December 7

Assignment #2

PROG1350 – Software Engineering Fundamentals

Verdi Rodrigues-Diamond

Table of Contents

Disaster #1 – Therac-25

a) Describe the background behind the incident.

The Therac-25 was a new model of a radiation therapy machine, which was produced after the Therac-6 and built off of the Therac-20. Radiation therapy through this type of machine is a commonly used technique for people who have cancer. It works by killing off the rogue cancer cells by damaging their DNA. This technique generally uses X-rays, gamma rays, and charged particles (such as beta particles) for treatment. (Garfinkel, 2005) This treatment technique damages normal cells as well as cancer cells so the setup and use of a radiation therapy machine must be carefully as to minimize side effects.

b) Describe the problem.

Given certain circumstances, the Therac-25 medical radiation therapy machine is prone a malfunction where the machine changes the radiation target somewhere slightly off from the desired location and then delivers high-power doses of radiation. Since healthy uninfected cells are also destroyed using this procedure (National Cancer Institute, 2010), it ended up being fatal to many patients at several different medical facilities. Also, as a design consideration when building this solution, the company decided that the software to run on this machine was so stable that it did not need any kind of emergency kill switch.

c) Describe the cause or causes behind the problem

The cause of this product malfunctioning was later found out to be a bug in the operating system where, if the operator types in the prescription too fast, the machine could not accept it properly and would configure for high power mode at an incorrect location. This type of error is commonly known as the "race condition" (FreeBSD Documentation Project), simply meaning a flaw which is determinant on two signals racing each other to influence the output first. This issue is predominant in software doing asynchronous I/O and using shared memory on multiple threads or processes. This issue is also prevalent in hardware under certain conditions. (Netzer & Miller, 1992)

d) What would have prevented the problem?

This issue could have been prevented if the engineers had tested operating system of the machine more closely and had looked further into the control of asynchronous threads. Also, this issue was not helped by the design choice of not including an emergency stop button to turn off the machine quickly if a malfunction occurs. This was left out however because the company decided that their software was going to be so stable that it wouldn't need one.

e) Did this occur because a requirement was changed inappropriately? Justify your answer.

I do not believe that events which forced the Therac-25 to cease being used were do to requirements being changed inappropriately however, I do certainly believe that the product would have benefitted from having a more specific set of requirements before the product was delivered for clinical use. Also, a more thorough run through on the inner workings of the operating system the Therac-25 operated upon would have certainly benefitted everyone involved.

f) Did this occur because the technology was rushed? Justify your answer.

In my opinion, the errors prevalent in the Therac-25 were not caused by the technology being rushed but rather because of an insufficient analysis of the requirements and expected use case as well as the removal of hardware interlocks. That is not to say that the making of the Therac-25 could not have benefited from having a slower more thorough development process. If the manufacturer of the Therac-25 had bothered to do more extensive testing and vetting of the base operating system before boasting of it's stability, they would have quickly discovered the errors which have made this product a gigantic failure.

g) Did this occur because the problem should have been caught by normal testing but was not? Justify your answer.

Since this error sounds like it would have been fairly difficult to reproduce unless a developer tests their code on a running machine themselves, I'm not entirely sure the problem would have been caught in normal testing circumstances. Despite this however, the original software engineers should have put more time into testing the operating system by itself before claiming that it was, software wise, bulletproof.

h) Did people pre-warn against the possibility of such a problem occurring? If so, what role did they have and why were their warnings ineffective. Justify your answer.

In this situation, people were certainly not pre-warned against the possibility of such a problem occurring. In fact, the company who produced the Therac-25 would, on occasion, boast about the stability of the platform and the operating system beneath it.

i) What role did software or electronic systems play in causing the disaster? Justify your answer.

In this disaster, the software and electronic systems teamed up to make something which is extremely destructive. This is due to the reliance on the inconsistency that is software and software development paired with the power that is "does something in real life" hardware. As an example, if the software was Carlo and the hardware was a gun, Carlo would have no trouble taking the gun and shooting someone in the head.

http://www.dcs.gla.ac.uk/~muffy/paper (Thomas, 1993)s/HIS1.pdf

http://www.ingentaconnect.com/content/jcaho/jcjqs/2004/00000030/00000012/art00007

Disaster #2 – Mars Climate Orbiter

a) Describe the background behind the incident.

The Mars Climate Orbiter was to spend a year in a near circular, near polar 400km orbit collecting weather data to help scientists better understand Mars's climate (NASA).

