nada AMIN 6.033 February 14, 2006
Rinard, TR 12 One-Pager #1

Report on *An Investigation of the Therac-25 Accidents*

The Therac-25 was a computerized radiation therapy machine, which caused several accidents, including deaths by massive overdoses, because of its malfunctions. Here, I will describe two problems, one in design and one in testing, and how they contributed to the accidents.

The Therac-25's predecessor, the Therac-20, shared many of the flaws of the Therac-25, and yet, the Therac-20 didn't cause any serious accidents by massive overdoses. Because it "had been designed around machines that already had *histories of clinical use without computer control*, … [the Therac-20] … had independent protective circuits for monitoring electron-beam scanning, plus mechanical interlocks for policing the machine and ensuring safety operation" (20). In the Therac-25, these hardware safety mechanisms were not duplicated, probably because they might have appeared to be an unnecessary cost. Instead, the Therac-25 relied more on software, which meant that a bug in the software was more likely to lead to a serious accident – and it did. Given the safety-critical nature of the system, sparing the redundant hardware protection was very risky.

The decision to rely on the software almost exclusively might have been understandable, had the software been tested sufficiently thoroughly to justify such a high confidence. Unfortunately, the software clearly wasn't tested methodically. It seemed that the testing consisted mostly of "2,700 hours of *use*" (20). It is unlikely that typical use would capture the subtle cases where the code fails. Most likely, the thousands of hours would just be repeating a few most common cases – which is not efficient, nor reassuring. In fact, one bug in the software, that triggered at least two tragic accidents, would probably have been detected by more thorough testing. The bug was that editing on the screen could possibly go unnoticed while the physical system was set up. This bug was buried in the code as it involved not a single subroutine but the interactions among a few of them. It could have been uncovered by testing whether the system indeed detected changes in input during the physical set up.

In conclusion, the software of the Therac-25 assumed a safety-critical role, which was not only unnecessary but also unjustified given the poor testing.