(5)
441

Feedback (please also refer to notes on your paper) 88/100 Great!

a) CONTENT: Scope and coverage of work; depth and penetration of analysis and evaluation; use of references beyond the ones suggested; relevance and validity of conclusions; pertinence and incisiveness of views expressed; individuality and creativity.	54 /60 Well done! Superb research, with different angles being considered. Use of literature is really good. Penetration of analysis is right for the size of the report.
b) STRUCTURE: Structure and organisation of work, sequencing and development of facts, ideas and arguments; relationship between findings and conclusions; degree of integration and synthesis.	18 /20 Brilliant - simple, well organised and effective. Paper flows very well, with each section and paragraph doing its own jobs. Congrats!
c) PRESENTATION: Clarity and conciseness of communication; fluency and consistency of style; visual quality and legibility; appropriateness in selection of modes of presentation (written, graphic statistical, etc). Includes correct referencing style and extent of reference sources.	16 /20 Outstanding presentation - just minor typos/missing words. Diagrams are great - figure 1 should be improved. Clarity good. Concise for the number of pages - well done!

80-100	Excellent. Outstanding performance that fulfils and exceeds designated learning outcomes
70-79	Excellent. Excellent performance relative to designated learning outcomes
60-69	Good Pass. Very good performance relative to designated learning outcomes
50-59	Pass. Good performance relative to designated learning outcomes
40-49	Low Pass. Satisfactory performance in designated learning outcomes
35-39	Borderline Fail
0-34	Fail

The Therac-25 Incident

ABSTRACT

A system structure not only comprises of hardware, but software as well. Most of the time, software is overly relied on due to its adaptability to change, and its reliability with maintenance. However, one of the worst cases in medical industry, which was the Therac-25 incident, proved that software should not completely replace hardware and that organisations and designers should take software design seriously in safety critical systems. This paper will consider the major causes of the incident in terms of organisational, human, and technical factors. These causes mainly arise from the lack of safety awareness in the organisation that resulted in innocent deaths of its users and loss to the organisation itself. If organisations were prepared to do a thorough investigation or have sufficient information stored, accidents could be minimized. This incident has given invaluable lessons about handling future accidents and reliance on software alone should be avoided.

KEYWORDS

Safety critical systems, accidents, Therac-25, software safety

1 INTRODUCTION

One of the most infamous incident in the medical industry to date is the Therac-25. The machine was designed to save people and it did save many lives but due to various reasons, the machine led to the death of three people and left three in serious injuries. The defective radioactive machine caused by a killer software bug showed the importance in understanding how the Therac-25 incident has happened. This incident is important not only because the machine is still used today [5], but also because the knowledge can be applied on understanding how accidents happen in other industries as well as being applied on building safer systems in another context. The incident also leaves an impression that software should not be a substitution for physical hardware. In this paper, the Therac-25 will first be introduced on its development and operation, as well as the major events that occurred in the incident. This will provide an idea of the importance of the Therac-25 machine and the amplitude of the consequences. Then, the major causes of what caused the accidents in terms of organizational, human, and technical factors will be discussed. These factors are then further investigated to find out the root causes within the socio-technical system of all parties involved in the incident. Furthermore, the consequences of the accident will serve as a lesson to future system designs as well as how accidents can be minimized in the event of occurrence. This incident has taught organizations not just in terms of safety culture but also leaves a question of ethics on who should be held responsible when accidents occur.

1.1 Development of Therac-25

The Therac-25 was a radiation therapy machine, also known as a linear accelerator that was used to treat cancer patients (see Figure 1). The machine was used to eliminate cancerous tissues and remove excess tumours found in cancer patients.

The Therac-25 was solely developed by Atomic Energy of Canada Limited (AECL) after partnering with a French company called CGR to produce Therac-6 and Therac-20 machines successfully. The machine was arguably cheaper, more powerful, and smaller than its predecessors. Although Therac-6 and Therac-20 used computers as a convenience, Therac-25 was fully operated by a computer controlled via a DEC VT100 terminal [1]. Nevertheless, AECL had first prototyped the machine in 1976, it was only available commercially near the end of 1982 which was claimed at the time that many tests had been done on the machine. As only one machine instead of two was used to shoot both electron and photon beams and there were no hardware interlocks for durability, it was thought to save economic costs because one machine instead of two machines was used and there was no need for hardware maintenance as software is durable. Without hardware interlocks, the machine fully relied on its software to maintain safety of the machine. Using a double-pass concept developed by AECL, the machine was more compact as it benefits from folding the electron accelerator such that the electrons can reach deeper into body tissues as the amount of energy increases.