Launched in December of 1998, the Orbiter was originally atop a Delta II launch vehicle. Within approximately a quarter of an hour and after several burns, the Orbiter had shed its solid-rocket boosters and was in orbit around Earth. Within forty-five minutes of launch, the Orbiter freed itself from Earth's gravity and was on its way to Mars (NASA, 1998).

During the Orbiter's journey, there were to be trajectory corrections (NASA). Also, as the Orbiter was not symmetrical, pressure from the sun would cause it to spin or rotate. Although the Orbiter had gyroscopes, burns were also required to stabilize the craft (Recer, 1999).

Mission reports released between the Orbiter's December 1998 launch and September of 1999 suggested that everything was working fine with the spacecraft (NASA 2000). On September 23rd, 1999, however, NASA announced that the Orbiter was believed to have been lost due to a suspected navigation error. The plan had been for the Orbiter to approach Mars at an altitude of 150km. After the craft disappeared, data showed that the approach had been much lower (approximately 60km) (NASA, 1999). On September 24th, 1999, NASA flight controllers abandoned the search for the device, believing that it could not have survived its mis-aimed approach and reviews began to determine the cause(s) of the loss (NASA, 1998).

b) Describe the problem.

Although everything had seemed fine until it was time for the final maneuvering to put the Orbiter in orbit around Mars, the Orbiter disappeared behind the planet as planned and then never reappeared. A review of the data leading up to the Orbiter's arrival indicated that it was at a much lower altitude than intended. In fact, this altitude was below the craft's minimum survival altitude (NASA, 1998) (NASA, 1999).

c) Describe the cause or causes behind the problem

By September 30th, 1999, NASA was reporting that its Orbiter team had discovered the likely cause of the loss. The Orbiter spacecraft team in Colorado and the mission navigation team in California were using different units of measurement – one English (e.g. inches, feet, and pounds) and the other metric. This led to incorrect maneuvering when trying to place the craft into orbit around Mars. For example, "Engineers on the ground calculated the size of the rocket firing using feet-per-second of thrust, a value based on the English measure of feet and inches. However, the spacecraft computer interpreted the instructions in Newtons-per-second, a metric measure of thrust. The difference is 4.4 feet per second" (Recer, 1999). With each firing of the rocket, the error increased.

Dr. Edward Weiler, NASA's Associate Administrator for Space Science said, "The problem here was not the error, it was the failure of NASA's systems engineering, and the checks and balances in our processes to detect the error. That's why we lost the spacecraft" (NASA).

By November of 1999, Lockheed Martin, the prime contractor for the Orbiter, announced that their "engineers were responsible for ensuring that the metric data used in one computer program were

compatible with the English measures used by another program. The simple conversion check was not done" (Recer, 1999).

In the same month, the mission failure investigation report was released. It identified the unit of measurement problem as the root cause of the loss, but also identified several other factors such as, "inadequate consideration of the entire mission and its post-launch operation as a total system, inconsistent communications and training within the project, and lack of complete end-to-end verification of navigation software and related computer models" (NASA, 1999).

d) What would have prevented the problem?

This problem could have been easily of been prevented if NASA had taken the proper steps to build a thorough set of requirements. This problem was not helped though by poor communication between the crew of said requirements as well as to bring their sibling stations and contracted partners onto the same page. If NASA had been able to be just that bit more clear when creating their requirements, I believe this project would have resulted completely differently.

e) Did this occur because a requirement was changed inappropriately? Justify your answer.

The issues which effected the Mars Climate Orbiter did not occur due to requirements changing but because some important and more specific requirements surrounding unit standardizations were never listed as requirements.

f) Did this occur because the technology was rushed? Justify your answer.

No. As layed out above, the issues concerning the Mars Climate Orbiter project were due primarily to an incomplete set of requirements which do not take into concern all of the required requirements. There is no evidence to support that the failure of this project was due to a lack of time and the technology being rushed.

g) Did this occur because the problem should have been caught by normal testing but was not? Justify your answer.

Despite the issues surrounding the Mars Climate Orbiter being more of a requirements issue more than anything else, I do believe that this was a testing issue as well.

h) Did people pre-warn against the possibility of such a problem occurring? If so, what role did they have and why were their warnings ineffective. Justify your answer.

No. The people involved in this project were not warned against the possibility of such a situation occurring because poor software requirements and poor communication led

i) What role did software or electronic systems play in causing the disaster? Justify your answer.

