Rohita Gangishetty

Michael Minzey

Computers and Modern Society

7 July 2024

Therac-25

Atomic Energy of Canada Limited (AECL) developed the Therac-25 in 1982 as a linear accelerator for cancer treatment which is a computer-controlled radiation therapy machine. The accelerator's operations and safety mechanisms were largely reliant on software. The machine was infamously unreliable, frequently malfunctioning on a daily basis. Tragically, it administered significant radiation overdoses to six patients, resulting in three fatalities, over a 20-month period from June 1985 to January 1987. These incidents were significantly influenced by the reliance on software safety features over hardware safety features and the reuse of code from prior models without sufficient testing.

The Therac-6 and Therac-20, which came before the Therac-25, had both hardware and software safety measures and could work without their control computers. But AECL's choice to make the PDP 11 minicomputer an important part of the Therac-25's operation, along with the loss of many hardware safety features, made the machine more likely to have software mistakes. While this method was meant to save money, it actually made people less safe.

The high number of incidents with the Therac-25 can be attributed to several factors. Primarily, the system relied heavily on software for its safety mechanisms, unlike its predecessors, which incorporated hardware interlocks. This over-reliance on software increased the risk of undetected errors causing harm. AECL reused code from the Therac-6 and Therac-20 without thoroughly testing it in the new context of the Therac-25, assuming its reliability would carry over, which proved incorrect. Additionally, AECL's investigation into initial reported incidents was insufficient, leading to repeated accidents. Communication failures between AECL and the machine's users also exacerbated the issue, as AECL downplayed the possibility of malfunctions leading to overdoses even after multiple incidents.

The Therac-25 software contained significant bugs, primarily involving race conditions. One such condition occurred when the operator corrected a mistake quickly; if the change was made within the time the magnets were still moving, the system failed to detect the edit and proceeded with the old settings, leading to an overdose. Another race condition involved the electron beam gun positioning, where a variable indicating the gun's position could roll over from 255 to 0. If the operator pressed the SET button at the exact moment this rollover occurred, the system incorrectly interpreted the variable, causing it to fire prematurely and deliver a massive dose of radiation. These bugs, along with the lack of hardware interlocks and proper safeguards, made the Therac-25 prone to catastrophic errors, resulting in multiple incidents and fatalities.

The ethical and professional responsibilities that the manufacturer AECL (Atomic Energy of Canada Limited) and their computer programmers violated can be analyzed using the Software Engineering Code of Ethics.

Principle one is Public. In clause 1.01, it states that software engineers should accept full responsibility for their work. At first, AECL didn't fully take responsibility for what happened, which made it take longer to fix the serious problems with their product. They didn't take full responsibility for the safety of their goods because they didn't look into the first cases right away or thoroughly. Clause 1.03 emphasizes that software should only be approved if it is safe and meets specifications. There were major safety problems with the Therac-25's software, and it wasn't tested fully, which led to terrible results.AECL cleared and dispatched the Therac-25 into service without properly checking to make sure it was safe, which is a straight violation of this rule. Additionally, Clause 1.04 mandates disclosing any potential danger to appropriate persons or authorities. This rule was broken when AECL didn't quickly warn of the possible risks after the first events. This puts public safety at risk. Principle 1 says that people should care about the health, safety, and happiness of others. These acts go against that principle.

Principle 2 is client and employer. AECL violated clause 2.01, which requires providing services in areas of competence and being honest about limitations. AECL wasn't honest about how safe their software was because they didn't talk about its flaws and possible problems enough. Furthermore, Clause 2.05, which mandates keeping confidential information private unless public interest is involved, was violated when AECL initially kept information about the problems and risks secret, putting clients and the public at risk. AECL did not act in a way that was best for their clients and the public because they put the needs of the company ahead of the safety and well-being of their clients and the public.

Principle 3 is that the product was also violated. Clause 3.01 requires striving for high quality, acceptable cost, and a reasonable schedule, ensuring significant trade-offs are clear. Cost and timeline were more important to AECL than thorough testing, so they didn't make sure the Therac-25 was safe and of good quality. Clause 3.10 emphasizes the need for adequate testing, debugging, and review of software. The serious software bugs in the Therac-25 made it clear that there wasn't enough testing and review, which led to bad results. Software engineers are required to make sure their products and any related modifications meet the highest professional standards, and this failure to ensure that products meet those standards is a clear violation of that principle.

Principle 4 is judgment states that it requires maintaining integrity and independence in professional judgment. Clause 4.01 states that technical judgments should support and maintain human values. AECL did not put people's safety first when making technology decisions, as shown by the fact that they did not fix known problems and kept using broken software.Clause 4.05 says that conflicts of interest must be reported. It's clear that AECL wasn't honest about the ways their business goals and safety worries were at odds with each other. AECL did not make choices that put people's safety and well-being first, which shows a lack of professional sense and honesty.

