ENGG404 TEAM PROJECT FINAL TECHNICAL REPORT:

Submitted by Team #: 14

Case Study: Therac-25:
AECL Medical, Machine malfunction, Various locations across Canada and the United States, 1985-1987

Date submitted: August 1st, 2018

Team Members	Student #s	Signatures
Pablo Vasquez-Gonzalez	1467079	
Mason Rubik	1458809	
Lucas Nieuwenhout	1464836	

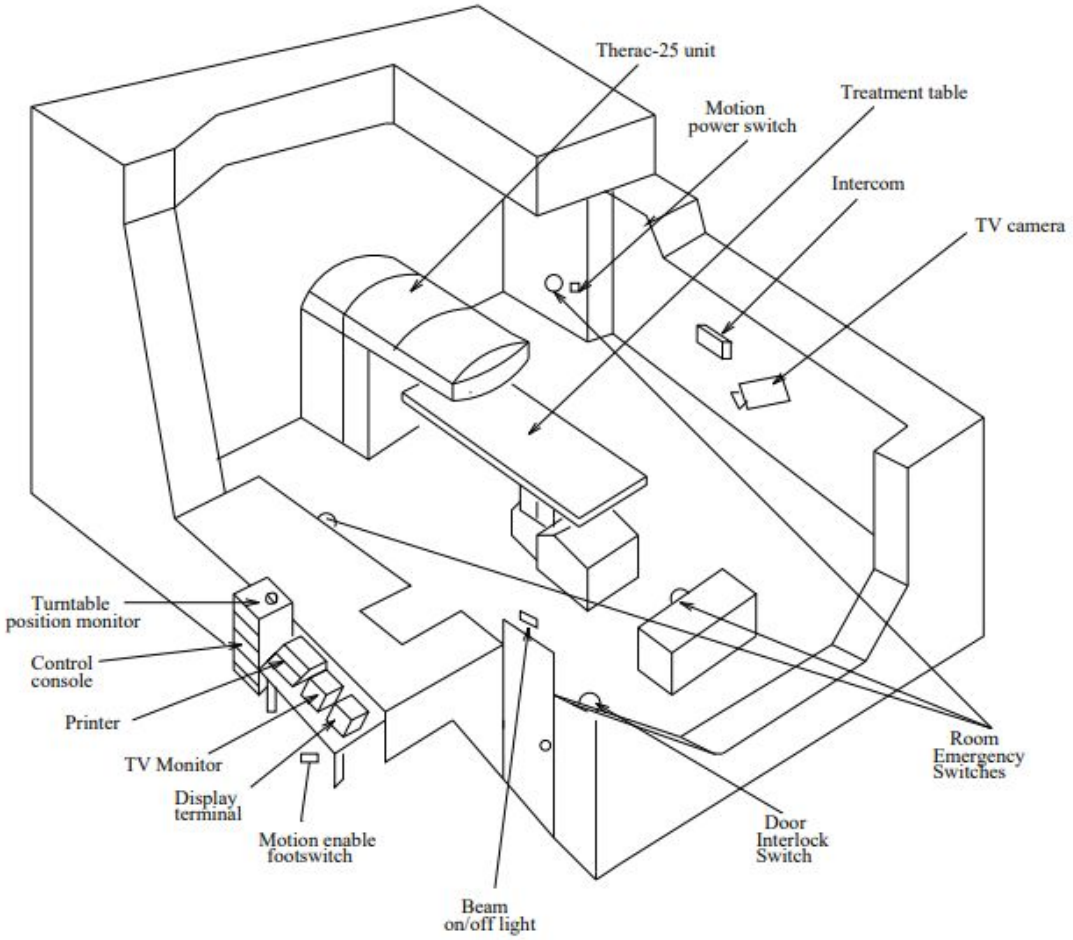


TABLE OF CONTENTS

EXECUTIVE SUMMARY

Incident Description and Losses:

Incident Description

In March 1986, a man went to the East Texas Cancer Center (ETCC) to receive radiation treatment for a tumour on his back. The ETCC, like many other institutions across Canada and the United States, used the Atomic Energy of Canada Limited (AECL) Therac-25 radiation machine for such treatments. The prescribed treatment for this patient was 180 rads of electron beam radiation, to be delivered to a small concentrated area on his back. Instead, later reports showed he was subjected to 25,000 rads, caused by a malfunction of the machine.

The patient was in pain immediately after the treatment, but it was not seen as anything serious, so he was discharged. Soon thereafter, the patient returned to the hospital spitting blood. Three of his limbs, his left vocal cord, and his diaphragm had all become paralyzed. The patient died four months later, due to radiation overexposure.

This patient was not the first, nor the last, to die from radiation over-exposure caused by software failures of the Therac-25. Since this event, and others surrounding it, the Therac-25 has had major safety changes, and is still operational in hospitals today, without association to any other incident.

Throughout these incidents, there were periods where the Therac-25 was under voluntary recall. Though this recall was mostly ignored by most hospitals (they were faced with the decision of letting their patients continue to suffer or facing the possibility of an incident), there were institutions that stopped using the Therac-25 amidst software fixes, hardware fixes, and conferences discussing the issues.

Losses to PEAP

There was no impact to the environment, since all the excess radiation was contained or absorbed by the patients.

In terms of asset loss, the deaths and injuries were the cause of multiple lawsuits, costing Canadian taxpayers potentially millions of dollars (no numbers disclosed). There was also the costs associated with investigating the incidents, creating corrective action plans, and designing and implementing hardware and software changes, of which one single incident cost $41,500 to the hospital, and $716,000 to AECL. There was also ban on AECL's medical equipment, preventing profits. Due to the necessary revisions and updates required, there was also the loss of profits to fix these issues.

Production loss was characterized by the inability to provide treatment to other patients whenever an incident occurred, and the potential restructuring of teams at AECL to investigate these incidents. Production was also stopped when the voluntary recall was instated and some hospitals discontinued their treatments with the machine, and the FBA ban from 1991 to 1994.

Due to these events, the branch of AECL responsible for the development of Therac-25 is no longer operational.

Context and Purpose:

AECL (Atomic Energy of Canada Limited) is a Canadian federal crown corporation, responsible for a variety of tasks involving the development, maintenance and management of nuclear assets, including energy and product commercialization. AECL Medical, a division of AECL, in conjunction with CGR (a French medical company), had designed other functional Therac radiation machines in the past: Therac-6 and Therac-20. The Therac-25 was an improvement on their past designs. It is a double-pass accelerator, it utilizes electricity as a power source opposed to pellets of radioactive cobalt, and it is predominantly controlled by software.

The Therac-25 was the leading radiation therapy machine used by hospitals and cancer institutes around Canada and the United States. This machine is still in use today.

It has been requested by the senior management of ABC Conglomerate that we conduct an incident investigation and root cause analysis regarding the incidents involved with AECL's Therac-25 linear accelerator. ABC Conglomerate is interested in expanding into the medical industry, specifically the engineering of machinery that uses nuclear energy. ABC Conglomerate would like to explore the dangers and lessons associated with this specific machinery in order to avoid similar incidents in the future.

The report created is to be delivered to ABC Conglomerate, providing insight into the Therac-25 incidents, the lessons we can learn from them, and our recommendations to avoid similar events through a rigorous root cause analysis . This report highlights the latent causes of the incidents, and the recommendations given, with attention focused on the two key recommendations that we believe will best help prevent incidents. A thorough business case will be presented to further illustrate the necessity of implementing a safety and risk management program based on our recommendations to ABC Conglomerate.

Inherent Risks

Dealing with nuclear technology comes with risks like environmental impact, and the safety of those working around the technology. This is further impacted when the technology is meant to be used as a health service, and the risks involved with radiation exposure are escalated to concern health and well-being as well.

Root Cause Analysis:

Scope and Boundaries:

The scope of our root cause analysis is the first ETCC incident (March 1986) where a patient was unintentionally exposed to a very large dose of radiation caused by an extreme case of latent cause **Design, Construction, Startup**. Specifically, the premise and design behind Therac-25 was flawed, as it ported code from earlier machines, but did not function in the same fundamental way. This led to a complete mismatch of design, which ultimately led to incidents. These ETCC incidents came after AECL had already been notified that other machines had malfunctioned, and AECL had already issued a possible fix to the design of the deployed machines. Needless to say, AECL was unsuccessful in finding the root cause of the other malfunctions, and the excessive exposures continued to happen, due to the complete

lack of (latent cause) **Incident Reporting, Investigation, Analysis and Actions.** There was insufficient incident reporting and investigation done by AECL as the evidence began mounting against Therac-25, and a subsequent lack of action on AECL's behalf. We will also address the fact that the machines were still being used despite other incidents having been reported, but we will not address the other incidents in the root cause analysis as it would encompass a significantly larger scope.

