EGS 4034 - ENGINEERING ETHICS AND PROFESSIONALISM
TEAM 3 – LIST OF PARTICIPATING MEMBERS:
Joshua Main-Smith
Stephen McDonald
Jordan Roysdon
Troy Crawford

ASSIGNMENT 3

---

1. **Explain the nature and purpose of the Therac-25, and how it was different from previous versions of the system.**

The nature of the Therac-25 is unlike its previous versions. The machine was produced by Atomic Energy of Canada Ltd. (AECL), a Canadian company. In conjunction with a French company, GCR, previous versions such as the Therac-6 and Therac-20. The Therac-25 was the first radiation machine to rely completely on software. Unlike the previous version, Therac-6 and Therac-20, had been designed around other machines that had clinical history that did not have software control. Both machines used a hardware interlocks for safety. However, the new Therac-25 did away with the hardware safety features and relied completely on software. Positioning the machine and entering the strength of radiation treatment was done through software. The Therac-25 did reuse portions of the Therac-6 and Therac-20 software. In addition, Therac-20 used independent circuits for monitoring the electron beam and mechanical interlocks to monitor the machine for safety. Both the Therac-6 and Therac-20 demonstrated an exceptional safety record [1].

The purpose of the Therac-25 is to provide radiation therapy to cancer patients. This machine uses a linear accelerator to deliver X-ray photons at 25 MeV, or electrons with a prescribed strength from the doctor. The electrons are used to treat tumors that are close to the skin. However, the X-rays are used to treat tumors that are deeper therapeutically. When using the electron mode, the Therac-25 creates a high energy beam on tumors with

minimal impact on surrounding healthy tissue. The higher dosage of electrons can target a tumor deeper under the skin without damaging shallow healthy tissue. This phenomenon is referred to as "depth dose". The amount of radiation is set before the procedure is conducted. If the dosage of electrons is too high, a patient can experience severe radiation poisoning which can result in burn marks and blisters on the skin or even eventual death [1].

2. **Summarize the key fundamental impacts resulting from system failures. Explain the main reasons that resulted in the incidents.**

The system glitches and failures resulted in severe patient injury as well as several deaths due to overdose. Aside from human error, systems engineering, software engineering, and lack of "fail-safe mechanisms" [2] are to blame for the incidents.

Between June 1985 and January 1987, there were at least six instances where an error in treatment utilizing the Therac-25. The average experience was similar to that of an account described in the text that ultimately ended in severe radiation poisoning and death of the patient. The machine's malfunctions caused the operator to believe the treatment was not yet complete, and so another dosage was administered. But in reality, the patient had received over ninety times the amount of rads he was intended to, all concentrated in a small, singular spot on the patient. The machine malfunctions caused several people to not only endure unnecessary pain, but to lose their lives. These both could have been prevented if the proper steps had been taken before allowing this machine to be responsible for such important treatments.

During design, the engineers neglected to include several features that would have had a tremendous effect on the outcome for these patients. The machine did not allow for an efficient way to correct an error entered by the operator – should they enter incorrect information initially, but change the settings so they are correct prior to turning the beam on, chances are the beam will still deliver the initial incorrect dosage [2]. The machine required time to reset, but did not alert operators to this waiting period. Additionally, because the machine did not incorporate any hardware related fail-safes, like its predecessors, there was no way to manually shut the beam off in an emergency should an excess amount of radiation be detected [2]. The machine was supposed to be programmed to do this on its own, but clearly it failed to do so. Beyond the design flaws itself, the machine did not receive the proper documentation and testing that it should have before being available for medical use [2]. Thorough testing is vital for any product that is put out to ensure consumer safety and satisfaction, especially when concerning medical treatments as serious as radiation. Furthermore, although the engineers are not completely liable for anticipating all human error that could occur, the machine should be able to protect the patient from extreme harm at the very least unless given a specific override. All of the previous points surmount to this, however it is still important to mention.

3. **Compare the ethical principles outlined in the ACM Code of Ethics. Identify (as they are outlined in the code) and explain those that you believe are most relevant and applicable to the issues in this case study.**

Section 1.1: Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing

The key thing to take from this principle is that engineers need to create products that ensure the safety of society, especially within the realms of critical infrastructure. Handling material that could threaten the lives of others should be handled carefully and thoughtfully. The productions and distribution of Therac-25 was done without

thoroughly testing for any bugs – a critical step for software that impacts the health of others.

Section 1.2: Avoid harm.

The question of Therac-25 causing unjust harm is self-evident. The patients trust the medical staff to give them the best feasible treatment for their condition. The medical staff know how to use the equipment, but they aren't expected to know the inner intricacies of how the software and hardware works. These are for the engineer to know and implement. This principle was violated by failing to minimize the unintentional harm of others.

Section 2.1: Strive to achieve high quality in both the processes and products of professional work.

