Journal of Telematics and Informatics (JTI)
Vol.1, No.1, March 2013, pp. 20~25
ISSN: 2303-3703

A Domestic Case Studies Probability to Overcome Software Failures

Ch Suresh Kumar*, D Raghu, P Ratna Kumar***
* Departement of Computer Science and Engineering, Anurag Engineering College, Kodad
** Departement of Computer Science and Engineering, Paulraj Engineering College, Bhadrachalam
e-mail: sureshkumar@jadr.co.in, sureshkumar@jadr.co.in, ratnakumar@niam.res.in

Abstract

Computers are the pervasive technology of our time. As computer become critically tied to human life, it also becomes more important that interactions with them are under control. They are no longer a novelty, but are integrated into the fabric of our world, performing both high and low-level tasks. That is, computers may be used to eliminate heavy, redundant work and more. Sophisticated machines have been deployed to perform remote surgery or detect subterranean landmines in repopulated civilian areas. The increasing importance of computers in our lives means that it is essential that the design of computer systems incorporates techniques that can ensure reliability, safety and security. This paper will examine technological mishaps involving the use of computers. This review will include notorious software bugs that have affected finance, communication, transit, defense, health and medicine and others systems or industries. The sequence and etiology of these accidents will be discusses as well as how catastrophes may be avoided in the future through lessons and practices based on research.

1. Introduction

1.1 The Nature of Errors

Despite their obvious success, computer-related errors occur more frequently than necessary. To determine the best way to be avoided, one must identify the series of incidents that led to the "accident". There are several theories on the nature of errors that may occur in a system, defined as a set of human and non-human elements interacting to achieve a common goal. In a complex system, the cause may be harder to discern, for it may be impossible to identify discrete elements or map the relationships between elements of the set. Some theorists have suggested all errors are human errors and can manifest themselves in many forms [1]. They can be slips, because an action conducted is not what is intended, or they may be lapses, such as memory failures or omissions. Mistakes can involve errors in planning, although action may proceed as intended. The situation could have been inadequately assessed, and/or could have involved a lack of knowledge [1], [2].

Perrow uses the term "Normal Accident" to define a series of multiple failures of seemingly independent components that are tightly coupled de facto (dependent upon one another) but may not seem related [1]. Faults (failures) in a system may occur without meriting the term "accident." However, when multiple faults occur their accumulation is an accident.
Perrow goes on to state: "An accident is an event that involves damage to a defined system that disrupts the ongoing or future output of the system [1]." In complex systems the best (and most common) way to analyze a major accident is by careful reconstruction of the conditions and circumstances that led to the accident and can lead to "hindsight bias" that helps researchers to better understand the multiple factors which may have interacted and contributed to the accident [2].

Reason distinguishes between three kinds of human errors – active, latent and lack of blocks [2]. Active errors are the ones which are immediately discernible, while latent errors are much harder to detect, and may require considerable analysis to discover or understand and missing unpredictable blocks of code. "The car hit the lamppost" is an example of an active error. If the driver had been under the influence of alcohol, or was driving 15 miles over the speed limit, these would be related but latent errors and he is unable to predict exact accident or failure. The latent errors that were deemed to have caused the Challenger accident were traced back nine years, and in the case of the faulty pacemakers recalled by Guidant, the latent errors

Received October 28, 2012; Revised December 28, 2012; Accepted January 18, 2013

were traced back four years [3], [4]. The active errors (like the errors in security which occurred in the attacks of September 11th, 2001) draw our attention, but the actual long-term improvements in system design and safety will only occur after the detailed latent analysis which must follow. Solution should be tested with high priorities based on accidents.

1.2. Computers and Risk

Risk assessment can indicate existing or potential system vulnerabilities. However, it is important to note, hazards can never be completely eliminated from all systems. The failure to design safety-critical systems could lead to loss of life, destruction to the environment and may result in financial penalties when used over time.

The various sources and the effects can characterize the nature of computer-related risk [5]. Source of problems arising from software development includes: system conceptualization, requirements definition, system design and hardware and software implementation. Sources of problems in system operation and use are: natural disasters, animals, infrastructural factors, hardware malfunction and software misbehavior. Our increasing dependence on computational machines to perform both low and high-level tasks indicates that risk should be thoroughly identified and accommodated.