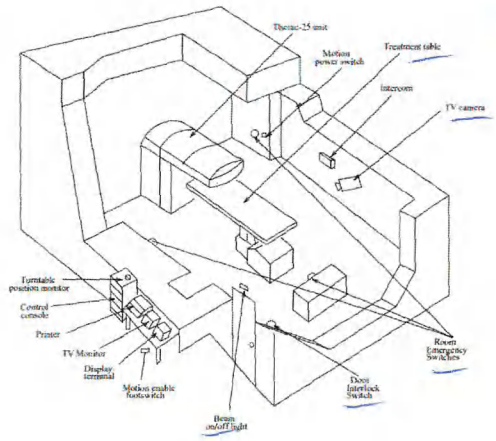

Figure 1. Layout of treatment room and Therac-25 machine [1].

1.2 Operation of Therac-25

The Therac-25 had two modes consisting of low energy mode and high energy mode [1,3]. The low energy mode shoots an electron beam of 200 rad (radiation absorbed dose) range directly on the patient while the high energy mode transforms the electron beam into photons or X-rays that penetrates the body by placing a metal plate between a beam of 25 million electron volts and the patient. Moreover, it has a field light that is used for adjusting the position of the patient.

Controlling these two modes of therapy was the turntable (see Figure 2), checked by three microswitches. In the X-ray mode, a beam flattener shaped like an inverted cone ensures that the beam produced are of equal treatment dose. If the turntable is not placed correctly, the beam flattener would also not be in place that results in overdose to the patient [1]. To prevent that from happening, the computer software is used to make sure that the patient, flattener, and photon chamber are in position. A mirror is placed in the machine for the operator to view where the beam will hit before a treatment begins. To start a treatment process, an operator keys in values for treatment manually into the display terminal inside and outside of the treatment room after the patient is in place on the treatment table. The operator also chooses the mode of the beam by keying in 'x' for x-ray beams and 'e' for electron beams. To deliver the beam towards the patient, 'b' is keyed into the terminal. The computer then checks the input variables if they match and rejects treatment if the variables do not match.

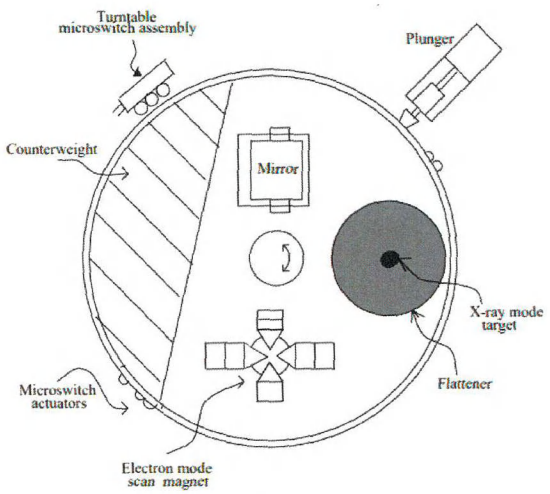

Figure 2. Assembly of upper turntable in Therac-25 [1].

In terms of software, the machine ran on a PDP 11/23 computer and was written in the PDP 11 assembly language [4]. The software was made up of four major components: (i) stored data, (ii) scheduler, (iii) set of critical and noncritical tasks, and (iv) interrupt services. These components share access to the same memory and there was no proper synchronisation was placed for shared variables [1]. The implementation of multitasking in the software partially led to accidents happening which shall be discussed in the paper [4].

1.3 Brief overview of Therac-25 incident

The incident was comprised of six accidents that led to three deaths and led to long-term effects in three other patients caused by the Therac-25 machine. An overdose diagnosis is of more than 1000 rads whereas a regular dose is only about 200 rads. From the table below (see Table 1), it clearly shows the amplitude of radiation overdose in the patients [3, 4,5].