Latent Causes:

There were many latent causes of the Therac-25 incidents as we have identified in our report. But, the main two causes were the initial design of the machine and the incident investigation and analysis. The initial design of the machine was a large factor in the incidents because the safety structure of the machine was switched from hardware to software interlocks, without properly altering the code that operated these functions. The code that was used to run the machine was ported from Therac-6 and Therac-20, which meant it contained bugs and had poor integration with the new machine. The other main latent cause is that AECL and other investigative teams could not re-create nor find the errors in the machine and the software. There had been other similar incidents, but no proper solution had been found because the analysis and actions taken after those incidents did not sufficiently address the issue.

List of Latent Causes:

Element	Latent Cause
Management, Leadership, Commitment and Accountability.	- Management did not budget for training program or take proper training as priority - Management did not budget for multiple developers - Management valued profit over safety
Risk Assessment and Management of Risks.	- Employees not taught or shown to anticipate every outcome and engineer for risks - Previous machine had been incident free and they did not correctly - Improper understanding of the end user and did not account for all scenarios - Did not foresee software failures - Errors dismissed because they are thought to be "less severe" - The small probability of lethal errors were downplayed and thus ignored - Sister machines (Therac-6 and Therac-25) were incident free and by association thought Therac-25 would be incident free
Community Awareness and Emergency Preparedness	- There was no culture of community outreach in the company.
Incident Reporting, Investigation, Analysis and Actions.	- Could not test adequately to find errors
Program Evaluation and Continuous Improvement.	- No formal audit or inspection program
Design, Construction and Start-up.	- Inadequate comparison testing of software and hardware interlock

	- Building was not optimally designed for safety in equipment failure
Operations and Maintenance	- No regular maintenance or reporting - No process to replace or fix broken equipment
Employee Competency and Training	- Training did not adequately cover operating procedures for testing the machines - Hospital Employees became complacent with “standard” procedure - Inadequate refresher training for hospital employees
Operations and Facilities Information and Documentation.	- Proper safety documentation was not deemed a priority

Key Recommendations and Alignment to Elements:

Rank	Recommendation	Gain Index	Effort Index	Total Score	Nature of Fix	Latent Cause Addressed (Numbers from Table in Appendix E)	Alignment (Number of Element)
1	Develop software with high fault detection and sufficient error logs that is self-recoverable from unexpected conditions. Implement mandatory peer review.	4	17.5	70	Low Hanging Fruit	**4,7**	**7**
2	Create internal regulations within the design team that each component of the machine that can cause damage must have at least two independent safety defences: one hardware and one software.	4	16	64	Low Hanging Fruit	**3,7,9,10**	**1,2**
3	Ensure that proper and complete documentation is created for all devices designed and released by ABC Conglomerate.	4	16	64	Low Hanging Fruit	**11,21**	**1,2**
4	Implement a thorough training program for all hospital technicians that will operate the devices.	3	19.5	58.5	Low Hanging Fruit	**1,12,15**	**2,9**
5	Create a program where the customer service department schedules weekly meetings with all hospitals that operate the medical devices.	3	19	54	Low Hanging Fruit	**20**	**3,5,11**
6	Hire an independent incident investigation team to conduct extensive investigations into all incidents involving the medical device.	2	18	36	Nice to Do	**4,7,16**	**2,5,6**

Business Case Analysis:

	Top Two Recommendations (CAD)
Cost Avoidance of a Loss Incident	$1,512,795
Initial Costs of Improvements	$100,000 + $500,000 = $600,000
Ongoing Costs of Improvements per Year	$10,000 + $5,000 = $ 15,000
Life of Project	30 years
Total Cost of Improvements	$600,000 + $450,000 = $1,050,000
Annual Risk Exposure without Improvements	$1,512,795 x (1.2) = $1,815,354
Annual Risk Exposure with Improvements	$1,512,795 x (1/1,000,000) = $1.50
Gross Benefit	$1,815,354 - $1.50 = $1,815,352.50
Net Benefit	$1,815,352.50*30 - $1,050,000 = $53,410,590

Over 30 years, the benefits of applying a safety and risk management program comes with a financial gain of $53,410,590, plus the added safety to our workers, hospital staff, and patients. This makes these changes “Low Hanging Fruit”.

There are limitations to this analysis. For example, many of the fiscal values were never reported, and are difficult to estimate. There are many different factors that lead to the overall financial losses/potential gains that are highly variable and are likely to be inconsistent over a 30 year period.

In extension, it is challenging to place numeric values on the physical and psychological damages suffered by the patients. This also carries to the machine developers and operators, who may personally blame themselves for the incident. For those that died, it is difficult to place a cost on human life.

Issues with Implementation:

Recommendation #1: Develop software with high fault detection and sufficient error logs that is self-recoverable from unexpected conditions. Implement mandatory peer review.

The topic that we have chosen to explore is the commitment of individuals to adopt a new implementation of safe behaviour. The two most likely obstacles to implementing this recommendation would be to convince the programmers writing the code to abide by the new style of programming and to commit to the peer review process.

First, many programmers are used to writing code in their own particular way, and have developed their own styles and methods. This is usually developed over years of experience, often making it very difficult to change and adding personal bias to their own work. It also may be difficult to implement a new method of programming, because there could be a significant learning curve to using a new method.

The second problem that may be faced is the implementation of the peer review process. This requires that the original programmers properly and thoroughly comment and document their code so that it can easily be checked and evaluated by their peers.

This could also be difficult to implement into the culture of the business, because programmers are notorious for poorly documenting and/or explaining their code, as long as it makes sense to them. The peer review process also creates an environment where methods and decisions are being evaluated and questioned by peers, and it may create tension in the workplace if not properly managed. Any tension will make the peer review process much less effective.

Next Steps:

ABC Conglomerate will soon be branching its operations to the medical machinery industry. With this comes a whole new set of ethical obligations surrounding the safety of the machinery we will be making. To make this transition effective, without falling into the same pitfalls as the companies before us, it is vital that we incorporate our outlined recommendations. We start by ensuring that all software development is done correctly and safely. The firmware must be self-recoverable from unexpected conditions. Furthermore, we implement hardware interlocks to each machine to add another layer of defense. Then, we create extensive documentation, encompassing every aspect of development and testing. This may seem superfluous, but it is necessary in order to declare with any steadfast conviction that our machines will not harm the patients on which they operate. We must hold ourselves to higher standards than those before. And fortunately, our recommendations will not only improve our safety standards and protect our reputation in the industry, but they will also save us money. With our recommendations, we can avoid the atrocity of incidents before. Ultimately, we can create efficient and safe machines, allowing us to save lives, not take them.

APPENDICES:

Appendix A: Incident Description and Losses:

The entire saga of the malfunctions of the Therac-25 machine spanned over a time period of about two years. This period included 6 injuries sustained from the operation of the machine and several investigations into the causes and solutions to these incidents. The overall time frame for the event is described below. For the purpose of our report and study we will be focusing on the March 1986 incident at the ETCC. The detailed description of that event follows the overall timeline.

The average annual cost of radiation therapy per patient in Texas in 1998 was approximately **$37,000USD** ($48,400 CAD)[3, Sec. 5.11] including everything. Taking an average of 40 sessions per patient, the cost of each therapy session is approximately $925 USD ($1,210 CAD). With an incident causing blackouts of the machine for at least the day, with at least 27 patients per day, the hospital suffers an estimated loss of **$25,000USD ($33,000CAD)** everytime an incident occured.

In terms of losses to the Canadian taxpayers, AECL needed to finance a team, we assume a team of 3 analysts dedicated to investigating the incidents for a year period. This comes to **$214,000CAD**. To pay for the commute of engineering team from Ontario (HQ of AECL)-Texas: **$1000CAD** round trip flight, **$200CAD** other transport, **$200CAD/day** hotel and food for 7 days.

Independent Contractors: A salary of $110k (engineer software consultant) with a team of 2, working for at minimum 2 weeks, will accrue a cost of **$8,500CAD ($6500USD)** hired by the ETCC to investigate the incident.