Errors associated with the failure to build a safety-critical system are manifested in a way consistent to their use. For example, if not safety-critical, computers used in health care can result in death, injury, misdiagnosis, incorrect billing and loss of privacy or personal information [6]. And in the defense industry, computers that are used for warfare could be associated with misidentification of adversary, failure to defend, accidental attack or accidental self-destruction [5].

1.3. Case Studies

In a complex system, a long history of latent errors may be ignored or undetected until a catastrophic event occurs [2]. We will discuss complex system failure by application, citing well-known software errors that have led to the dramatic loss of resources in the space, transportation, communication, government, and health care industries including:

1. NASA Mars Surveyor Program (1998 &1999)
2. Patriot Missile Defense System (1991)
3. Iran Air Flight 655 (1988)
4. AT&T Breakdown (1990)
5. Guidant Technologies ICDs (2005)
6. Therac-25 (1986)
7. Public In-convince

1.3.1 Space

1.3.1.1 NASA Mars Surveyor ’98 Program

The Mars Surveyor Program deployed two spacecrafts to study Martian climate and the subsurface environment, each launched separately. Lockheed Martin Astronautics was selected by NASA as the prime contractor for the project. Both crafts, the Mars Climate Orbiter, launched on December 11, 1998 and the Mars Polar Lander, launched January 3, 1999, were lost [7]. Both were launched at Cape Canaveral Air Station, USA, and carried instruments to map the surface of Mars and detect aspects of its environment, such as ice reservoirs of traces of water.

The Mars Climate Orbiter’s failed mission was attributed to a software error involving calculation. A report issued by NASA states the root cause was “failure to use metric units in the coding of a software file, “Small Forces,” used in trajectory models [8]. An investigation revealed that the navigation team was calculating metric units and the ground calculations were in Imperial units. The computer systems in the crafts were unable to reconcile the differences resulting in a navigation error.

The second craft was the Mars Polar Lander [9]. This spacecraft sent its last telemetry just prior to landing on the surface of Mars. The investigation report revealed that the most likely cause of failure was a software error that mistakenly identified the cause of a vibration as the touchdown when it was the deployment of the legs. This could have signaled the engines to cut-off 40 meters above the surface rather than on touchdown. An alternative theory suggests that it was the inadequate preheating of catalytic beds for the rocket thrusters. The remains of the spacecraft remain space.

1.3.2 Defense

1.3.2.1Patriot Missile Defense System (1991)

During the Gulf War, a software error was attributed to the death of 28 soldiers when the US Patriot Missile Defense System failed to intercept an incoming Scud missile that struck military barracks [10]. The “accident” was attributed to an error in calculation. The systems internal clock was measured in tenths of seconds and the actual time was reported by multiplying the internal clock’s value with a 24-bit fixed-point register. As a result, two systems intended to share a universal time, instead had independent system clocks.

1.3.2.2 Aegis Combat System, Iran Air Flight 655 (1988)

On July 3, 1988, the Aegis combat defense system, used by the U.S. Navy, was involved in an incident in which USS Vincennes mistakenly shot down Iran Air Flight 655 in 1988 resulting in 290 civilian fatalities [11]. The investigation inquired into all the events which occurred prior to, during, and immediately following the engagement of Track Number (TN) 4131, later identified as Iran Air Flight 655. Timelines became essential elements of the investigation, particularly as regards the short time period (minutes and seconds) in which the Commanding Officer was required to make his decision to fire. This time period is referred to as the “critical time period” throughout the report.

Using the missile guidance system, Vincennes's Commanding Officer believed the Iran Air Airbus A300B2 was a much smaller Iran Air Force F-14A Tomcat jet fighter descending on an attack vector, when in fact the Airbus was transporting civilians and on its normal civilian flight path. The radar system temporarily lost Flight 655 and reassigned its track number to a F-14A Tomcat fighter that it had previously seen. During the critical period, the decision to fire was made, and U.S. military personnel shot down the civilian plane.

1.3.2.3 Ariane 5, Flight 501 Failure

It took the European space Agency 10 years and $7 billion to produce Ariane 5, a giant rocket capable of hurling a pair of three-ton satellites into orbit with each launch and intended to give Europe overwhelming supremacy in the commercial space business. All it took to explode that rocket less than a minute into its maiden voyage last June, scattering fiery rubble across the mangrove swamps of French Guiana, was a small computer program trying to stuff a 64-bit number into a 16-bit space.