Table 1: Six accidents of Therac-25

Date	Location	Description
3 June 1985	Kennestone Regional Oncology Center, Marietta, Georgia	61-year-old woman suffered severe radiation burns after treatment. It was estimated that she had received 15,000 to 20,000 rads. Her shoulder became unmovable and had to remove both breasts due to overdosed radiation.
26 July 1985	Ontario Cancer Foundation, Hamilton, Ontario, Canada	40-year-old woman reported burning, pain, and swelling. She died 3 months later of her initial cancer being exposed to estimated 13,000 to 17,000 rads.
December 1985	Yakima Valley Memorial Hospital, Yakima, Washington, United States	A woman developed erythema (a skin reaction) of a striped pattern on her hip after treatment. She was scarred, needed skin grafts and slightly disabled.
21 March 1986	East Texas Cancer Center, Tyler, Texas, United States	A man felt skin burn on his back and was observed to develop erythema after being overdosed of estimated 16,500 to 25,000 rads. Within weeks, he lost both legs and left arm. He died five months later from numerous damages in his body.
11 April 1986	East Texas Cancer Center, Tyler, Texas, United States	A man with skin cancer experienced burns on his back from 180 rads of radiation. He died after 3 weeks from exposure to

		radiation on the right temporal lobe and stem of the brain.
17 January 1987	Yakima Valley Memorial Hospital, Yakima, Washington, United States	The patient experienced skin burns with a striped pattern like previous case. He died from overexposure to radiation 3 months later.

2 MAJOR CAUSES OF THERAC-25

The Therac-25 was caused by many different factors, which was like a snowballing effect. This paper will explore the causes in terms of organizational, human, and technical factors. Organizational being the organisations involved including the main manufacturer AECL, government regulations including Food and Drug Administration (FDA) and the Canadian Radiation Protection Bureau (CRBP), and the treatment sites implementing the use of the Therac-25. Human factors include the designers of the machine. In terms of technical factors, it would be the faults in the software and hardware of Therac-25.

2.1 Organizational factors

2.2.1 AECL. The machine was first developed by the company and was considered to hold the most responsibility for the malfunction of the machine. The company structure itself lacks communication with the users in the management level as well as the technical department that designed the machine.

Technical department. Even before the accidents occur, the company lacked proper organisation in its technical system structure. According to Nancy [4], AECL lacked software documentations of the requirements and test plans. Despite having done numerous tests on its software of up to 2700 hours of use, it was found that the company mainly performed integrated system tests (as whole machine) in which timing analysis and unit testing (as separated modules) should also be performed [4,5]. AECL further argued that their software tests were done on a hardware simulator as well as under field conditions such that errors in the code are reduced to minimal. Furthermore, it was claimed that a hazard analysis was performed on the product with a fault tree analysis. However, the analysis did not cover software aspects such as residual errors. This later caused execution errors and random errors in the program. Another serious issue was that there was no justification to how the probabilities were assessed. Indeed, the possibility of "Computer selects wrong energy" was assigned to be 10^{-11} while it was 4×10^{-4} for "Computer selects wrong mode" [4] after investigation was carried out. It may be possible that proper numeric assessments were unavailable at the time for better estimation of such numbers which resulted "a popular number" to be assigned to items related to software [1].

Following the fourth and fifth accidents, it was found that the company lacked documentation for system errors. In these accidents, it was described that a 'Malfunction 54' error had appeared on the terminal screen, but it was mostly unknown what the errors meant [4]. The deficiency of information led to operators ignoring the error messages and further carried on the procedure of the machine. As reported in the investigation of the second accident, the operator had seen a 'No Dose' message on the computer but repeatedly keying 'P' to proceed the dose of up to 5 times. The machine with an error on the terminal the proceeded to hit the doses on the patient based on the number of times the key was pressed, leading to the patient's death due to overdose [4,5]. This suggested that the company did not practice good programming documentations and indirectly led accidents to occur.

Besides that, the whole program of the software was done by only one programmer within the company. Programming practices promotes pair programming, or at least a review of code. The self-bias of the programmer may cause problems in the code. Another serious issue was the handing of the entire software development to a program without any background check or records. There was no information on the programmer's background nor experience other than having some form of involvement in the Therac-20 [4,7]. The programmer had no formal training and no further details were stored to carry out internal investigation after the accidents had happened. This posed an unanswered question about why routines for Therac-20 was found in Therac-25. Perhaps it was due to the success of previous machines and that there were no errors detected in previous machines, the old software was modified for the Therac-25 which had similar functionality instead of designing a new software for the machine [1, 4,7].

Managerial department. Although the first accident happened after about more than two years of successful treatments, their initial response to the first accident were poor that resulted later accidents to happen. McQuaid noted that the first accident was not reported to FDA until after the fourth and fifth accidents happened [7]. A physicist even asked if overdose is possible but AECL denied the possibility after the first accident [1]. The company showed negligence to the incident by not even conducting minimal investigation to the cause of the accident.