Assuming AECL needed to hire a defense lawyer to both deal with the lawsuits and to be present in all negotiations between them, the FDA, and the hospital's administration, this adds another **$300,000CAD** for the two years. In terms of the lawsuits, for something as severe as radiation overdoses, an easy estimate of $100,000 CAD can be found. However, since the primary purpose of the legal action was to force AECL to make their records on the Therac-25 public, it is highly likely that AECL paid much more than $100,000 CAD to settle outside of courts and keep their records sealed. For the purpose of this report, we will assume that AECL ended up paying **$200,000CAD** at a minimum.

Total cost to hospital:	Total cost to AECL:
$33,000CAD	$514,000CAD
+ $8,500CAD	+ $200,000CAD
= $41,500 CAD / incident	+ $2,600CAD
	= $716,600 CAD / incident

Timeline: (1985-1987)

June 3, 1985, Kennestone Regional Oncology Center, Marietta, Georgia:

A 61 year old woman getting radiation treatment done by the Therac-25 on her lymph nodes was burnt by the radiation beam. The patient complained to the technician

at the time, but the technician said that it was impossible for the machine to have harmed her. The hospital physicist contacted AECL to inquire about the machine, but not only did they inform him that the situation was impossible, but they also threatened him with defamation, stating he had no basis to his claims against their machine [2]. The patient filed a lawsuit November 13,1985. The lawsuit was meant to force AECL to speak on the incident through a deposition, but before any information came out, the lawsuit was settled outside of courts [2]. This was the first alert to AECL staff that the Therac-25 was malfunctioning, but AECL only formally notified employees of the incident in March 1986, claiming to have had no earlier knowledge of it [1, Sec. 3.1].

By the time of the patient died, the Therac-25 overdose had caused severe necrosis in her chest, causing a hole to be formed through her chest and back. Her left arm had also become paralyzed [2].

This patient was not directly killed by the Therac-25. She died in 1990, in a car crash.

July 1985, Ontario Cancer Foundation, Hamilton Ontario:

The patient was a 40 year old woman attending her 24th treatment with the Therac-25 machine on July 26, 1985. After the operator's first attempt to run the machine, the machine displayed "no dose" and "treatment pause". This being common, the operator tried again, and again, until unknowingly applying 5 repeated radiation doses to the patient before a technician was called. The patient returned 3 days later for further treatment, and complained of burning and hip pain in the region of treatment.

The patient was admitted to hospital the next day, eventually dying from her cancer on November 3, 1985. An autopsy revealed that though she died of her cancer, should she had survived, she would have required a hip replacement due to the radiation burns [1, Sec. 3.2].

AECL then informed the FDA and the Canadian Radiation Protection Bureau of the machine's mechanical malfunction, but they did not mention that a patient was burned. Though AECL tried to keep things quiet, word spread among the physicists at the Ontario Cancer Foundation of the incident [2]. Shortly following, a Class 2 voluntary recall was put out by the FDA. A report written by the Canadian Radiation Protection Bureau (RPB) outlined 4 modifications required for the Therac-25 to comply with Canada's Radiation Emitting Devices(RED) Act; the most important being that any and all mis-dosages shall trigger a "treatment suspend" condition rather than a "treatment pause". They also required the reintroduction of at least one independent hardware interlock. AECL did not comply with either of these requests [1, Sec. 3.2.2]. Rather, they did their own analysis, trying to reproduce the mechanical failures that occurred, but they were unsuccessful. They did, however, speculate that the incident could have been due to a microswitch failure. But, this speculation came from a hard-wiring of the error condition, and hence unlikely to reflect the actual cause [1, Sec. 3.2.1]. AECL sends out recommendations to fix the microswitches.

December 1985, Yakima Valley Memorial Hospital:

A woman was treated in December 1985 at Yakima Valley Memorial Hospital (YVMH). The Therac-25 at the hospital had been modified following AECL's recommendations, yet it still malfunctioned [2]. Following the overdose, the patient

developed erythema in a striped pattern on her hip. With the operator unaware of the events in Kennestone and Ontario, treatment was continued. The erythema was not linked to possible machine malfunction. Later, the hospital decided to contact AECL about the erythema, but like in Kennestone, they were notified that it was impossible for the Therac-25 to be the cause. In talks with YVMH, AECL claimed that they had not even heard of any other incidents involving the machine [2]. With this confirmation, the Therac-25 at YVMH was put back into service.

Shortly after this incident occurred, the physicists working with Therac-25s at various institutions around Canada and the United States started to talk and conduct their own investigation on the Therac-25 incidents [2].

This patient is still alive today, with the necrotic tissue removed and replaced with skin grafts.

March 1986, East Texas Cancer Center:

A patient went in to receive radiation treatment for a tumour on his back. The expected treatment of 180 rads was instead delivered at up to 25,000 rads. At first try, the operator was shown a “Malfunction 54” code, but since the error codes were not documented and very common (usually 4 per day), the treatment was continued [2]. During the second dosage, the patient got up from the chair and went banging on the door, which is when the machine was finally shut down. The patient felt something severely went severely wrong and complained, with the ETCC physicist asking AECL to investigate. AECL sent over an engineer, who again stated that the modified Therac-25s (fixed microswitch) could not possibly deliver an overdose. The ETCC physicist then asked AECL if they were aware of any other radiation overexposure events related to Therac-25 and again AECL responded that they were not aware of any other incidents [1, Sec 3.4.1]. Unsatisfied with this response, the ETCC hired an independent investigator to inspect the machine, though they also found it impossible for the machine to deliver an overdose [2]. With this confirmation, the Therac-25 at ETCC was put back into service.

The patient returned to the hospital spitting blood. His left arm, both legs, his left vocal cord, and his diaphragm, all becoming paralysed [2].

This patient died four months later, diagnosed as radiation overexposure [1, Sec 3.4].

April 1986, East Texas Cancer Center:

Four days after the ETCC’s Therac-25 being put back into service, another patient was given an overdose [2]. The same operator was running the Therac-25. The operator mistakenly entered “x-ray beam” mode rather than “electron beam mode”. The error was noticed before the procedure began, so the operator switched modes. However, the software failed to recognize the mode switch, so instead of delivering a safe treatment, it delivered a full power x-ray to the patient’s head. The patient claimed that he heard “the sound of frying eggs” when the machine started [1, Sec 3.5]. The patient developed disorientation, that later lead to a coma.

This patient died three weeks later due to neurological damage to the temporal lobe and brainstem [1, Sec 3.5].

April 1986, Post Incidents:

Unwilling to let these incidents go uninvestigated, the ETCC's physicist and his technician worked tirelessly to recreate the error, and for the first time, they were successful [2]. They immediately notified AECL (and all of the other hospitals using the Therac-25) of their findings.

AECL responds by notifying all users (and the FDA) that the solution is to not make any edits [2]. Rather than using the interface to edit any errors in inputs, the machine would require a hard restart. This "incredibly lacking accident report" is reviewed by the FDA. However, the Therac-25 remains in use. There were still patients that needed their treatment, and given the Therac-25 being the only device capable of offering such treatment, the hospitals continued its use [2]. In an attempt to temporarily make operations safe, AECL notified all Therac-25 users of how to disable the "up" key in the console, which they believed would eliminate the chance of malfunction that came from editing [1. Sec 3.5.4].

May 1986:

The Therac-25 is declared defective by the FDA. The FDA does not approve of AECL's accident report. The accident report did not contain any information as to why the "up" key should be disabled, and the fix they suggested was purely temporary [1. Sec 3.5.4]. AECL writes the first revision of a corrective action plan (CAP) [2].

June 1986:

First CAP is completed, but the FDA said it was missing information on software changes. Especially software testing plans [1. Sec 3.5.4].

August 1986:

The annual conference of the American Association of Physicists in Medicine is held, and the various operators of the Therac-25 meet to discuss the incidents [2]. During these talks, many additional problems with the Therac-25 are brought to light, including problems that causes patients to receive an underdose in 10-30% of all treatments [1. Sec 3.5.4].

September 1986:

AECL responds to the FDA's requests, providing much more documentation on software, but still not providing a software testing plan [1. Sec 3.5.4].

December 1986:

CAP revision 2 submitted to the FDA. This revision included software and hardware test plans [1. Sec 3.5.4].

