

B Good writing flow, but:
- who should have noticed the warning sign? what should they have done?
- many statements could be made more specific.

Dan Ports

February 10, 2003

R9: Karger TR1

v Generally good job though. — Chris

Misplaced Trust in Software in the Therac-25

The Therac-25's catastrophic failure was principally caused by errors in the control software. The first patient injuries reported to the manufacturer revealed the inadequacy of the software interlock system for ensuring safe operation. ~~The critical flaw was that~~ the designers did not take into account the possibility of software failures, in spite of the fact that the system's safeguards were implemented exclusively in software.

warning sign?

The Hamilton clinic incident, the first injury reported to the manufacturer, resulted from the turntable being in the incorrect position when the beam was activated. This unsafe condition should not have been possible, and the fact that it occurred should have served as a warning sign that the system design was deeply flawed. The system should have had carefully validated interlocks in place to ensure that unsafe conditions could not exist. Instead, the designers chose a software system that was not sufficiently reliable.

A warning sign to whom? what should that person have done?

red.

~~AECL's engineers relied on software for safety-critical elements of the Therac-25, and assumed the software was infallible. They consistently failed to acknowledge that design or implementation errors in the software could lead to safety problems.~~ In the initial design, they generated a fault tree, identifying potential ways in which the hardware could fail. However, software errors were not included in this fault tree, apparently because the engineers simply assumed the software was correct and would never fail. ~~The number of software errors later encountered reveal the fallacy of this thinking.~~ In fact, this form of incomplete safety analysis may have been more damaging than performing no safety analysis at all: the misleading probabilities specified for hardware failures conveyed a false sense of reliability, and led at least one user of the system to assume that it must have been safe.

Not included: I think they were, but with low probability

Spec.?

Once problems began to appear, AECL focused on fixing specific bugs as they became aware of them. This approach could not make the system safe. ~~Engineering a complex software system like the Therac-25's is no simple task, and making it bug-free is practically impossible.~~ As each bug is fixed, it is only a matter of time until the next bug is exposed, ~~as was seen with the multiple bugs encountered in the Therac-25.~~ To develop a safety-critical system, it is necessary to identify specific invariants that must be maintained: for example, the beam must not be able to turn on if the turntable is not verified to be in the correct position. These invariants must be maintained by carefully tested safety interlocks. It is possible to rely on software, but only if it has been very

Good, spec. ex.

Spec: how can it be proven?

carefully tested and proven to ensure safe conditions: the reused, inadequately-tested code in the Therac-25 certainly does not meet this standard. A set of redundant interlocks is best; the Therac-20 caused no injuries despite probable software flaws because a separate hardware safety shut down the system. ~~If those types of interlocks had been present in the Therac 25, these tragic injuries may have been averted. (obvious, e.g. red.)~~

How was Therac testing inadequate?