ENGR 401 handout Week 3 -Scan into ecs…

Student ID:

1. Therac-25 Computer Controlled Radiation Therapy Incident:

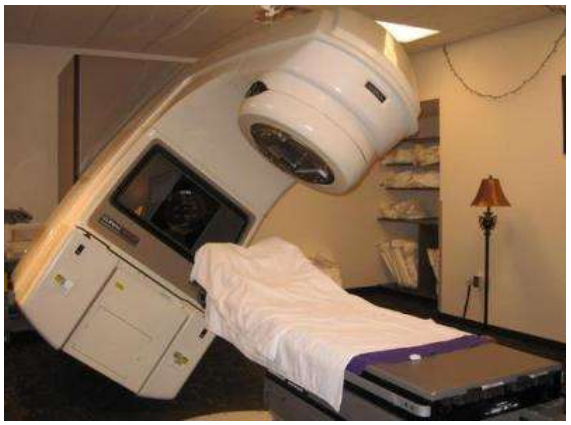
Sources:

- https://en.wikipedia.org/wiki/Therac-25
- https://hackaday.com/2015/10/26/killed-by-a-machine-the-therac-25/
- https://www.youtube.com/watch?v=41Gv-zzICIQ

Summary

What was the Therac-25

The Therac-25 was the latest in a generation of radiation therapy machine, ostensibly a "cancer zapper". Machines if this class use beams of x-rays or electrons to target and kill specific areas of tumour cell, potentially deep deep inside the body. While there is always going to be a certain amount of collateral cell damage, like chemotherapy the hope is that more cancerous material will be killed rather than healthy.



The device was originally made up of an electron beam which could run in a low-power or high-power mode, and a turntable that positioned different targets for the beam to strike before it reached the patient depending on the type of treatment needed.

- X-Ray Treatment Mode - The beam was in **high-power mode**, and the turntable would be set to cause it to hit a tungsten target that both converts the beam to X-Rays, and disperses them over the treatment area.

- Direct Electron Treatment Mode – The beam was in **low-power mode**, and the turntable would be set to cause it to be dispersed over the treatment area using magnets.

These electron and x-ray beams therefore need to be highly regulated and controlled, an inappropriately aimed beam or beam with an incorrect level of power could be highly damaging if not fatal.

The original editions of the Therac included physical safety interlocks to prevent patients being exposed to unsafe radiation such as from a direct hit of the high-powered electron beam used for X-Rays.

One example is that if the high-powered electron beam was selected to be fired at a patient, without the X-Ray target in place between the patient and the beam, the electric circuit that was created by that arrangement would result in a fuse blowing and disconnecting power from the Therac.

For the Therac-25, these physical safety features were removed from the hardware, and instead it was left up to the newly attached PDP-11 computer to control the configuration of the beam and turntable and monitor for any unsafe configurations. The computer was faster to run the motors on the device and set it up for the procedure, something that hospital staff and administrators loved for simplicity and speed and perceived accuracy.

What unfortunately happened

For six patients between 1986 and 1987, something went wrong with this configuration setup. The Therac-25 exposed them to massive overdoses of radiation, killing four patients and leaving two with lifelong injuries.

When things went wrong, the patients under treatment were reporting feeling tremendous amounts of heat and burning. In some cases, the machine would stop with an error “Malfunction 54”, which the operators only knew as either too much or too little energy had been released. The error could be cleared, and then the beam restarted.

The supervising hospital physicist would report to the vendor AECL and their local medical regulator that an overdose happened. Initially AECL denied that the Therac-25 was capable of delivering an overdose due to the amount of software protections in place that would throw errors and if anything, deliver less than the required radiation not more.

However, there was that much confidence in the correct operation of the computer-controlled system, that initially it was seen as impossible for this to have happened.

What turned out to be happening

After the second of the incidents that occurred at the East Texas Cancer Center in Tyler Texas, the staff physicist Fritz Hager was determined to get to the bottom of the issue. He and a radiotherapy technician worked through the night and weekend to try and reproduce the specific error “Malfunction 54” that was not mentioned in the manuals.