One bug, one crash. Of all the careless lines of code recorded in the annals of computer science this one may stand as the most devastatingly efficient. From interviews with rocketry experts and an analysis prepared for the space agency, a clear path from an arithmetic error to total destruction emerges.

1.3.3 Telecommunications

1.3.3.1 AT&T Breakdown (1990)

In January of 1990, unknown combinations of calls caused malfunctions across 114 switching center across the Unites States. This series of events resulted in 65 million calls unconnected nationwide. The company had a marketing campaign based on “reliability claims” of a “virtually foolproof system”. The cause was attributed to a sequence of events that triggered an existing software error.

The cause of the AT&T network failure was also a “fault in the code” [12]. The improvement that was made improved the way the company reacts to the series of events that resulted in the 1991 system failure and uses internal logic to monitor switch activity.

1.3.4 Health Care and Medicine

Many people around the world are harmed as a direct result of medical errors that can occur while receiving medical treatment. These can be made by the human expert, novice or introduced by the computer design. Medical errors are alarmingly common, costly, and often preventable [6], [13], [14]. The IOM report, To Err is Human, Building a Better Health System, increased public and political attention to the prevalence of medical errors in the Unites States. The IOM set a clear goal of a 50% reduction in medical errors over the next five years. Although the United States did not meet this benchmark, many policy makers believe this is achievable by automating informal processes and standardizing information for electronic exchange among

doctors' offices, hospitals, laboratories, patients, the government, and others. However, the adoption of health information technology has been a slow process with moderate success.

1.3.4.1Guidant's Implantable Cardioverter-Defibrillator (2005)

In 2005, after notifying the FDA, Guidant, a subsidiary of Boston Scientific, urgently recalled 26,000 defective ICDs [4]. Shortly after the FDA issued a Preliminary Public Health Notification and identified Guidant as the maker of three different models of pacemakers that the FDA report identifies as having a malfunction the "could lead to a serious, life-threatening event" [15].

Earlier that year, two physicians, Hauser and Maron, published an article a medical journal reporting the death of a 21-year old patient who had received a Prizm 2 DR model 1861 ICD pulse generator in 1991 [3]. While jogging with his girlfriend, the patient went into sudden cardiac arrest and could not be resuscitated. His ICD was returned to Guidant and they determined that the device failed during the delivery of a shock. This directly attributed to a short circuit that developed between a high-voltage wire and tube used to test the housing (casing) during manufacturing. At this point in time, Guidant was aware of 25 other device failure reports on this same model and manufacturing changes were made in 2002 to prevent short-circuiting. However, Guidant declined to inform patients or physicians and felt such a communication was inadvisable and unnecessary. The physicians, who felt it was their moral and ethical responsibility to disclose the device failure to the medical community and the public, took their concerns to the New York Times, triggering intense media attention and a wide-scale, highly publicized device recall [4], [16].

1.3.4.2 Canadian Cancer Therapy Machine (Therac-25, 1986) Designed by Atomic Energy of Canada, Ltd. (AECL)

Therac-25 was a software controlled radiation therapy machine used to treat people with cancer [17]. Between 1985 and 1987 Therac-25 machines in four medical centers gave massive overdoses of radiation to six patients. An extensive investigation and report revealed that is some instances operators repeated overdoses because machine display indicated no dose given. Some patients received between 13,000 - 25,000 rads when 100-200 needed. The result of the excessive radiation exposure resulted in severe injuries and three patients' deaths.

Causes of the errors were attributed to lapses in good safety design. Specific examples are cite failure to use safety precautions present in earlier versions, insufficient testing, and that one key resumption was possible despite an error message. The investigation also found calculation errors. For example, the set-up test used a one byte flag variable whose bit value was incremented on each run. When the routine called for the 256^{th} time, there was a flag overflow and huge electron beam was erroneously turned on.

An extensive investigation showed that although some latent error could be traced back for several years, there was an inadequate system of reporting and investigating accidents that made it hard to determine the root cause. The final investigations report indicates that during real-time operation the software recorded only certain parts of operator input/editing. In addition, the radiation machine required careful reconstruction by a physicist at one of the cancer centers in order to determine what went wrong [18].

1.4 Public In-Convince

1.4.1 Student Loan Service

In August of 2006 a U.S government student loan service erroneously made public the personal data of as many as 21,000 borrowers on its web site, due to a software error. The bug was fixed and the government department subsequently offered to arrange for free credit monitoring service for those affected.