February 1987, Yakima Valley Memorial Hospital #2:

Under the pretense that AECL's modifications made the Therac-25 safe, the Therac-25 at YVMH was still operating. However, when a man went in for treatment for his carcinoma, he was overdosed [2]. Immediately, the FDA and the Health Protection Branch (a division of Canada's Health and Welfare ministry) requested that AECL send

a recommendation to all Therac-25 users to discontinue its use until further notice [2]. AECL did not comply.

This patient died in April, 1987.

Upon investigation, AECL discovered it was a different software issue that caused the incident[1. Sec 3.6.1]. It was caused by a counter overflow. AECL immediately notifies all users that there will soon be a new software update released to fix this.

April 13, 1987:

The FDA and Canada's Health and Welfare organisation threaten to shut down all Therac-25s until the promised permanent modifications are made by AECL, deeming it too dangerous to use in the meantime [1. Sec 3.6.2]. Another CAP revision is created. Another Therac-25 users meeting is held to discuss the most prominent problems.

May 1987:

CAP revision 4 is issued to resolve the concerns brought forth from the second users meeting.

June 1987:

The 4th revision of the CAP concluded that the Therac-25's software failure rate was only 10^{-4}, given its temporary fixes. With this information, the FDA reduces the recall to class 1. The third Therac-25 users meeting takes place.

July 1987:

The final revision to the CAP (revision 5) is released. A plan to have all necessary changes finished by August 1987 is formed.

Post August 1987:

There have been no incidents since the corrective measures proposed in the final revision of the CAP were implemented.

In 1991, the FDA comes under fire from U.S Congress for being "too soft" on AECL for the Therac-25 incidents. In response, they pose a ban on all Theratronics (the medical branch of AECL, renamed in 1988) medical equipment [2]. This political move is criticized, but the ban remains until 1994.

Theratronics still remains a crown corporation to this day, though the Canadian government has been attempting to sell it to the private industry since 1990 [2].

Detailed Description of the first of the East Texas Cancer Center Incident (March 1986):

The victim of the incident had been prescribed a series of 22 MeV electron beam treatments of 160 rad each over a period of six and a half weeks. He had already attended many of his treatments at the same facility with no adverse effects or incidents.

The patient was taken into the treatment room by the operator and positioned beneath the machine to begin treatment. The operator closed the door to the operation

room and returned to the adjacent control room. Due to the audio monitor being broken and the video monitor being unplugged, there was no direct form of communication between the two rooms.

The operator quickly entered the prescription data (the operators get pretty fast at entering similar data) into the Therac-25's console, but mistyped one of the fields. Upon realizing this, the operator used the "up" key to move the cursor back to the erroneous field, and corrected the input. Before making this correction, it is important to note that the operator had yet to confirm the selection of treatment. After the data had been entered, the machine confirmed that it was ready to begin and the operator initiated the treatment. The machine began the treatment (in the wrong mode), then showed an error message, "Malfunction 54", alongside a display indicating that a mere fraction of the treatment had been given. These errors, where the machine simply pauses, were quite common (usually 4 per day [2]), and to the operator's knowledge, did not indicate anything that could be of harm to the patient. So, the operator initiated the command for the machine to continue treatment. Upon unknowingly administering a second round of overdose, the operator heard banging on the operating room door and rushed to attend to the patient. The patient described to the operator that he felt he had been electrically shocked. The patient was immediately taken to a physician, but was shortly discharged with no overdosage entered into his records.

Unbeknownst to anyone at the time, the patient had been dosed with a highly concentrated beam of approximately 16,500-25,000, rads. This developed into radiation-induced myelitis, causing his left arm, both legs, his left vocal cord, and his diaphragm to become paralysed.

The patient died from the effects of the overdose approximately 5 months after the incident [1, Sec 3.4].

Losses:

People:

- 4 patients killed. 2 left with chronic symptoms.
- Operators who unknowingly administered overdosages are likely to feel guilt
- Hospital staff, physicists and technicians are likely to feel some guilt for continuing usage of the machine during voluntary recall
- The programmer of the Therac-25 no longer works for AECL, and his identity is classified
- Due to AECL being a crown corporation, Canadian taxpayers were burdened with the asset losses described below

Environment:

- Negligible. Though, there was excessive radiation released during the malfunctions, it is unfortunately highly unlikely that this radiation was not absorbed by the patients (due to the nature of their consequent medical conditions).
- Minor additional material use in hardware fixes

Assets:

- Lawsuit following the Kennestone overdose, settled outside of court.

- Lawsuit following the Texas incidents.
- Cost of investigation of the incidents: sending engineers to inspect and analyze the malfunctioning machines.
- Cost of creating a corrective action plan (CAP), and all of its revisions.
- Cost of creating and implementing hardware and software changes.
- Loss of profits due to the FDA's ban on AECL's medical equipment from 1991-1994.
- Even through a rebranding, renaming the medical division Theratronics, corporate reputation suffered so much that nobody in the private industry is willing to purchase it.
- Canadian government is stuck with Theratronics.

Production:

- FDA bans AECL's medical equipment from 1991-1994.
- Intermittent periods where the Therac-25 was not used in Hospitals. These periods were very short though, on the order of days to weeks. [*The machines would stop being used after an incident, but the AECL would quickly reply that they are safe, and they would quickly go back to regular usage. Also, the only other choice they had would be to discontinue use of the Therac-25 and deny their patients critical care.*]

Appendix B: Context and Purpose:

AECL (Atomic Energy of Canada Limited) is a Canadian federal crown corporation, responsible for a variety of tasks involving the development, maintenance and management of nuclear assets, including energy and product commercialization. AECL is responsible for Canada's radioactive waste decommissioning. They also coordinate with the Canadian Nuclear Laboratories (CNL), providing technical services, research, and development for companies on a commercial basis. Currently, CNL runs the nuclear research facilities, AECL is not currently directly involved in this researched, however they are directly responsible for the management of nuclear facilities, notably their decommissioning and general waste management. However, during the period of these incidents, prior to the formation of CNL, AECL was responsible for the operations and management of these research facilities. AECL aims to make contributions to nuclear science, such that new technologies can be developed to benefit society across a variety of facets from advanced medical technologies, to cleaner energy. As the nuclear field progresses and expands, they contribute by managing and coordinating nuclear resources.

AECL Medical, in conjunction with CGR, had designed other functional Therac radiation machines in the past, the Therac-6 and Therac-20. The Therac-25 was an improvement on their past designs as it was a double-pass accelerator, utilized electricity as a power source opposed to pellets of radioactive cobalt, and was predominantly controlled via software. These improvements combined to create a radiation machine with more capabilities and that was simpler for a technician to use. The integration of software control led to a belief that hardware safety interlocking mechanisms were no longer necessary, but no software safety mechanisms were put in their place. The lack of software error-detection led to massive amounts of radiation being applied to patients, and ultimately led to the death of four and chronic injury of two.

Inherent Risks:

The field of nuclear technology comes with many risks, especially environmental and safety risks. Since radiation exposure and leaks are dangerous to all life, the risks are highly associated with health and safety. By nature, nuclear technology has the capacity to become dangerous if it malfunctions or is improperly used.

AECL's involvement with Therac-25 also carries the same risk of any healthcare equipment. Any malfunction carries the possibility of either inflicting more damage to the patient, or not healing the illness it is meant to treat.

Purpose of this Report:

It has been requested by the senior management of The ABC Conglomerate that we conduct an incident investigation and root cause analysis regarding the incidents involved with AECL's Therac-25 linear accelerator. ABC Conglomerate is interested in expanding into the medical industry and specifically the engineering of machinery using nuclear energy. This report will cover the entire situation that transpired over the approximately two year period from 1985-1987 but will focus on the first incident at The ETCC in March of 1986. This is the fourth known incident involved with the machine and it is believed to be the most informative of the incidents. At the time of this incident

AECL had already been informed about malfunctions with the machines and they had tried to remedy the cause of the incidents but had failed. ABC Conglomerate is interested in exploring the dangers and lessons associated with this specific type of machinery. This report is created to be delivered to ABC Conglomerate, providing insight into the Therac-25 incidents, the lessons we can learn from them, and our recommendations to avoid similar events.