What they eventually found was that if a user would move the cursor using the arrow keys, select “X-Ray Mode”, and the turntable would begin turning to align the X-Ray target as well as set the electron beam to high-power. This would take approximately 8 seconds.

If during these 8 seconds the user used the arrow keys to switch the machine to electron beam mode, the turntable would not switch to the correct position, instead being left in an unknown state.

This was due to a race condition in the software, where the code was essentially assuming that no-one would try to make changes to the configuration while the turn table was still rotating.

An operator in another facility reproduced this behavior on their Therac-20, which you will remember had a safety interlock fuse that was removed on the Therac-25. In that facility the safety fuse blew, that would have prevented the electron beam from energizing.

During the investigation of the incidents, there were two related causal issues. First that all physical safety interlocks that had prevented the previous generations of the Therac from being incorrectly setup for a patient were removed from the Therac-25, with control given over to the PDP-11 computer attached to the device. Then the software that the computer runs to control the setup of the device's radiation exposure contained undetected bugs.

What it "seems" the later investigation found

While the vendor AECL never officially released the source code, reports of investigations showed that the software that controlled the system and provided the only safety functions seemed to be written by a programme with little experience in real-time systems. There were few comments, and no proof that timing analysis and been performed.

There was allegedly no testing of the Therac-25 hardware and software together before the unit was assembled at a hospital, with the "testing" hours counted as only the time when a hospital staff operator was using the machine on a patient.

Of more important note, when AECL had been considering the incidents reported to them from the first patient onwards, the design of the software was not considered – instead focusing purely on the hardware and assuming the software was free of bugs.

Evaluate using both the "Public Services Commission Protected Disclosures Act" & the "Engineering NZ Practice Note 8 – Being Ethical" frameworks described in class (links available on ECS ENGR401 Page).

Considering the issue only under the "Engineering NZ Practice Note 8" regulations;

1. What ethical issues do you spot in this scenario?

2. Who are the stakeholders involved in this case?

3. What (if any) obligations in the public interest do you think are relevant?

4. If you were involved with the **servicing or operation on patients** of a Therac-25 whether its electrics, mechanics, or computer software and became aware or suspected these problems, then what (if any) obligations relating to your personal conduct do you think are relevant any why?

Considering the issue only under the "NZ Protected Disclosures Act 2022" legislation;

5. Considering now the same scenario as #4 with regards to the NZ Protected Disclosures Act 2022, what (if any) additional actions or obligations would you feel are relevant and why?

6. Are there any differences between your answers to #4 and #5 which are material, and if so, what are the factors driving them? Which answer would take precedence and why?

7. Reflect on the same scenario regarding the Therac-25 under the Markkula Framework given in class previously and any differences in your ethical analysis when driven by 'legislative' versus 'non-legislative' ethical criteria. Does having familiarity now with the 'legislative' frameworks alter how you would interpret things under Markkula?

8. Did discussion with your group change your view at any points - which points and why? Consider also whether when discussing with your group, did any of your personality characteristics (from lecture #2 handout) introduce bias your recgonised to your discussion?

2. Boeing 737 MAX Crashes due to MCAS

Sources:

- ENGR401 Lecture Slides – Week 3 – Professional Ethics
    - https://ecs.wgtn.ac.nz/foswiki/pub/Courses/ENGR401_2024T1/LectureSchedule/4.ENGR401%20-%20Professional%20Ethics%20.pdf
- https://www.youtube.com/watch?v=zfQW0upkVus
- https://en.wikipedia.org/wiki/Maneuvering_Characteristics_Augmentation_System

Summary

(NB – Purposefully less information provided c/- covering the background of this in class)

The 737 MAX, Bigger Engines, and MCAS

When Boeing wanted to put larger more effective engines underneath the wings of the Boeing 737 MAX as part of competing with the new Airbus A320, it had a challenge in that the engines would not physically fit under the wings. This is due to the airframe for the Boeing 737 essentially still being the same shape and dimensions as it was when first created when jet engines were much smaller and thinner due to the lack of a big high-speed thrust fan at the front.