In the crash of the Mars Climate Orbiter, the both the software and hardware aboard the vessel and on ground control played an important part in affecting the outcome of the events yet to come. Although

poor requirements and improper communication were the true cause of NASA losing control, it was later determined to be, as an indirect result, a maths error between conflicting stations with one using imperial units and the other using metric. When precision mathematics are used as a definitive source of control, any decent business analyst would collect which unit would be preferred because, as happened with the climate orbiter, bad things will happen if you do not collect and standardize all of the requirements before the project has been completed.

Disaster #3 – Aeroperu Flight 603

a) Describe the background behind the incident.

Aeroperu flight 603 was a scheduled flight between Lima, Peru and Santiago, Chile. Shortly after arriving from the previous flight, the Boeing 757 underwent maintenance operations to make sure that the airplane was in good working condition for the next flight. Within a few minutes after take off, the pilots noticed that the airplane was giving off readouts for altitude and airspeed that did not seem to correlate with what was going on around them and signalled for emergency. Unfortunately however, due to what seemed to be a myriad of impossibly different indicators going off at the same time and the inability to decipher which readouts were correct and which weren't, the airplane's wing touched water and then 20 seconds later crashed into the Pacific Ocean.

b) Describe the problem.

During flight 603, the airplane in use (a Boeing 757) delivers incorrect information about airplane airspeed and altitude. Since the flight occurred overnight and over water, the crew could do nothing but trust their sensors and radar reports from the ground station.

c) Describe the cause or causes behind the problem

The cause to the problems with the airplane's airspeed indicator and altimeter was later discovered to be due to blocked static pitot tubes after a quick maintenance cleaning between flights. An airplanes airspeed and altitude are determined by a moving membrane and barometer. These two sensors use the air around the airplane, through static ports, to calculate speed and altitude. When the static pitot tubes are blocked however, this instrumentation will provide erroneous readings that do not correlate with what is actually happening.

Because an airplanes pitot tubes are sensitive equipment and do not handle … well, they are blocked during regular cleaning and polishing procedure to make sure that animals, dust & debris, and other materials do not get in and clog the sensors. Unfortunately in flight 603 however, this blocking material, later found out to be a piece of masking tape, was never properly removed when the airplane was going through take-off inspection.

d) What would have prevented the problem?

This problem could have been prevented by the maintenance staff remembering to remove the tape from the airplane's static ports before take off. This would have been easily corrected if more strict policies around retrieving aircraft from storage were implemented. After flight 603, the NTSB put out a safety warning to the FAA to force airplane companies to use specialized brightly coloured protective covers for when an airplane goes under maintenance so that this is not forgotten again.

This issue may have also been preventable if the airplane's computers were less insistent on what was actually going on. When the crash occurred, the airplane was reading overspeed, stall, and land something. Each of these indicators has it's own horn, light, and in the case of the land something something called a "stick shaker" where the aircraft controls move violently to force the captain to lift the airplane up.

e) Did this occur because a requirement was changed inappropriately? Justify your answer.

This error did not occur because of requirements before take off changing inappropriately although I do think that it occurred due to an improper checking of said requirements. Every member of the staff who worked the plane in question before flight 603 took off had their own checklist of equipment and parts of the plane to check over including the pilot's final check over of the entire plane. The block of the pitot tubes should have been caught as part of the maintenance check over checklists but wasn't because it was dark and the masking tape used matched the color of the plane almost exactly. Also, the opening for the static pressure pitot tubes are quite high up making it difficult to see in the dark with a flashlight from ground level.

f) Did this occur because the technology was rushed? Justify your answer.

I don't think this error occurred because the technology was rushed but I do think it could definitely be improved with the more recent technology of today. Using dynamic and static pitot tubes to measure speed and altitude is an extremely effective tactic for getting accurate readings. I do however think that there should have been some kind of fall back sensor of a different type to rely on in cases such as this where one type of sensor has failed so thoroughly. When these planes were manufactured back in the day, GPS would not have been an option because it didn't exist but now it would make a lot sense to equip these planes with GPS because it gives accurate readings without needing the direct use of the environment around it like with pitot tubes. Therefore I think that GPS would have been of great use as a secondary sensor to provide a more reliable and stable contrast against the erroneous pitot tube readouts in the unfortunate crash of flight 603.

g) Did this occur because the problem should have been caught by normal testing but was not? Justify your answer.