Appendix C: Root Cause Analysis – Chart:

Root Cause Analysis chart is appended at the end of this document

Appendix D: Root Cause Analysis – Discussion:

Scope and Boundaries:

The scope of our root cause analysis is the first East Texas Cancer Center (March 1986) incident where the patient was unintentionally exposed to a very large dose of radiation, caused by a malfunction of the Therac-25. This incident was after AECL had been notified that other machines had malfunctioned, and had already issued a possible fix to the design of the deployed machines. However, AECL was unsuccessful in finding the root cause of the other malfunctions, and the excessive exposures continued to happen. We will address the fact that they machines were still being used despite other incidents having been reported, but we will not address the other incidents in the root cause analysis.

We will also not continue with the operator initially inputting the incorrect configuration parameters or becoming too quick at entering the information. It is a component of the incident but it is not the fault of the operator and the Therac-25 should have been able to handle it.

Key Latent Cause #1:

Incident Reporting, Investigation, Analysis, and Action

One of the most important latent causes was the fact that AECL had been informed about other incidents before this one but had not properly identified and addressed the problems with the machines. The patient was dosed with a large amount of radiation because the ETCC was still using the Therac-25 to treat patients. This is because they were not told that the Therac-25 was malfunctioning and actively harming patients. The ETCC were unaware of the incidents because there was only a voluntary recall and the management of AECL didn't want to publicly admit the major incidents. The reasons that the recall was voluntary was because nobody could recreate the incidents that had happened to the patients and they were convinced that it was impossible for this to happen using the Therac-25.

Key Latent Cause #2:

Design, Construction and Start-up

Another important latent cause of this incident is the poor design of the machine's hardware and software. The Therac-25 was a successor to other similar machines made by AECL called the Therac-6 and the Therac-20. The patient was dosed with the large amount of radiation because the Therac-25 was not in the correct mode and the machine didn't stop the excessive radiation from being applied to the patient. This is because AECL had switched from using hardware interlocks to software interlocks on the new Therac-25, but the scope of the software interlocks did not capture software failures. Hence, when the software failed, there was nothing preventing the machine from operating. The Therac-25 also used a lot of the same code that was used for the operation of the previous Therac machines because there were so many similarities. However, they did not account for the quicker entry of the configuration parameters that was possible with the Therac-25 and did not design the code to be robust to these new capabilities.

Appendix E: Application of the Cause and Effect Model – Discussion:
Immediate Causes:

Substandard Conditions:

- Exposure to radiation - with malfunction of the machine
- Defective Equipment - Broken audio monitor
- Inadequate warning system - Errors carry no meaning
- Inadequate documentation for Therac-25
- Inadequate Safeguards - no safeguard against excessive exposure

Substandard Work Practices:

- Disabling guards or safety systems - unplugged video monitor
- Incidents reported to AECL were not properly communicated or investigated
- Disabling safeguards - Operator minimizes errors and doesn't investigate
- Not following Safety Procedures - Operator regularly saw these errors but didn't report

Basic Causes:

Engineering Design Factors:

- inadequate technical design - of the Therac-25 in many aspects
- inadequate inherently safe design - safety not priority when designing
- inadequate monitoring of construction - no oversight and accountability during design and writing of code

Job Factors:

- Inadequate maintenance - audio monitoring equipment not maintained
- Inadequate job procedures - no proper procedure for when machine gives errors
- Inadequate training - Operator was uninformed about error codes
- Monotonous Task - operator was used to doing this job and became complacent

Personal Factors:

- Operators are indifferent to machine errors, habituated to them -- complacency
- Operator became a proficient worker, able to quickly fill out necessary prescription, but became too fast for the software to recognize the changes
- Inadequate identification of critical safe behaviors - should have known that without the safeguards that there was increased risk

Latent Causes (weaknesses in Management System Elements):

- Reports of other incidents ignored and not dealt with (Incident Reporting, Investigation, Analysis and Actions)
- Lacking training on the safe operation and testing of the Therac-25 (Employee Competency and Training)
- AECL believed that malfunction of the machine was impossible (Risk Assessment and Management of Risks)
- Code designed using older machine and partially refitted (Design, Construction and Start-up)

- Only a single employee in charge of writing subroutines when there was work for more than one (Employee Competency and Training)
- Management valued profit over safety by not including hardware interlocks and shortening development periods (Management, Leadership, Commitment and Accountability)
- Software interlocks instead of Hardware interlocks, thought they were equivalent (Risk Assessment and Management of Risks)
- Proper safety documentation not a priority (Operations and Facilities Information and Documentation)
- No regular maintenance or checks on equipment like audio equipment (Operations and Maintenance)

Latent Cause Number	Latent Cause	Risk Management Element
1	Training did not adequately cover operating procedures for testing the machines	Employee Competency and Training
2	Management did not budget for training program or take proper training as a priority	Management, Leadership, Commitment and Accountability
3	Employees not taught or shown to anticipate every outcome and overengineer against risks	Risk Assessment and Management of Risks
4	Could not test adequately to find errors	Incident Reporting, Investigation, Analysis, and Action
5	Previous Machine had been incident free and they did not correctly assess the existing risks	Risk Assessment and Management of Risks
6	Improper understanding of the end user and didn't account for all scenarios	Risk Assessment and Management of Risks
7	Did not foresee software failures	Risk Assessment and Management of RIsks
8	Management did not budget for multiple developers	Management, Leadership, Commitment and Accountability
9	Management values profit over safety	Management, Leadership, Commitment and Accountability
10	Inadequate comparison testing of software and hardware interlocks	Design, Construction, and Start-up
11	Errors dismissed because they are thought to be "less severe"	Risk Assessment and Management of Risks

12	Hospital Employees became complacent with “standard” procedure	Employee Competency and Training
13	No regular maintenance or reporting	Operations and Maintenance
14	No process to replace or fix broken equipment	Operations and Maintenance
15	Inadequate refresher training for hospital employees	Employee Training and Competency
16	No formal audit or inspection program	Program Evaluation and Continuous Improvement
17	Building was not optimally designed for safety in equipment failure	Operations, Design and Start-up
18	The small probability of lethal errors were downplayed and thus ignored	Risk Assessment and Management of Risks
19	Sister machines (Therac-6 and Therac-25) were incident free and by association thought Therac-25 would be incident free	Risk Assessment and Management of Risks
20	There was no culture of community outreach in the company.	Community Awareness and Emergency Preparedness
21	Proper safety documentation was not deemed a priority	Operations and Facilities Information and Documentation

Appendix F: Key Recommendations:

Recommendation #1: Develop software with high fault detection and sufficient error logs that is self-recoverable from unexpected conditions. Implement mandatory peer review.

Description: To prevent and minimize severity of exposure incidents, the code will enter a safe lock-out state on the detection of abnormal program conditions. An error logging system will track past errors, dating and documenting them. The code architecture must be peer reviewed by both a different internal development team and by a third-party contractor. This ensures high and safe performance of the software in an efficient manner.

Deliverables:

- Initial code should be go through the peer review process at least twice, one for initial startup and one for the final deliverable, in this way the code is both focused and strengthened
- Ongoing updates will address existing bugs, with detailed patch notes and delivery dates announced
- Any updates or changes to operational code must be peer reviewed by at least a second development team and a third party, to ensure that the changes are safe and decrease the chance missed errors
- Detailed log system, capable of creating self documentation with dated incidents and change tracking, and easily accessible from the mainframe
- Code integrates fail safes and automatic emergency shutdown procedures to minimize consequences of accidental exposures

Latent Causes:
Could not test adequately to find errors.
Did not foresee software failures.

Risk Management Elements:
Design, Construction and Start-up

Effort:	17.5
1. Requires simple technology 2. Will require some investment by company to fund a development team 3. Will require ongoing cost of third party developers and updates 4. Solution can be implemented within three months to develop platform for sharing and discussing 5. Will require less than three months to complete code - Subsequent revisions will be shorter 6. Once per year for annual update	1. 3 2. 3 3. 3 4. 3 5. 2.5 6. 3
Gain:	Total: 4
- Will eliminate hazards and has the greatest reduction in risk	

- Eliminates the latent cause of inherent software failure and eliminating lethal exposure possibility - Eliminates the basic cause of the lack of error documentation available, which prevents accidental double exposure

Complex Gain Index: Low Hanging Fruit	**70**

Recommendation #2: Create internal regulations within the design team, mandating that each component of the machine that can cause damage must have at least two independent safety defences: one hardware and one software.
Description: There can be faults in software and hardware systems, so there must be multiple independent safeguards for each hazard presented by the machine. Safety can be ensured by implementing both hardware and software safeguards such that if one fails, then the other safeguards can still prevent the incident. Also if there's report that one of the safeguards has failed on a machine, then all treatments must be stopped until the safeguard can be restored.
Deliverables: - Each sufficiently hazardous component of the machine must have a software and a hardware safeguard. - There must be testing conducted on each safeguard to show that they do not depend on the other safeguards and capable of preventing or lessening the consequences. - Create dependencies in the machine that prevent it from operating if any of the safeguards are not functioning.
Latent Causes: Did not foresee software failures. Management prioritizing profit over safety. Inadequate testing of hardware and software interlocks. Employees not taught or shown to anticipate every outcome and overengineer against risks.
Risk Management Elements: Risk Assessment and Management of Risks. Management, Leadership, Commitment and Accountability.