Figure 1 - 737-200 and Engines


Figure 2 - 737 MAX and Engines

To fit the engines under the wings without changing the length of the landing gear (which would also result in changing the rest of the plane), they were moved forward and up in a mounting position.

This altered the center of gravity for the aircraft and also altered its flying characteristics, causing the aircraft to want to pitch up (nose up) more than a pilot would experience when flying an earlier version of the Boeing 737.

To accommodate this handling change, and get the plane to be as close to what pilots were familiar with as possible, Boeing added a software feature not documented in the manuals and training – MCAS (Maneuvering Characteristics Augmentation System).

In response to this system detecting that the nose of the aircraft was getting too high through reading the position setting of only one of the two Angle of Attack Sensors on the nose of the aircraft, it would start moving the big horizontal stabilizer at the tail of the plane to push the nose back down. It’s important to note that it was moving the entire flying surface, not just the little elevator tabs at the back of the tailplane.

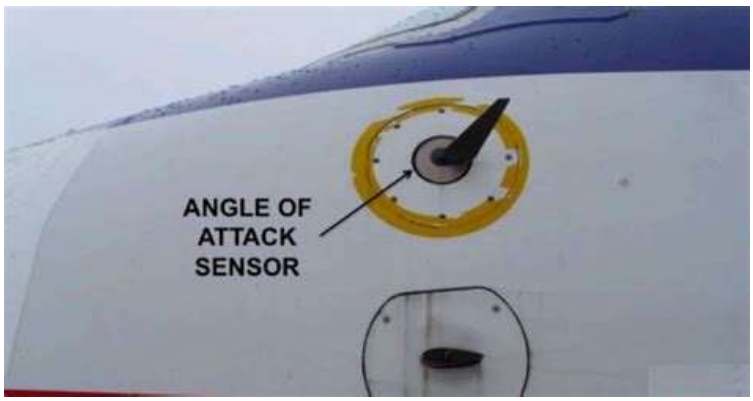


Figure 3 Angle of Attack Sensor

This would cause a dramatic nose down effect, that during a stall would get the aircraft flying again, but if applied incorrectly would push the nose of the aircraft down so forcefully that the pilots would be unable to pull up simply using the control yoke. They would need to know to turn off the MCAS system, and then manually use a wheel to move the horizontal stabilizer back into a normal flying position.

