Brandon Davies

6271977

Submitted: Nov. 4, 2014

Disaster R­­­­­oport

Software Engineering Fundamentals PROG1350

# Mars Climate Orbiter – Sept 23, 1999

1. NASA wanted to send a probe to mars to collect data on the atmosphere and act as a relay helping the next lander “Mar Polar Lander” transmit data back to earth. Lockheed was contracted by NASA to build the probe and NASA was to get it to mars.
2. When the probe approached mars’ orbit, the probe got to close mars and was destroyed by the atmospheric resistance.
3. The cause of this incorrect trajectory was that Lockheed used the improper units when building the unit and that caused wrong numbers to be used when calculating the trajectory. The contract between NASA and Lockheed specified the units as newton-seconds and Lockheed used pound-seconds.
4. If Lockheed would have used the units of measurement specified in the requirements contract the orbiter wouldn’t have crashed.
5. This was not caused by a requirement being changed. The unit of measurement was defined in the requirements and did not change.
6. The mars climate orbiter did crash because it was rushed. The testing had been cut down to much less than it should have been to meet time constraints. If there was more testing done, there is a good chance that the mistake would have been caught.
7. The difference in units that caused the crash should have been caught in testing but was not. The testing phase was much shorter that in was supposed to be and this led to the mistake being missed.
8. There was no documented warning that this could have been an issue in this project.
9. Software played a role by not catching the mismatched units.
10. <http://en.wikipedia.org/wiki/Mars_Climate_Orbiter>

Douglas Isbell, (Sept 30, 1999) *MARS CLIMATE ORBITER TEAM FINDS LIKELY CAUSE OF LOSS*. Retrieved Nov. 1, 2014 from: <http://mars.jpl.nasa.gov/msp98/news/mco990930.html>

NASA, *Mars Climate Orbiter Mission Overview*. Retrieved Nov. 1, 2014 from: <http://mars.jpl.nasa.gov/msp98/orbiter/mission.html>

James Oberg, (Dec 1, 1999). *Why the Mars Probe went off course*. Retrieved Nov. 1, 2014 from:

<http://spectrum.ieee.org/aerospace/robotic-exploration/why-the-mars-probe-went-off-course>

# Therac-25 1985 to 1987

1. Atomic Energy Commissions Limited (AECL) was working on a new linear accelerators designed to radiate patients for medical purposes. All previous models of the machine where primarily hardware base and only used software as a convenient add on. All of the previous versions had hardware locks that would prevent over radiation of the patient. In the new Therac-25 was designed to rely on software and they had removed the hardware safeties to save money and relied only on the software to prevent any problems.
2. The Therac-25 was giving some patients a lethal dose of radiation.
3. If an operator provided manual input at the same time as a counter overflowed, then the interlock that stopped the system from harming the patient would not work and could give the patient with 100 times the intended dose.
4. The problem could have been avoided if the code that was written was modular and able to be properly tested. This would be done by following proper coding standards. The system (machine and software) needed to be test together before implementation. The software needed to go through a larger testing regiment.
5. I do not think this was caused by a requirement being changed. The system programing had bugs and didn’t have to do with the requirements.
6. There are no signs that the system was rushed. The system was just poorly designed and tested.
7. This problem should have been caught during testing but the system was never properly tested. When safety test where done, the software was excluded because it was assumed it was tested already and would not fail. The software was never tested with the therac-25 and was never tested by anyone not working closely on the program.
8. Nobody pre-warned that this could happen. When it happened everyone assumed the allegations where false because it was assumed that it couldn’t happen.
9. The software plaid the main role in the disaster. The software was not designed properly, and wasn’t tested properly. The software let conditions happed where the machine would admit doses of radiation far greater than what was acceptable. The program would often give a malfunction error with no detail as to what the error was or how to proceed and allow the operator to resume administering the radiation with a single key stroke.
10. <http://en.wikipedia.org/wiki/Therac-25>

Nancy Leveson, (July 7, 1993). *An Investigation of the Therac-25 Accidents*. Retrieved Nov. 2, 2014 from: <http://courses.cs.vt.edu/professionalism/Therac_25/Therac_1.html>