Effort:	Total: 16
1. Applying complex technology with the combination of the software and hardware solutions 2. The upfront cost would be in the neighbourhood of a half million to cover the expenses of programming and designing 3. The ongoing cost would be less than $10,000, there would be slightly more maintenance than just software interlocks but not significantly more 4. We must allow for new internal regulations to be drafted	1. 2 2. 3 3. 3 4. 3 5. 1 6. 4

5. It would require a significant amount of time to design and test these improvements to safety systems 6. This is a single time event	
Gain:	4
- This recommendation will directly address the latent cause of: Inadequate comparison testing of software and hardware interlocks - This would cause the greatest reduction in risk - The initiation event would not be eliminated, but it would have effect anymore	
Complex Gain Index: Low Hanging Fruit	**64**

Recommendation #3: Ensure that proper and complete documentation is created for all devices designed and released by ABC Conglomerate.

Description: This documentation includes, but is not limited to sections on; general information, safety precautions, maintenance routines, physical structure overview, mechanics overview, electrical overview, operation routines, error codes, troubleshooting and emergency shutdown procedures. The section on error codes must contain detailed information on the source causing each error, and the required corrective action to be taken by the operator. All errors and warnings are to be unique to a specific issue and the corrective action plan should not be singular (redundancy). To create this documentation, there must be a dedicated person responsible for its completion. This person must actively seek complete information from the designers and develop documentation according to an international machine manual standard (e.g, IEEE).

Deliverables:
- A dedicated team member responsible for the development of documentation
- Documentation must be reviewed by designers/developers for accuracy check
- Documentation must adhere to an international standard level
    - Error codes must be paired with a corrective action plan
- Error codes are to be unique to individual error sources
- Each error source must have an error code

Latent Causes:
Proper safety documentation not a priority.
Errors dismissed because they are incorrectly thought to be "less severe" and it is more convenient.

Risk Management Elements:
Risk Assessment and Management of Risks.
Management Leadership and Accountability.

Effort:	Total: 16

1. Solution is not technology, only documentation 2. There would be some significant initial cost to implement the documentation 3. There will be a small ongoing cost 4. Need to create to test set needed for documentation of error codes, can be implemented within 3 months 5. This would require less than 3 months to develop 6. One per year, assuming yearly updates, these codes need to be updated	1. 4 2. 3 3. 3 4. 3 5. 2 6. 3
Gain:	4
- Addresses the latent cause of errors being dismissed because they were thought to be less severe. - Even though it address latent causes it does not eliminate hazards so it is not worthy of a grade of 4	
Complex Gain Index: Low Hanging Fruit	**64**

Recommendation #4: Implement a thorough training program for all hospital technicians that will operate the devices.
Description: The training program will have an initial training session with repeated quarterly refresher seminars. This would assist in keeping operating knowledge fresh and reinforce proper procedures.
Deliverables: - semi-annual operator workshops, with a mock planned inspection carried out by operators to further associate with proper procedure - review current operated machinery - full fledged course on any upcoming/new machinery, with documentation run-through and all potential safety issues covered in the workshop - training program will have operators undergo multiple planned inspections, completely random, in order to test for effective knowledge
Latent Causes: No refresher training training for hospital employees. Training did not adequately cover operating procedures for testing the machines. Hospital Employees became complacent with “standard” procedure.
Risk Management Elements: Employee Competency and Training. Risk Assessment and Management of Risks.
Effort: Total: 19.5

1. Requires no technology 2. Initial cost is minimal 3. Ongoing costs of training program is significant as it requires constant workshops throughout year 4. Timing can be implemented within 3 months 5. Duration of initial training would be completed within 3 months - Subsequent sessions would be shorter 6. Solution, design, and implementation would be done once	1. 4 2. 4 3. 1 4. 3 5. 2.5 6. 4
Gain:	3
- Addresses latent cause of employee competency regarding error codes, but does not prevent the initial incident from happening in the first place - Promotes proactive behaviour, preventing further incidents from occurring	
Complex Gain Index: Low Hanging Fruit	**58.5**

Recommendation #5: Create a program where the customer service department schedules weekly meetings with all hospitals that operate the medical devices.

Description: The weekly meetings should include conversations any abnormal experiences that technicians had with the machine or any new questions that they may have. ABC Conglomerate should also make sure to inform the hospitals of any ongoing investigations into relevant incidents. This will help to keep the lines of communication open and allow urgent matters to be communicated quickly and efficiently. All meetings should be recorded and documented by at least one supervisor.

Deliverables:
- Regular weekly meetings
  - Include updates on open investigations
  - Allow for questions
  - documented
- Create fast and easy method for hospitals to contact ABC Conglomerate in the case of an emergency

Latent Causes:
There was no culture of community outreach within the company.

Risk Management Elements:
Community Awareness and Emergency Preparedness.
Incident Reporting, Investigation, Analysis and Actions.
Operations and Facilities Information and Documentation.

Effort:	Total: 19
1. It requires no new technology 2. The initial cost will be minimal	1. 4 2. 4

3. The ongoing cost will be spread over technician salary and HR staff 4. Solution can be implemented immediately 5. It would take less than a week to perform the weekly meetings 6. This needs to be frequent and ongoing	3. 2 4. 4 5. 4 6. 1
Gain:	3
- Reduces incidents by preventing subsequent conditions by keeping everyone up to date - Address the basic cause of no cross-communication, which is a job factor - Does not eliminate the hazard or have the greatest reduction in risk levels	
Complex Gain Index: Low Hanging Fruit	**54**

Recommendation #6: Hire an independent incident investigation team to conduct extensive investigations into all incidents involving the medical device.

Description: All incidents in the hospital that involve the machine should be investigated by the independent investigation team. This includes all near misses, and incidents where the cause is indeterminate, but the machine was a reasonable probable cause. This allows for lessons to be learned from failures, such that repetition is avoided. All reports are to be public record, and shared with the other hospitals where the same and/or similar devices are being operated.

Deliverables:
- All incidents are to be reported in written form
- All reports must follow a detailed template
- Reports are to peer reviewed and published
- Published reports are to be available in an online database for other companies to access

Latent Causes:
No formal audit or inspection program
Did not foresee software failures
Could not adequately test for errors

Risk Management Elements:
Incident Reporting, Investigation, Analysis and Action.
Risk Assessment and Management of Risk.
Program Evaluation and Continuous Improvement.

Effort:	Total: 18
1. Solution is not technology, only documentation 2. The initial cost would be much less than $100,000, since it would only cover the cost of finding a company willing to do the work	7. 4 8. 4 9. 1 10. 4

3. At least $100,000 per year, as a single incident would require a full team with initial investigation, follow ups, etc 4. This could implemented immediately 5. The duration of a single investigation could require more than one month 6. This would happen one time per incident, depending on the frequency of incidents it could vary	11. 2 12. 3
<u>Gain:</u>	2
- This would address the latent cause of: No formal audit or inspection program. - Having the third party identify the problem would result in subsequent events stopping	
Complex Gain Index: Nice to do	**36**

Appendix G: Summary of the Recommendations:

