Online Ethics Center
FOR ENGINEERING AND SCIENCE

An Investigation of the Therac-25 Accidents (Abstract)

Author(s)

Nancy G. Leveson
Clark S. Turner

Year

1993

Description

This is an abstract of a 1993 article from IEEE Computer about the Therac-25 computerized radiation therapy machine and its software flaws, which caused massive overdoses to patients.

Body

The Therac-25, a computerized radiation therapy machine, massively overdosed patients at least six times between June 1985 and January 1987. Each overdose was several times the normal therapeutic dose and resulted in the patient's severe injury or even death. Overdoses, although they sometimes involved operator error, occurred primarily because of errors in the Therac-25's software and because the manufacturer did not follow proper software engineering practices.

Overconfidence in the ability of software to ensure the safety of the Therac-25 was an important factor which led to the accidents. The Therac-20, a predecessor of the Therac-25, employed independent protective circuits and mechanical interlocks to protect against overdose. The Therac-25 relied more heavily on software.

Moreoever, when the manufacturer started receiving accident reports, it, unable to reproduce the accidents, assumed hardware faults, implemented minor fixes, and then declared that the machine's safety had improved by several orders of magnitude.

The design of the software was itself unsafe. The Therac-25 supported a multitasking environment, and the software allowed concurrent access to shared data. This precarious implementation caused program failure under certain conditions.

Risk assessments were, from the start, unrealistic. A risk assessment performed by the manufacturer seems to consider only hardware failures as it lists the possibilities of the computer selecting the wrong energy or mode as 1e-11 and 4e-9 respectively. Justification never appears for these numbers, but, more surprisingly, the company accepted this low risk assessment easily.

Follow-through on accident reports was unacceptable. After one accident, the manufacturer tried to reproduce the condition which occurred at the treatment. When it could not, it concluded that a hardware error caused the accident, and implemented a solution based on that assumption. It declared that the system was several orders of magnitude safer, but accidents did not cease.

The Therac-25 incidents demonstrate that several misconceptions in the manufacturer's attitude led to the accidents. Poor software design, overconfidence in the software's abilities, unreasonably low risk assessments, and poor manufacturer response to complaints all contributed to the overdoses. Companies must understand that for safety-critical software design rigorous testing and failure analyses are essential and that trained software engineers, not simply any reasonably experienced engineers, should implement the software design.

See also:

- ComputingCases.org Case Materials for Therac 25
  - An extensive case with teaching guide, also based on Levenson and Turner's article. The Computing Cases website also has other materials for the teaching of computer science ethics.
- Nancy Levenson's Home Page at MIT
  - Levenson's page includes a later version of the article abstracted here and many other articles on software safety

Notes

Nancy G. Leveson and Clark S. Turner (abstract by Philip D. Sarin) "An Investigation of the Therac-25 Accidents" IEEE Computer 26.7 (July 1993): 18-41.

Contributor(s)

Philip D. Sarin

Rights

Resource Type

Case Study / Scenario

Parent Collection

Therac-25

Publisher

Online Ethics Center