A high-quality product can be different depending on its purpose. Functionality is usually one of those aspects as a client generally expects a product to work as intended. In the case of Therac-25, one functionality that is expected to work as intended are the failsafe mechanisms that prevent radioactive material from hitting the patient until there is an assurance the product will work as intended. This was attempted using a software directed failsafe, but this was unfortunately ineffective compared to the hardware failsafe mechanisms in previous versions. This would be expected to be caught with proper bug testing and quality assurance.

Section 2.2: Maintain high standards of professional competence, conduct, and ethical practice.

Professional competence, in the context of Therac-25, requires the recognition of what needs to be tested, how it is to be tested, the risk of software failure, the consequences of software failure, the best way to minimize harm, and to have the appropriate skills to effectively produce and distribute a product to society. Therac-25 failed to meet these standards.

Section 2.5: Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

The patients coming to the doctor with their condition will trust the doctor to give them the best treatment they can within their ability. The doctors and medical staff in turn trust the equipment and technical products that have been purchased to work as they are purported to work. This trust increases as a product's reliability has gained a reputation (as was the case with previous versions of Therac working as intended). This trust gives all professionals to work effectively within the scope of their responsibilities. The extraordinary care that was needed to produce Therac-25 was missing.

Section 3.1: Ensure that the public good is the central concern during all professional computing work.

The production of Therac-25 could be considered an endeavor in keeping the public good the central concern of their professional work when considering the product can increase the longevity of many people. The final product, on the other hand, resulted in

shortening the lifespan of several people due to its shortcomings. Developing a product like this requires a focus not only on the positive effects it can have on society, but also the negative consequences if it fails and to evaluate its risk. As such, the public good was not fully the central concern of AECL.

Section 3.6: Use care when modifying or retiring systems.

The previous iterations of Therac had worked as intended. The issue with Therac-25 arose with a switch between using systems failsafe mechanisms to software failsafe mechanisms. Regardless of the reason for making this switch, care should be taken when switching features of a product by using thorough testing. In hindsight, switching from a systems failsafe approach to a software one cost the lives of several people.

4. **Lecture 9.1 discussed the types of moral responsibilities that exist in engineering and technology organizations. Evaluate and summarize the types of responsibilities involved in this case.**

Atomic Energy of Canada Ltd (AECL) has a moral responsibility to notify their clients and the public as soon as an issue was recognized. Evaluating the moral responsibilities involved in this case meant lives were endangered and that required an urgent reaction. Furthermore, errors in similar such projects require investigations and considerations. For example, engineering code of conduct states that, “hold paramount the public safety, health and welfare.” Therefore, we must first look at the blame responsibility, or more specifically the person, team, or organization responsible for the error. If further investigations reveal that specific teams or individuals removed the safety hardware of the Therac-25, without knowing the ramifications, this could be considered an honest mistake. On the other hand, this error could be considered negligence if the engineers were working in a field that they did not feel competent within. However, honest mistakes do occur, and the nature of the negligence can be determined using blame responsibility or oversight responsibility.

Throughout the course, the idea that engineers have an obligation to use reasonable care to prevent harm to others is prevalent. Considering the AECL did not use reasonable care by removing safety hardware and relying exclusively on the software to work correctly. Based on this information, one could surmise this was a negligent mistake. "Many software engineering errors were made during the development of the Therac-25, including inadequate documentation and testing of the software modules and the software" [2]. In order to protect public safety and welfare, engineers are not only responsible for carrying out their work competently, but they must also be aware of the broader ethical issues. Based on the case study, AECL did not demonstrate professional responsibility by working diligently and competently.

Official responsibility stems from one's job or office. Therefore, considering the engineers role in the organization will be crucial in blame responsibility. For example, was there something in design or implementation that a diligent senior engineer or engineering manager could reasonably detect? One key concept with respect to engineering responsibilities is the idea of using due care. Although, engineers can never account for all mistakes and misuse, this organization violated their responsibility to act within a reasonably prudent fashion of another individual acting under similar circumstance. Based on the engineering code of conduct this is a breach of the standard of care and a textbook case of negligence.

References

[1] N. Leveson and C. S. Turner, "An Investigation of the Therac-25 Accidents," *An Investigation of the Therac-25 Accidents*. [Online]. Available: https://web.mit.edu/6.033/2004/wwwdocs/papers/Therac_1.html. [Accessed: 16-Mar-2021].

[2] C. B. Fleddermann, in *Engineering ethics*, 4th ed., Upper Saddle River, NJ: Prentice Hall, 2012, pp. 131–134.

ACM Code of Ethics

TEAM 3 PEER AND SELF EVALUATION MATRIX

ASSIGNMENT 3	Jordan Roysdon	Joshua Main-Smith	Stephen McDonald	Troy Crawford	**TASK MGR.(Y/N)**
Jordan Roysdon	100	100	100	100	Y
Joshua Main-Smith	100	100	100	100	N
Stephen McDonald	100	100	100	100	N
Troy Crawford	100	100	100	100	N
AVERAGE	100	100	100	100	