Until the second accident happened, AECL did not investigate the machine further. They sent a service technician to the treatment site but as the malfunction could not be reproduced, it was concluded that the microswitches in the turntable had to be fixed and nothing was wrong with the software [1]. Their response later was to ask users check

manually the position of the turntable before use in case the microswitches needed to be fixed [4]. Although an independent consultancy had suggested the use of an independent physical interlock known as a potentiometer, AECL did not adhere to the recommendation and only incorporated tracking of the microswitches movement following the accident [4, 6]. The company even claimed the machine to be 10,000 times safer after the hardware fix [7]. The company did not question the software and only fixed the hardware at this point. Due to AECL's statement, there was no fixes to the software in which errors were later found in it that caused the machine malfunction [1, 4].

When the third accident happened, AECL feigned ignorance again. They declared that the "damage could not have been produced by any malfunction of the Therac-25 or by any operator error" [4]. They even denied responsibility of previous two accidents by stating that there were no other similar incidents to the third patient [6]. However, it was known that there was an evidence of overdosed radiation from Yakima Memorial Valley Hospital [7]. As AECL was the manufacturer of the machine, they should take the responsibility of the faults caused by the machine and not taking any actions to stop the issues from happening further caused more accidents than necessary.

When the fourth accident happened, it was obvious that AECL lacked procedural protocols in case of risks occurring. They did not take immediate and suitable actions even after mortality of patients had occurred such that the machine was still being used when it had problems. Following the fourth accident, AECL did not seem to take the safety of the product nor the situation seriously by denying possible problems even though an electrical fault was suggested to be the cause [6].

The repeated denials from the company caused accidents to continue as the first cases of accidents occurred. The company's inability to handle the situation and unwillingness to take responsibility may be one of the main contributing factors for the accidents to happen [7]. Although the incidents were finally reported after the fourth and fifth accident, it was too late to stop the sixth accident from happening. It further showed that the company did not take safety of the product seriously and had overconfidence in their machine's previous successions.

2.2.2 FDA and CRBP. The organisations were part of the government to conduct tests and safety analysis. They should be the organisations that sets standards and guidelines for machines to be approved for industrial use.

Prior to the incident, the fact that Therac-25 did not undergo a thorough analysis may be a factor of the accidents to happen. It was suggested that there was bias towards Therac-25 due to the success of its predecessors and the assumption of software being safer than hardware [11]. In addition, the organisations lacked communication with AECL and the users of the product because of incomplete reporting requirements [7]. If the accidents were known earlier, the accidents may not occur. According to the United States Government Accountability Office study at the time, most injuries that were mainly caused by hardware failure and design flaws in machines were unreported to FDA [11]. If they communicated better with the hospitals, they would be aware of the incidents despite AECL's denial of responsibility.

In addition, the two organisations were notified after the second accident and while FDA audited the modifications to the microswitches, they may have overlooked the process as further accidents still happened [7].

2.2.2 Treatment sites. The hospitals hold partial responsibility for the accidents happening as they implemented use of the machine.

According to Nancy [4], there were no proper education or training to the operators at the hospitals then. Despite some hospitals offering classes to operators, they were not standardized as a unique curriculum such that operators were all trained differently [12]. Prior to the fourth accident, it was already known that the video monitor was unplugged and broken, but the operator had proceeded in using the machine without having a visual supervision of the situation inside the treatment room [7]. From the controls, it was reported that a "Malfunction 54" error had occurred but instead of checking the machine, the operator had ignored the error message and proceeded to key in buttons for up to five times that caused severe overdose to the patient. If the hospitals provided protocols or training on handling machines, such accidents would not occur.

2.2 Human factors

2.2.1 Designers of Therac-25. As mentioned previously, a whole new feature of the Therac-25 machine was introduced which was the use of software and removing hardware interlocks. It was suggested that these hardware interlocks were not even replaced by software interlocks that would perform the same functionality [13]. There was a lack of documentations including user manual such that it was insufficient and vague [12]. In addition, the programmer did not redesign the software for the Therac-25 but instead reused routines from Therac-6 and Therac-20. The reuse of software carried a bug from Therac-20 to Therac-25 [11] and due to the absence of hardware interlocks that would have cut off the power supply to the machine to prevent an accident from happening, the machine proceeded with the treatment which led to an overdose of radiation.