Principle 5 is management. Clause 5.01 mandates ensuring good management for any project, including effective procedures for quality promotion and risk reduction. AECL's management failed to implement effective procedures to ensure the quality and safety of the Therac-25. Clause 5.11 also says that managers can't ask software workers to do anything that is inconsistent with the Code. This rule would have been broken if AECL's management told engineers to put meeting targets ahead of thorough testing. The concept of ethical management in software development is directly broken by bad management practices that don't improve quality and lower risk.

Principle 6 is profession.Clause 6.01 requires helping develop an organizational environment favorable to acting ethically. AECL did not create that kind of atmosphere because the way they handled the events showed that they did not care about ethics or public safety. Clause 6.10 advises avoiding associations with businesses and organizations that conflict with the code, AECL's decision to keep running and releasing software even though there were safety concerns went against ethical standards.

Principle 7 is colleagues which mandates fairness and support towards colleagues. Reviewing other people's work in a fair and honest way is emphasized in Clause 7.04. The software wasn't reviewed well enough, and the first problems weren't properly recorded or fixed. This shows that there wasn't enough peer review and writing. Not helping and being fair to coworkers with review and feedback methods goes against the professional concept of helping and being fair to coworkers.

Lastly, principle 8 is self which requires lifelong learning and promoting an ethical approach to the profession.Clause 8.06 stresses the importance of learning more about the Code, how to understand it, and how to use it. The fact that AECL and its experts broke the code of ethics so many times shows that they didn't understand or follow it properly while working on the Therac-25. If AECL and its experts were dedicated to lifelong learning and doing things in an honest way, they would have fixed the bugs in their software sooner.

If the issues with the Therac-25 had remained undisputed or undiscovered, the global impact could have been severe. Potentially fatal radiation overdoses and widespread exposure would have had a direct impact on public health, raising medical expenses, provoking lawsuits, and undermining public confidence in medical technology. Economically speaking, this may have put a heavy financial strain on healthcare systems and providers around the world, increasing the expense of legal fees, equipment replacement, and regulatory compliance, among other things. The harm to AECL's and other manufacturers' reputations would have discouraged investment and innovation in medical technology, which would have had an impact on patient outcomes and the delivery of medical technology.

Radiation therapy machines play a crucial role in treating cancer by delivering targeted radiation to destroy cancer cells. However, their operation and maintenance can impact the environment in several ways. Firstly, these machines contain components like lead and mercury. When these parts are replaced or repaired, it's essential to handle them properly because these materials can be hazardous if not managed correctly. Improper disposal could lead to environmental contamination, affecting soil, water, and potentially harming wildlife and human health.Secondly, radiation therapy machines consume significant amounts of electricity to operate effectively. This high energy consumption contributes to greenhouse gas emissions and air pollution, indirectly impacting the environment. Efforts to minimize energy use or adopt energy-efficient technologies can help mitigate this impact. Overall, while radiation therapy machines are vital for medical treatment, their environmental footprint needs careful consideration. Responsible management of their components and energy use is essential to minimize adverse environmental effects while continuing to provide life-saving treatment for cancer patients.

AECL uses social context towards hospitals and clinics for them to keep continuing using their machines. To persuade hospitals and clinics to keep using their equipment despite the accidents, AECL most certainly combined technical assistance, training programs, and maybe financial incentives. To keep confidence, they may have underlined the historical dependability of their older model like Therac-6 and Therac-20 which downplayed the seriousness of the events, and given promises of continuous development and safety precautions. Their reputation may have been strengthened even further by partnerships with prestigious medical schools and sponsorships of powerful doctors, therefore promoting ongoing use.

As a software engineer at AECL handling inquiries from clinics after incidents, my main focus would be on ensuring transparency and taking proactive measures. Every inquiry will be carefully examined and addressed, with comprehensive investigations conducted to identify and understand the issues. You can expect detailed explanations regarding any software bugs and their potential impact. First and foremost, it is crucial to take immediate action by releasing patches or updates to address any vulnerabilities that have been identified. Additionally, it is important to conduct thorough testing and validation to ensure the effectiveness of these measures. Lastly, comprehensive training should be provided to healthcare professionals to ensure they are well-equipped with safe usage practices. Working closely with governmental organizations and independent experts is crucial to rebuilding trust and ensuring commitment to the highest safety standards. Building confidence in AECL's products and reducing future risks would require consistent communication, support, and a dedication to improving software design and safety protocols.

Works Cited

Gotterbarn, Don, et al. "Software Engineering Code of Ethics." *Communications of the*

*ACM* vol. 40, no. 11, Nov. 1997, pp. 110-118. DOI: 10.1145/265684.265699.

Huff, Charles. "A History of the Introduction and Shut Down of Therac-25." *Online Ethics*

*Center*, 2003, https://onlineethics.org/cases/therac-25/history-introduction-and-shut-down-therac-25.

Lichter, Katie E., et al. "Quantification of the Environmental Impact of Radiotherapy and

Associated Secondary Human Health Effects: A Multi-Institutional Retrospective Analysis and Simulation." *The Lancet Oncology*, vol. 25, no. 6, June 2024, pp. 790-801, https://doi.org/10.1016/S1470-2045(24)00148-7.