Rank	Recommendation	Gain Index	Effort Index	Total Score	Nature of Fix	Latent Cause Addressed (Numbers from Table in Appendix E)	Alignment (Number of Element)
1	Develop software with high fault detection and sufficient error logs that is self-recoverable from unexpected conditions. Implement mandatory peer review.	4	17.5	70	Low Hanging Fruit	**4,7**	**7**
2	Create internal regulations within the design team that each component of the machine that can cause damage must have at least two independent safety defences: one hardware and one software.	4	16	64	Low Hanging Fruit	**3,7,9,10**	**1,2**
3	Ensure that proper and complete documentation is created for all devices designed and released by ABC Conglomerate.	4	16	64	Low Hanging Fruit	**11,21**	**1,2**
4	Implement a thorough training program for all hospital technicians that will operate the devices.	3	19.5	58.5	Low Hanging Fruit	**1,12,15**	**2,9**
5	Create a program where the customer service department schedules weekly meetings with all hospitals that operate the medical devices.	3	19	54	Low Hanging Fruit	**20**	**3,5,11**
6	Hire an independent incident investigation team to conduct extensive investigations into all incidents involving the medical device.	2	18	36	Nice to Do	**4,7,16**	**2,5,6**

Appendix H: Business Case Analysis:

	Top Two Recommendations (CAD)
Cost Avoidance of a Loss Incident	$1,512,795
Initial Costs of Improvements	$100,000 + $500,000 = $600,000
Ongoing Costs of Improvements per Year	$10,000 + $5,000 = $ 15,000
Life of Project	30 years
Total Cost of Improvements	$600,000 + $450,000 = $1,050,000
Annual Risk Exposure without Improvements	$1,512,795 x (1.2) = $1,815,354
Annual Risk Exposure with Improvements	$1,512,795 x (1/1,000,000) = $1.50
Gross Benefit	$1,815,354 - $1.50 = $1,815,352.50
Net Benefit	$1,815,352.50*30 - $1,050,000 = $53,410,590

Quadrant

Over 30 years, the benefits of applying a safety and risk management program comes with a financial gain of $53,410,590.00, plus the added safety to our workers, hospital staff, and patients. In terms of the quadrant, this would fall under “Low Hanging Fruit”.

Conclusions

From our business case analysis, investing in a risk management safety program has the potential of saving significant capital, not to mention the prevention of bad press and negative image. From what we have found, we would advise ABC conglomerate to diligently consider these changes. This is a very preliminary level of investigation, with many variable factors that could greatly influence the outcome. However, from the conclusions we came to, it looks very promising to continue investigation on these changes and consult on future action. It is possible that every invested dollar returns, on average, $519.

Factors Considered

In doing this analysis, we came across a variety of unknown factors and assumptions that we have discussed. In terms of financial analysis, we built this business case using a variety of estimations. First, we estimated the cost of avoidance of lost incident based on publicly available labour data from the United States from 1985 [4]. We then used the average USD to CAD conversion rate of 1985, 1.36 [5]. These values were then converted from 1985 CAD to 2018 CAD (average inflation rate of 1.91%) [6].

Another aspect to consider when analyzing the business case of an incident is the effect on the stock price of the company. This was not considered in the impact on assets because AECL was a crown corporation and the incidents had no effect. However this would be something to account for if ABC Conglomerate were to ever have an incident. The implementation of safety features and safeguards within a

company can actually raise stocks as it would prevent incidents and show to investors the commitment to safety and reliability.

Due to the lack of public information about these incidents (including the amount for which the lawsuit was settled was not disclosed), it is difficult to determine precise capital losses. Moreover, the number of people at AECL and the team size of the third party investigators is unknown, hence we can only estimate the required number of workers and their expected salaries. It is also very hard to put a number value on company reputation, which is takes a great toll from these sorts of incidents.

Moreover, to investigate annualized costs, we had to make assumptions on the expected incident rates. We base the exposure on 1.2 incidents per year (the machine first went into use 1982 and from then to 1987 there were 6 incidents). According to FDA regulations, our devices would not only fall under Medical Class III regulation, but also under the regulations for devices that emit radiation. The FDA will recall similar devices when they determine their failure rate to be greater than one in a thousand. Moreover, there is a range of acceptable failure rates for similar machinery that is usually in the 1/100,000 to 1/1,000,000 range. Hence, since our machine is Class III and emits radiation, we can safely estimate our machine is on the upper end of this range, and must fall in a failure rate category of one in a million, to fit FDA regulations.

We also adjusted the table to provide an accurate net benefit. It previously compared a yearly savings compared with the total cost of improvements but we changed it to subtract the total cost of improvements from the total benefit of the improvements over 30 years. This is a more accurate way to calculate the net benefit of our recommended improvements over the 30 year project lifetime.

Additionally, it is challenging to place numeric value on the physical and psychological damages suffered by the patients. This also carries to the machine developers and operators, who may personally blame themselves for the incident. For those that died, it is difficult to place a cost on human life.

Appendix I: References:

[1] Nancy Leveson, “Medical Devices: The Therac 25*”, Safeware: System Safety, and Computers* (Update of the 1993 IEEE Computer article ed.), Addison Wesley, 1995. http://sunnyday.mit.edu/papers/therac.pdf

[2] Barbara Wade Rose, “Fatal Dose”,*Saturday Night,* June 1994.[Online], Available:http://www.ccnr.org/fatal_dose.html [Accessed:June 16,2018]

[3] Texas Health Information Council, “The Cost of Cancer in Texas”. (1998). 1st ed. [ebook] Available at:http://alt.coxnewsweb.com/statesman/politifact/041711_cancercoststudyLBJ.pdf [Accessed 8 Jul. 2018].

[4] Earl F. Mellor, “Weekly earnings in 1985: a look at more than 200 occupations”, *Bureau of Labour Statistics.* Available:https://www.bls.gov/opub/mlr/1986/09/rpt1full.pdf

[5] “U.S. Dollar to Canadian Dollar Spot Exchange Rates for 1985 from the Bank of England”, Available: https://www.poundsterlinglive.com/bank-of-england-spot/historical-spot-exchange-rates/usd/USD-to-CAD-1985

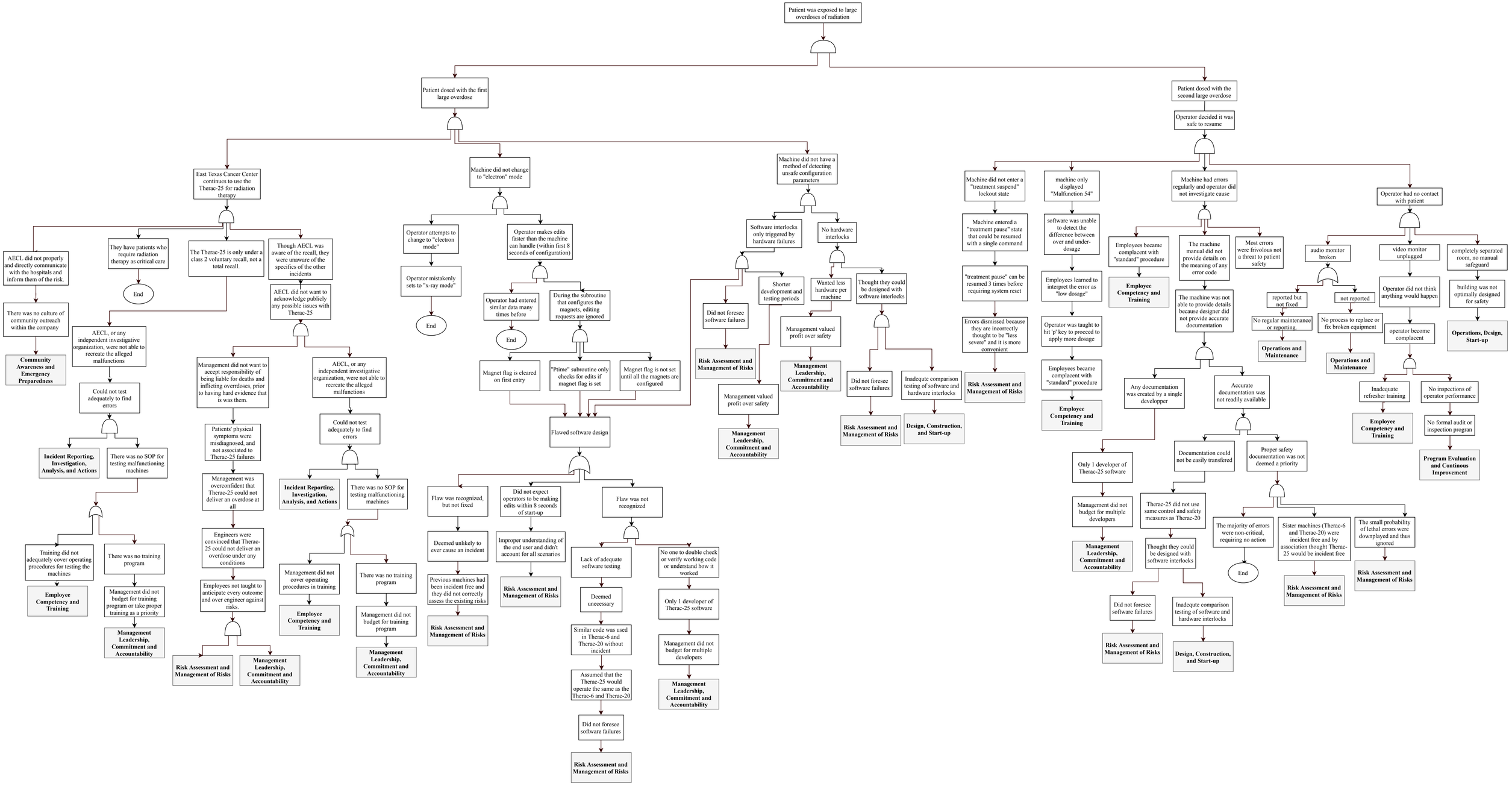
[6] “Canadian Inflation Rate Calculator”, Available: http://www.in2013dollars.com/1998-CAD-in-2018?