# The Mile Island March 28, 1979

1. Three Mile Island is a Nuclear Generating Station. On March 28, 1979 one of the two reactors was down for refuelling and the remaining reactor (TMI-2) was running at 97% capacity.
2. The reactors cooling system and back-up failed and then a pressure release valve allowed for far too much coolant to escape causing the reactor to overheat and partially melt down.
3. During a routine cleaning of a filter, the operator accidently forces some cleaning product into an instrument airline. This caused the cooling systems for TMI-2 to stop functioning properly and the plant to perform an emergency shutdown. The valves for the axillary cooling pumps had been closed for maintenance causing the axillary cooling pumps to not work and this led to no way of cooling the system. This caused pressure to start building in the primary cooling system but when the pressure got to high an automatic pressure release valve opened to release pressure. This valve should have closed when the pressure dropped but it got stuck open allowing for coolant to keep emptying after it should have been stopped causing the reactor to overheat and partially melt down. No one noticed the pressure release valve was stuck open because the indicator light only indicated if the valve had been told to close, not if it was actually closed.
4. There are a number of things that should have been done to prevent this disaster. The safety protocols should have been followed in that the reactor is shutdown if the auxiliary cooling system is offline. The personal should have been taught the indicator was an indication of the intended state of the valve, not the true state of the valve and how to check the true state of the valve using the temperature gauge. Lastly the indicator light should have indicated the actual valve position not the intended position.
5. This may have occurred because requirements where changed inappropriately. The requirements may have originally required the indicator light to display the true position of the valve but then been changed later to save time or cost.
6. This may have happened because the project was rushed. The system may have originally been designed to monitor the actual position of the valve but was changed later to save time.
7. The issue that the light indicated intended position instead of actual position was known to well train employees.
8. I have not found any repots of anyone specifically waning that this light could cause a meltdown but this was a known issue.
9. The led not properly indicating the position of the valve changed the insistent form an emergency to a partial meltdown. If the indicator showed that the valve was stuck open then the problem could have been fixed and coolant could have been saved, possibly stopping the meltdown.
10. <http://en.wikipedia.org/wiki/Three_Mile_Island_accident>

World Nuclear Association, (March 2001). *Three Mile Island Accident*. Retrieved Nov. 3, 2014 from: <http://www.world-nuclear.org/info/safety-and-security/safety-of-plants/three-mile-island-accident/>

# Ariane 501 June 4 1996

1. Ariane 501 was a rocket designed to deliver an unmanned payload to low earth orbit. The rocket was largely based off of its predecessor the Ariane 4. The Ariane 5 used much of the same software and hardware with some key differences. On June 4th, 1996 the first Ariane 5 (Ariane 501) was set to deliver scientific equipment to low earth orbit.
2. Shortly after takeoff (39 seconds) the autopilot aboard the rocket turned the engines hard right and turned the rocket horizontal to the flight path. The air resistance ripped the rocket apart and it the proceeded to auto destruct.
3. The cause of the problem was that the telemetry sensor used to find the rockets angle gave the system a 64 bit number but the system used a 16 bit number. The vibrations during the takeoff caused the telemetry unit to give the software a number larger than it could handle and overflow the data. The system then used this bad data to find its current angle and found that it was 90⁰ off course and proceeded to turn violently.
4. To prevent the problem the data from the telemetry unit should have been properly dealt with and not be allowed to overflow the data type.
5. A large portion of the design come from the Ariane rocket so it may be assumed the requirement for Ariane 5 resemble the requirements for the Ariane 4. The crash happened because a mismatch of data between the old hardware Ariane 4 and new Ariane 5 software so I think it is safe to say that changes in the requirements are partially to blame.
6. There is no evidence that the technology was rushed, it seems that some testing steps were missed though.
7. Yes, this bug should have been caught during testing. It was not caught because there was no test to simulate the takeoff condition for the telemetry sensors so the bad data was never fed into the software.
8. There was no warning on that an event like this may happen.
9. The software played the entire role in this disaster. It was a bug in the software that caused the engines to turn as far as they could because the software thought the rocket was 90⁰ off course.
10. J. L. Lions, (July 19 1996). *ARIANE 5 Flight 501 Failure*. Retrieved Nov. 3, 2014 from: <https://www.ima.umn.edu/~arnold/disasters/ariane5rep.html>