2.3 Technical factors

The main issue with the software of the Therac-25 machine was a fatal bug was also found in the Therac-20 machine [2]. However, the hardware interlocks in Therac-20 had intervened the accident from happening [4]. This bug was identified as a "race condition" that could be triggered by an experienced operator for editing the input but not being registered by the computer due to a time dependent input [10, 11, 13]. This condition refers to the access of a variable at the same time without an intervening synchronization [7, 14]. This produced an error known as "Malfunction 54" and was later reproduced by a physicist after the fifth accident [4]. It takes 8 seconds for the machine to switch between low energy mode and high energy mode. If a fast typist edited the inputs before 8 seconds, the error would be triggered [11].

Another flaw in the software of the machine was the poor user interface. It was suggested that the poor user interface led information of the prescription and dose rate to be keyed improperly [7]. If error messages were to appear, it was vague what caused the malfunction and no explanation of the error that operators became insensitive to the "Malfunction 54" errors [4]. Furthermore, if other error messages appeared, they were basically identical and could also be overridden [11].

3 FLAWS IN SAFETY CULTURE

The main causes leading to the accident was a result of flaws in safety culture. AECL was lacking in terms of investigation, testing, as well as documentations and guidelines. AECL's poor responses to the various accidents resulted from an overconfidence in software that they underestimated software-related risks by replacing hardware interlocks with software checks [1, 12]. Their assumption of risk decreasing over time placed their machine in high risk. This became critical when AECL had the assumptions that software does not fail and that programming errors can be reduced by testing on simulators instead of real hardware [14]. The company should know that unobserved errors in previous machines do not mean that errors do not exist. In addition, without following up or investigating reported accidents, it was clear that they did not take safety of the machine into priority [1]. By assuring the users of the machine that it was impossible for overdose to occur, they had showed ignorance to serious events that could occur even if it was of a low chance [1]. The deficiency of information on several accidents had been clear that AECL was ineffective with technical activities.

4 RESULTS OF THE THERAC-25 INCIDENT

The accidents had caused a great loss to the patients themselves, and emotional pain to families and friends of the patients. Innocent lives were taken away due to the malfunction of a machine. Despite the first patient attempt to sue AECL, there were no further news of that lawsuit and no punishments were given to any party after the accidents [1].

Furthermore, AECL had to suffer the consequences to deal with the issues founds in the machine. In 1991, FDA banned the Therac-25 and all other machines produced by AECL [2]. It was not until 1994 that the ban was entirely lifted. During this period, a demand for personnel were increased to get the machine repaired and to implement guidelines for future products [1]. The company most likely suffered a great loss in terms of financial costs and reputation.

Following the accidents, the government took steps to avoid such accidents to happen again by increasing safety standards [1]. They also made the legislation for communication with users of medical devices by making it mandatory for incidents to be reported to the FDA and manufacturers [11]. Moreover, policies were put in place and required further documentations such that third-parties can examine and retrace flaws in devices [11].

5 MINIMIZING RESULTS OF THE ACCIDENT

5.1 Attempts

Although AECL had failed to minimize the risks by fixing the machine, it should be taken note that they did attempt to. Following the second accident, AECL had fixed the interlocks of the machine. It was until the sixth accident that they shut down their systems and do a complete investigation and repairs to the machine which was after FDA had taken actions to ban the machines [1,4].

5.1 What could have been done

According to [13], stress testing and fault injection during the test phase could predict problems with the software. A stress test is in which multiple requests are sent to the system to assess the workload of the system. By using fault injection analysis with test cases including time-dependent input cases, the main bug that caused the Therac-25 would be detected [13].

Other suggestions include a thorough software evaluation before the release of the product. Through software testing, measurement of system behaviour (such as benchmark and acceptance tests), as well as measurement of software development process [8], qualities of the product can be verified. A software validation and verification can also be further extended to include user interfaces to avoid the human factor issues in the incident [8]. This implies that designers should also consider the conditions of use, commonality of the software, and the feedback process for fixes to be delivered prior to accidents happening [9].

From another perspective, AECL should have taken prompt and immediate actions following the accidents. If they have

reported the incident since the first accident to the FDA and taken thorough investigations as to what have led the machine to malfunction, the later accidents could have been prevented.

6 LESSONS LEARNT

Before the accidents happened, there are a few lessons to be learnt such as having sufficient information stored about the products, and the staff in the company. The background information about the staff is relevant as it provides details on the experience and knowledge in the field as well as being able to contact them in event of risk. User manuals and maintenance guides should also be kept on record to implement fixes. In other words, a company should have complete documentation and practices for programming and tests. On top of that, a system should not depend on previous software that had worked but instead, redesign a new structure for it [7].