Module 3-07-404-1: Final Technical Report Marking Rubric – For Use by Students

Date:	Team #: 14 Case Study Name: Therac-25: AECL Medical
Team Members:	Lucas Nieuwenhout, Mason Rubik, Pablo Vasquez-Gonzalez

Final Technical Report Focus Areas	**Comments**	**Team's Marks**	**Total Marks**
Cover Page and Table of Contents			**5**
Executive Summary:			
ES: Incident Description and Losses			**5**
ES: Context and Purpose of the Incident Investigation			**5**
ES: Root Cause Analysis Summary			**5**
ES: List of the Latent Causes			**5**
ES: Recommendations:			**5**
ES: Business Case Analysis			**5**
ES: Issues with Implementation			**10**
ES: Next Steps:			**15**
Appendices:			
A: Incident Description and Losses			**10**
B: Context and Purpose of the Incident Investigation			**10**
C: Root Cause Analysis – Chart			**20**
D: Root Cause Analysis – Discussion:			**15**
E: Application of the Cause and Effect Model:			**20**
F: Key Recommendations			**30**
G: Summary of Recommendations			**10**
H: Business Case Analysis			**15**
I: References			**5**
Overall: Spelling, Grammar, Format, Organization, Presentation, Rational and Logic; Overall Flow			**10**
	Total:		**205**

Team Project Total Mark:	**Team's Marks**	**Total Marks**	**Total Marks, %**
The Progress Report		120	/ 5%
The Final Technical Report		205	/ 25%
Total		n/a	/ 30%


Patient was exposed to large overdoses of radiation
Patient dosed with the first large overdose
East Texas Cancer Center continues to use the Therac-25 for radiation therapy
AECL did not properly and directly communicate with the hospitals and inform them of the risk.
There was no culture of community outreach within the company
Community Awareness and Emergency Preparedness
They have patients who require radiation therapy as critical care
End
The Therac-25 is only under a class 2 voluntary recall, not a total recall.
AECL, or any independent investigative organization, were not able to recreate the alleged malfunctions
Could not test adequately to find errors
Incident Reporting, Investigation, Analysis, and Actions
There was no SOP for testing malfunctioning machines
Training did not adequately cover operating procedures for testing the machines
Employee Competency and Training
There was no training program
Management did not budget for training program or take proper training as a priority
Management Leadership, Commitment and Accountability
Though AECL was aware of the recall, they were unaware of the specifics of the other incidents
AECL did not want to acknowledge publicly any possible issues with Therac-25
Management did not want to accept responsibility of being liable for deaths and inflicting overrdoses, prior to having hard evidence that is was them.
Patients' physical symptoms were misdiagnosed, and not associated to Therac-25 failures
Management was overconfident that Therac-25 could not deliver an overdose at all
Engineers were convinced that Therac-25 could not deliver an overdose under any conditions
Employees not taught to anticipate every outcome and over engineer against risks
Risk Assessment and Management of Risks
Management Leadership, Commitment and Accountability
AECL, or any independent investigative organization, were not able to recreate the alleged malfunctions
Could not test adequately to find errors
Incident Reporting, Investigation, Analysis, and Actions
There was no SOP for testing malfunctioning machines
Management did not cover operating procedures in training
Employee Competency and Training
There was no training program
Management did not budget for training program
Management Leadership, Commitment and Accountability
Machine did not change to "electron" mode
Operator attempts to change to "electron mode"
Operator mistakenly sets to "x-ray mode"
End
Operator makes edits faster than the machine can handle (within first 8 seconds of configuration)
Operator had entered similar data many times before
End
During the subroutine that configures the magnets, editing requests are ignored
Magnet flag is cleared on first entry
"Prime" subroutine only checks for edits if magnet flag is set
Magnet flag is not set until all the magnets are configured
Flawed software design
Flaw was recognized, but not fixed
Deemed unlikely to ever cause an incident
Previous machines had been incident free and they did not correctly assess the existing risks
Risk Assessment and Management of Risks
Did not expect operators to be making edits within 8 seconds of start-up
Improper understanding of the end user and didn't account for all scenarios
Risk Assessment and Management of Risks
Flaw was not recognized
Lack of adequate software testing
Deemed unecessary
Similar code was used in Therac-6 and Therac-20 without incident
Assumed that the Therac-25 would operate the same as the Therac-6 and Therac-20
Did not foresee software failures
Risk Assessment and Management of Risks
No one to double check or verify working code or understand how it worked
Only 1 developer of Therac-25 software
Management did not budget for multiple developers
Management Leadership, Commitment and Accountability
Machine did not have a method of detecting unsafe configuration parameters
Software interlocks only triggered by hardware failures
Did not foresee software failures
Risk Assessment and Management of Risks
Shorter development and testing periods
Management valued profit over safety
Management Leadership, Commitment and Accountability
No hardware interlocks
Wanted less hardware per machine
Management valued profit over safety
Management Leadership, Commitment and Accountability
Thought they could be designed with software interlocks
Did not foresee software failures
Risk Assessment and Management of Risks
Inadequte comparison testing of software and hardware interlocks
Design, Construction, and Start-up
Patient dosed with the second large overdose
Operator decided it was safe to resume
Machine did not enter a "treatment suspend" lockout state
Machine entered a "treatment pause" state that could be resumed with a single command
"treatment pause" can be resumed 3 times before requiring system reset
Errors dismissed because they are incorrectly thought to be "less severe" and it is more convenient
Risk Assessment and Management of Risks
machine only displayed "Malfunction 54"
software was unable to detect the difference between over and under-dosage
Employees learned to interpret the error as "low dosage"
Operator was taught to hit 'p' key to proceed to apply more dosage
Employees became complacent with "standard" procedure
Employee Competency and Training
Only 1 developer of Therac-25 software
Management did not budget for multiple developers
Management Leadership, Commitment and Accountability
Machine had errors regularly and operator did not investigate cause
Employees became complacent with "standard" procedure
Employee Competency and Training
The machine manual did not provide details on the meaning of any error code
The machine was not able to provide details because designer did not provide accurate documentation
Any documentation was created by a single developper
Accurate documentation was not readily available
Documentation could not be easily transfered
Therac-25 did not use same control and safety measures as Therac-20
Thought they could be designed with software interlocks
Did not foresee software failures
Risk Assessment and Management of Risks
Inadequte comparison testing of software and hardware interlocks
Design, Construction, and Start-up
Proper safety documentation was not deemed a priority
The majority of errors were non-critical, requiring no action
End
Sister machines (Therac-6 and Therac-20) were incident free and by association thought Therac-25 would be incident free
Risk Assessment and Management of Risks
The small probability of lethal errors were downplayed and thus ignored
Risk Assessment and Management of Risks
Most errors were frivolous not a threat to patient safety
Operator had no contact with patient
audio monitor broken
reported but not fixed
No regular maintenance or reporting
Operations and Maintenance
not reported
No process to replace or fix broken equipment
Operations and Maintenance
video monitor unplugged
Operator did not think anything would happen
operator become complacent
Inadequate refresher training
Employee Competency and Training
No inspections of operator performance
No formal audit or inspection program
Program Evaluation and Continous Improvement
completely separated room, no manual safeguard
building was not optimally designed for safety
Operations, Design, Start-up