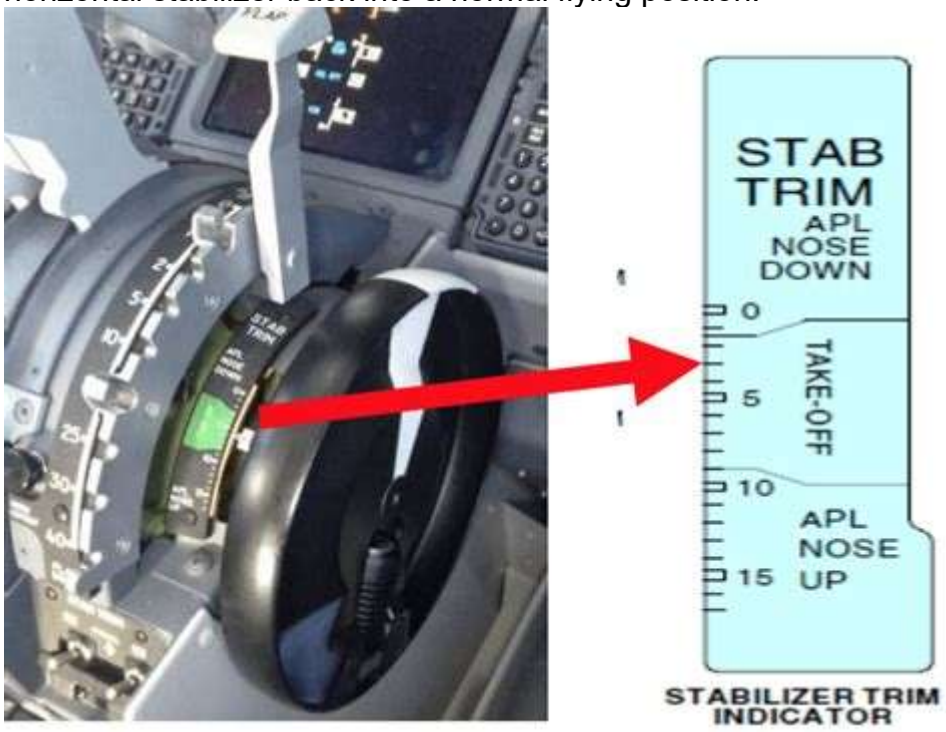


Figure 4 - Manual Trim Wheel (black and white wheel next to flap handle)

The problem is that during the initial crash the pilots were not aware of the existence of this system nor how to respond. In a subsequent crash, they did know about the potential for the horizontal stabilizer to “run-away” and had cut the power supply to the stabilizer motors, but unfortunately there was so little time to be able to do this along with the pressures involved during a real-time emergency situation, they were unable to recover the aircraft before crashing.

Summary of thoughts on why Boeing did not publicise this feature

Boeing was seeking to minimize pilot retraining requirements. If you sit in the cockpit of an earlier 737 and the 737 MAX, much of the layout of switches and controls is very similar if not identical. Boeing saw that minimizing any necessary retraining of existing 737 pilots would make the new model highly attractive to airlines and other operators that already had a 737 fleet, pushing sales.

Boeing were criticized by the NTSB as not undertaking sufficient testing of the 737 MAX, and made incorrect assumptions about the pilots response to the triggering of horizontal stabliser movements due to incorrect triggering of the MCAS system. Further, a review found that the FAA had failed to adequately review MCAS in part hampered by Boeing not having provided adequate and updated technical information regarding the MCAS System.

Further (potentially) related information
If you have further interest in organizational cultural changes that may have contributed to these events, then you may find the 2022 Documentary "Downfall: The Case Against Boeing" of interest to watch. It is not required or expected that you watch this documentary as part of or prior to the submission of this assignment.
(https://en.wikipedia.org/wiki/Downfall:_The_Case_Against_Boeing)

Evaluate using both the "Public Services Commission Protected Disclosures Act" & the "Engineering NZ Practice Note 8 – Being Ethical" frameworks described in class (links available on ECS ENGR401 Page).

Considering the issue only under the "Engineering NZ Practice Note 8" regulations;

1. What ethical issues do you spot in this scenario?

2. Who are the stakeholders involved in this case?

3. What (if any) obligations in the public interest do you think are relevant?

4. If you were involved with **construction** of a Boeing 737 MAX whether its electrics, mechanics, or computer software and became aware or

suspected these problems, then what (if any) obligations relating to your personal conduct do you think are relevant any why?

Considering the issue only under the "NZ Protected Disclosures Act 2022" legislation;

5. Considering now the same scenario as #4 with regards to the NZ Protected Disclosures Act 2022, what (if any) additional actions or obligations would you feel are relevant and why?

6. Are there any differences between your answers to #4 and #5 which are material, and if so, what are the factors driving them? Which answer would take precedence and why?

7. Reflect on the same scenario regarding the 737 MAX under the Markkula Framework given in class previously and any differences in your ethical analysis when driven by 'legislative' versus 'non-legislative' ethical criteria. Does having familiarity now with the 'legislative' frameworks alter how you would interpret things under Markkula?

9. Did discussion with your group change your view at any points - which points and why? Consider also whether when discussing with your group, did any of your personality characteristics (from lecture #2 handout) introduce bias your recgonised to your discussion?