The Therac-25: A Case Study in Software Safety

Introduction

The Therac-25 was a linear accelerator designed to treat cancer patients with either X-rays or electron beams. Developed by Atomic Energy of Canada Limited (AECL), the machine was heavily reliant on software, unlike earlier models. Unfortunately, a series of incidents between 1985 and 1987 revealed severe flaws, with several patients receiving massive radiation overdoses, leading to painful injuries and even fatalities.

The Problem

Therac-25's design flaws stemmed primarily from software bugs, lack of proper safety mechanisms, and poor user feedback:

- **Software Bugs:** A critical software error occurred when operators switched modes quickly, bypassing essential safety checks.
- **Poor Feedback:** The interface provided minimal feedback on system status, so operators weren't alerted to critical errors.
- **Isolation and Lack of Escape:** Patients were isolated from the operator without adequate communication. In one instance, the intercom was broken, and the video monitor was unplugged, so the operator remained unaware of the patient's distress.

Organizational Issues

AECL initially denied any fault, attributing incidents to operator error and ignoring the software issues reported by hospital staff. This lack of transparency delayed corrective measures and further exposed patients to harm.

Outcomes and Lessons Learned

The Therac-25 incidents underscored the need for rigorous testing and user-centered design in medical devices:

- **Rigorous Testing:** Software-based safety systems alone proved insufficient, emphasizing the importance of hardware backups.
- **Clear Feedback Systems:** Medical devices must alert operators to issues clearly and promptly to prevent misuse.
- **Regulatory Changes:** The incidents led to the establishment of stricter FDA regulations, requiring comprehensive testing for medical device software.

Conclusion

The Therac-25 case remains a powerful reminder of the risks associated with software in critical systems. It demonstrates the necessity of robust testing, transparent communication, and putting patient safety at the forefront of medical technology design.