This issue was not caused due to improper testing because, in the maintenance handbook from Boeing, it was listed as one of the requirements that the aircraft's static ports must remain clear for the aircraft to fly. This should have been caught though by the maintenance crew after cleaning or the during the Captain's pre take off check.

h) Did people pre-warn against the possibility of such a problem occurring? If so, what role did they have and why were their warnings ineffective. Justify your answer.

The aircraft manufacturer did provide a warning in their maintenance handbook and provided warning that the aircraft would not work properly but I don't think that any company could really predict the horrific events of flight 603. While testing software in the lab, it is easy to make assumptions about intended use cases and expected failures but, when it comes to the real world, there ends up being a lot more to think about.

i) What role did software or electronic systems play in causing the disaster? Justify your answer.

In flight 603, software was not directly the cause of the crash, but it didn't help either. The crash of flight 603 was due to erroneous readings coming from hardware sensors on the outside of the plane. These readouts are crucial to flying a plane and, without them, the crew was basically flying blind. The problem with the software in the Boeing 757 is that it believes the airplane's sensor readouts almost unconditionally. Despite the autopilot having an automatic disengage when the captain and the co-pilot's readouts are so different, it still uses the captain's readouts for indicators such as overspeed and stall. When these indicators fire, flashing lights appear on the plane's control panel and horns are sounded. When something like an overspeed situation and stall condition conflict, and error which could never happen in real world conditions, it has the effect of making the pilot's area a hostile place and very hard to make good decisions in.

Disaster #4 – Royal Majesty

a) Describe the background behind the incident.

The Royal Majesty was a cruise line run by Majesty Cruise Lines between Bermuda and Boston Massachusetts.

b) Describe the problem.

On June 10th, 1995, the Royal Majesty ran aground about on Rose and Crown Shoal about 10 miles east of Nantucket Island, Massachusetts.

c) Describe the cause or causes behind the problem

This crash was caused by the overdependence on GPS technology, a poorly communicating crew, and the lack of concern to cross reference information gathered from modern technology with more traditional techniques of positional tracking. The Royal Majesty was equipped with two different technologies for positional tracking on the water, GPS and Loran-C.

d) What would have prevented the problem?

This problem could have been prevented if the crew had cross checked the information they gathered from both GPS and Loran-C with more traditional forms of position tracking such as using waypoints for guidance. Because more modern technologies such as GPS are so often accurate, it builds a mistrust and overreliance on a technology that can so often be misleading. Also, the crew of the ship communicated in a fashion much like the old game "telephone" in that they did not fully mention or debrief all of the events of the shift when to the new officer on shift when the first one was relieved from duty for the night.

e) Did this occur because a requirement was changed inappropriately? Justify your answer. (National Transportation Safety Board, 1997)

This error did not occur due to a requirement that was changed inappropriately but I do believe that better creation and enforcement of new requirements about safety for more modern technologies for positional tracking would have certainly aided the situation. Because the crew was not forced to, by requirements, to check GPS and Loran-C as well as more traditional forms of tracking, the crew was able to build an overreliance on one form of technology. If more strict requirements were in place, I do not believe this would error would have occurred.

f) Did this occur because the technology was rushed? Justify your answer.

I do not believe that this error occurred due to the technology being rushed in it's implementation however, I do believe that ship crews had had enough time after the technology's implementation to grow accustomed to the ins and outs of when and how It works and when you should ignore it and use something else. Because of an overdependence on these newer technologies, other tactics for position tracking were not used and therefore an incident like this was able to occur.

g) Did this occur because the problem should have been caught by normal testing but was not? Justify your answer.

This incident was not directly caused due to technology providing issues which should have been caught in normal testing as the equipment was tested regularly and, when testifying, the navigator mentioned that he checked all positional equipment 30 minutes before the ship's departure and verified that they were all working as expected.

h) Did people pre-warn against the possibility of such a problem occurring? If so, what role did they have and why were their warnings ineffective. Justify your answer.

Nowadays, it is almost commonplace to have a distrust of technology as a sole provider of data with a special concentration of distrust on GPS specifically. So much so that it seems almost to be engrained in our society. Back in the day however, people weren't as hard core in not believing GPS. This is why I believe that the crew aboard MS Royal Majesty were able to so easily rely on using GPS as a sole positional tracking utility. Because our society has changed since 1995 however, I don't think this as possible to happen any more.

i) What role did software or electronic systems play in causing the disaster? Justify your answer.

