Software Engineering Homework 1

Jude Jang

The blame for the Therac-25 accidents cannot solely be put on any one party. However, the party most responsible for the Therac-25 accidents is Atomic Energy of Canada Limited (AECL), the manufacturers for Therac-25. There were several issues in AECL’s Therac-25 that consequently led to patient’s deaths.

One engineering issue for Therac-25 is the reused software from Therac-6 and Therac-20. Therac-20 had “independent protective circuits for monitoring the electron-beam scanning plus mechanical interlocks for policing the machine and ensuring safe operation” [1]. This meaning, Therac-20 was designed with specific hardware interlocks in place to prevent faults, whereas Therac-25 mostly relied on software to prevent faults. Therac-25’s reused software illustrates the dangers of assuming that reused software will be safer due to previous testing and AECL’s overconfidence.

Another instance of AECL’s overconfidence is the Ontario Cancer Foundation incident on July 1985 in which after a patient had received a lethal overdose due to a malfunction, AECL responded that they could not reproduce the malfunction that had occurred and concluded that the malfunction was due to a micro-switch failure, confident the issue was not due to their software.

More issues leading to the Therac-25 incident is AECL’s lack of explanation on malfunction codes in the operator’s manual giving no indication that patients may be at risk. In one case, “An operator involved in one of the accidents testified that she had become insensitive to machine malfunctions. The operator further testified that during instructions she had been taught that there were “so many safety mechanisms” that she understood it was virtually impossible to overdose a patient” [1].

The Therac-25 accidents could have been avoided had certain factors been different. Software should not have been reused believing it would be safer. Due to not having any incidents with their older Therac-6/Therac-20 products, AECL was overconfident in their reused software and refused to believe that the software used for Therac-25 could be the cause of the incident.

AECL should have had better incident analysis procedures in the case of an accident and investigative measures to prevent further incidents. After the Kingstone Regional Oncology Center incident on June 1985, there should have been an immediate investigation into Therac-25, instead of AECL waited until more incidents occurred and FDA involvement before taking the incidents seriously.

Therac-25 should have had both self-checks in the software and machine interlocks to prevent faults. Therac-25 also should have had more checks in place making it less possible for mistakes to occur due to user-error and remove the possibility of fatal mistakes if user-error were to occur. Overall, Therac-25 should have been designed with the thought in mind that the worst case possible might happen when operating the machine.

The Therac-25 and Boeing 737 MAX accidents had some similarities and differences in both the technical aspects and in the reporting process. In both the Therac-25 and Boeing 737 MAX accidents, software faults were the cause of the accidents. In the Boeing 737 MAX accidents, data concluded that a system designed to help the plane avoid stalling appears to have malfunctioned, pushing down the nose of the plane [2].

Additionally, key people were unaware of certain software decisions, in the Therac-25 case, “The quality assurance manager was apparently unaware that some Therac-20 routines were also used in the Therac-25 [1].” In the Boeing 737 MAX incidents the software responsible for the accidents had not been made aware to the pilots that the software was implemented until after the first crash.

One key difference between Therac-25 and the Boeing 737 MAX accidents is that the faulty software for Therac-25 was reused software from older models and the faulty software for the Boeing 737 MAX accidents was a new developed system onto an already existing product. All of this to say that regardless of if the software is reused or not, solely relying on software to prevent malfunctions is dangerous and instead should work in tandem with hardware interlocks as well.

**References**

[1] N. Leveson “Medical Devices: The Therac-25\*”

[2] T. Sgobba “B-737 MAX AND THE CRASH OF THE REGULATORY SYSTEM”