An important lesson to be learnt from the period of accident occurring is to conduct thorough investigation to know what triggered the accident [7]. It would be too late to fix the problem when the harms had been done. Also, a look for the root cause should be done instead of surface causes with proven evidence [6]. A report of this results should be communicated as well to the users and employees to avoid repeating the mistake.

Aside from the situation itself, lessons can be learnt from the machine itself. It is possible that the Therac-25 had other undetected errors other than the known bugs. However, with hardware interlocks installed after the accident, the bugs were not observed. In terms of software, a system log can be placed such that the inputs are recorded to find where an error was triggered [7]. It is essential to remember that reliability is not equivalent to safety and as such, even if the machine had worked successfully most of the time, the fact that a small number of accidents is still deemed unacceptable [6].

Future systems should consider moral responsibility for legislation of law to take place. It is crucial to consider whether software programmers should be held responsible for poor design of computers as errors are unavoidable but not always detected [10, 16].

CONCLUSION

The Therac-25 incident acts as a guidance for future safety critical systems to be built. Although it may seem like most responsibility was played by the level of management in the manufacturer company, AECL, the design issues made by the designers within the company should not be neglected as well including the technical errors that took place. The main causes of the accidents were resulted from a lack of awareness about safety culture at that time and teaches an important lesson about software designs. Accidents may not be intentional, but they should be expected, if not, there should be protocols for such incidents to happen. It should be taken note that besides tests, quality assurance and risk assessment would minimize or at least contain accidents should they occur. An important lesson learnt from this incident is to not overly rely on software and to think about who should be held responsibility should such an accident happen again.

REFERENCES

[1] Leveson, N. *Safeware: System Safety and Computers*. Addison-Wesley, Boston, Mass., 2001.

[2] Fatal Dose - Radiation Deaths linked to AECL Computer Errors. *Ccnr.org*. http://www.ccnr.org/fatal_dose.html.

[3] Fabio, A. Killed by a Machine: The Therac-25. *Hackaday*, 2015. https://hackaday.com/2015/10/26/killed-by-a-machine-the-therac-25/.

[4] Leveson, N. and Turner, C. An investigation of the Therac-25 accidents. *Computer 26*, 7 (1993), 18-41.

[5] Gallagher, T. Therac-25: Computerized Radiation Therapy. https://web.archive.org/web/20071212183729/http://neptune.netcomp.monash.edu.au/cpe9001/assets/readings/www_uguelph_ca_~tgallagh_~tgallagh.html.

[6] Kletz, T. *Learning from accidents in industry*. Butterworths, London, 1988.

[7] McQuaid, P. Software disasters-understanding the past, to improve the future. *Journal of Software: Evolution and Process 24*, 5 (2010), 459-470.

[8] McDaniel, J. Improving system quality through software evaluation. *Computers in Biology and Medicine 32*, 3 (2002), 127-140.

[9] Huff, C. Unintentional power in the design of computer systems. *ACM SIGCAS Computers and Society 26*, 4 (1996), 6-9.

[10] Huff. C.W., & Brown, R. "Integrating ethics into a computing curriculum: A case study of the Therac-25." In A. Akera & W. Aspray (Eds.), Using history to teach computer science and related disciplines. Washington DC: Computing Research Association. 2004, pp. 255-277.

[11] A History of the Introduction and Shutdown of Therac-25. *ComputingCases.org*. http://www.computingcases.org/case_materials/therac/case_history/Case%20History.html.

[12] Madadipouya, Kasra. 2016. Rules of software quality assurance to prevent and reduce software failures in medical devices: Therac-25 case study. DOI: 10.6084/M9.FIGSHARE.3362281.V3.

[13] Voas, J. Software Fault Injection: Growing Systems. *Aerospace Conference*, 1997. DOI: 10.1109/AERO.1997.578000.

[14] De Florio, V. *Application-layer fault-tolerance protocols*. Information Science Reference, Hershey, 2009.

[15] Mandrioli, D., Morasca, S. and Morzenti, A. Generating test cases for real-time systems from logic specifications. *ACM Transactions on Computer Systems 13*, 4 (1995), 365-398.

[16] Birsch, D. Moral Responsibility for Harm Caused by Computer System Failures. *Ethics and Information Technology 6*, 4 (2004), 233-245.