In this disaster, the software and electronic systems aboard MS Royal Majesty were the mainstay of the entire incident. The positional systems aboard provided a situation very much like being the genius person in a class who sits in a corner and is almost never wrong. When they are however, they are very very wrong. Because these systems are so often correct and are checked for providing accurate information regularly, it is very easy to become accustomed to them always accurate. Unfortunately, the crew was forced to learn the hard way that this is not always true and their methodology was clearly proven to be a mistake.

Bibliography

DIRECTORATE GENERAL OF AIR TRANSPORT. (n.d.). *ACCIDENT INVESTIGATION BOARD OF THE DIRECTORATE GENERAL OF AIR TRANSPORT.* Retrieved December 7, 2012 from SKYbrary: http://www.skybrary.aero/bookshelf/books/1719.pdf

FreeBSD Documentation Project. (n.d.). *3.7 Race Conditions*. Retrieved November 22, 2012 from FreeBSD Handbook.

Garfinkel, S. (2005, November 8). *History's Worst Software Bugs*. Retrieved 11 22, 2012 from WIRED: http://www.wired.com/software/coolapps/news/2005/11/69355

Lloyd, R. (1999, September 30). CNN. *Metric Mishap Caused Loss of Nasa Orbiter* .

Cairo, J., Horstman, F., Leider, J., Waltzer, R. (Producers), Lund, K., Scott, T., DeMille, N., Block, T. (Writers), & Scott, T. (Director). (2012). *Mayday: Flying Blind* [Motion Picture]. Canada.

NASA. (1999, November 10). *Mars Climate Orbiter Failure Board Releases Report*. Retrieved December 7, 2012 from Mars Polar Lander: http://mars.jpl.nasa.gov/msp98/news/mco991110.html

NASA. (1998, December 11). *Mars Climate Orbiter Mission Status*. Retrieved December 7, 2012 from Mars Polar Lander: http://mars.jpl.nasa.gov/msp98/news/mco981211.html

NASA. (n.d.). *Mars Climate Orbiter Science Goals*. Retrieved December 7, 2012 from Mars Climate Orbiter: http://mars.jpl.nasa.gov/msp98/orbiter/science.html

NASA. (n.d.). *MARS CLIMATE ORBITER TEAM FINDS LIKELY CAUSE OF LOSS*. Retrieved December 7, 2012 from Mars Polar Lander: http://mars.jpl.nasa.gov/msp98/news/mco990930.html

NASA. (n.d.). *Mars Climate Orbiter/Mars Polar Lander Mission Overview*. Retrieved December 7, 2012 from Mars Polar Lander: http://mars.jpl.nasa.gov/msp98/mission_overview.html

NASA. (n.d.). *Mars Surveyor 98 Status Reports*. Retrieved December 2012, 2012 from Mars Polar Lander: http://mars.jpl.nasa.gov/msp98/news/status.html

NASA. (1999, September 23). *NASA'S MARS CLIMATE ORBITER BELIEVED TO BE LOST*. Retrieved December 7, 2012 from Mars Polar Lander: http://mars.jpl.nasa.gov/msp98/news/mco990923.html

National Cancer Institute. (2010, June 30). *Radiation Therapy for Cancer*. Retrieved 11 22, 2012 from National Cancer Institute: http://www.cancer.gov/cancertopics/factsheet/Therapy/radiation

National Transportation Safety Board. (1997, April 7). *MARINE ACCIDENT REPORT.* Retrieved December 7, 2012 from National Transportation Safety Board: http://www.ntsb.gov/doclib/reports/1997/mar9701.pdf

National Transportation Safety Board. (1996, November 15). *Safety Recomendation.* Retrieved December 7, 2012 from National Transportation Safety Board: http://web.archive.org/web/20081101013700/http://www.ntsb.gov/Recs/letters/1996/A96_141.pdf

Netzer, R. H., & Miller, B. P. (1992). What are race conditions?: Some issues and formalizations. *ACM Letters on Programming Languages and Systems (LOPLAS)* , 74-88.

Recer, P. (1999, November 10). *Contractor takes blame for math goof that crashed Mars probe*. Retrieved December 7, 2012 from http://www.cse.lehigh.edu/~gtan/bug/localCopies/marsOrbiter

Thomas, M. (1993, August 12). *The Story of the Therac in LOTOS.* Retrieved December 7, 2012 from http://www.dcs.gla.ac.uk/~muffy/papers/HIS1.pdf