1.4.2 Metro Rail Accident

A software problem contributed to a rail car fire in a major underground metro system in April of 2007 according to newspaper accounts. The software reportedly failed to perform as expected in detecting and preventing excess power usage in equipment on a new passenger rail car, and evacuation and shut down of part of the system.

Failure of computers is not breaking news today; however the study of these projects reveals new factors for analysis.

2. Research

We came from an engineering background and know that even within tech companies, there are lots of screwed up projects run by managers who don't fully understand the intricacies of software development. Based on these experiences, I've come up with a list of things one should understand before agreeing to go ahead with a software projects.

1. Hire a Component Software Project Manager or consulting firm.
2. Hire Quality Developers/Testers/etc.,
3. Adopt an Iterative Development Process.
4. Adopt a Modeling Design technique.
5. Good Communication needs to be built into the process and culture.
6. Organize the Project Around small, semi-Autonomous Teams.
7. Ensure there is Accountability at all a level.
8. Periodically Review and tweak the process.
9. Postmortem success or failures.
10. Preserve volumes for future use.

Safety-Critical Practices

As opposed to concentrating on errors, other researchers have focused on what makes certain industries such as military aircraft carriers or chemical processing highly reliable [19]. Their findings emphasize that accidents can be prevented through good organizational design and management [20]. Success factors include a high organizational commitment to safety, high levels of redundancy in personnel and safety measures, and a strong organizational culture for continuous learning and willingness to change [20].

Research suggests failure to design safety-critical systems can be attributed to a mismatch between a technological system and a human operator, manifested at the "syntactic" and "semantic" levels. A knowledge representation can be syntactically correctable, but if its semantic structure is wrong, then no amount of human technology can correct it [21].There is a common misconception that increasing reliability will increase safety.

Many software-related accidents have occurred despite the software being compliant with the requirements specification. Semantic mismatch is characterized by errors that can be traced to errors in the requirements – what the computer should do is not necessarily consistent with safety and reliability [18].

Here are the main issues for further consideration:

We have inscrutable software.

- Who is writing the software and should they be certified?
- Who is responsible?
- Well-designed Human Interfaces are needed.
- Consider Modeling Concepts which reduces complexity.
- Human factors are critical - In many complex systems human factors are critical to whether the system will operate, be understood in adverse conditions, and how preventative measures may be taken.
- Redundancy and self-Checking, and testing are needed.

3. Conclusion

The analysis of case studies pertaining to common and severe failures depicts that a software failure at any stage could lead to the loss of lives, financial losses, wastage of time, effort and other intangible losses like discomfort, stress, good will, reputation, confidence, peace etc. In current information age the application of software has penetrated in each and every industry unlike traditional approach where software was altogether a separate entity. As software has become integral part of every product and process so there is a need to make a full proof system so that the software failures could be avoided. There is further requirement of root cause analysis of these software failures to understand the problematic area and suggest the areas of improvement in the current process as several corrective & preventive actions needs to be taken while developing products and software systems.

Already a threshold point started for the failures of software and let us all try to enhance our future software for better society. Where we can keep our coming generations safe and acknowledge them about failures which can occur.

References

[1] Perrow Charles. *Normal Accidents: Living with High-Risk Technologies*. Basic Books, NY. 1984.
[2] Reason J. *Human Error*. Cambridge. Cambridge University Press. 1990.
[3] Gornick CC, Hauser RG, Almquist AK, Maron BJ. Unpredictable implantable cardioverter-defibrillator pulse generator failure due to electrical overstress causing sudden death in a young high-risk patient with hypertrophic cardiomyopathy. *Heart Rhythm.* 2005; 2(7): 681-3.
[4] Hauser RG, Maron BJ. Lessons from the failure and recall of an implantable cardioverter-defibrillator. *Circulation*. 2005 Sep 27; 112(13): 2040-2. Epub 2005 Sep 19.
[5] Neumann, Peter G. *Computer Related Risks*. New York: Addison Wesley. 1995.
[6] Kohn LT, Corrigan JM & Donaldsen MS (Eds.). *To Err is Human: Building a Safer Health System*. Washington D.C.: National Academies Press. 1999.
[7] Euler EE, Jolly SD, and Curtis HH. "The Failures of the Mars Climate Orbiter and Mars Polar Lander: A Perspective from the People Involved". *Proceedings of Guidance and Control 2001, American Astronautical Society*, paper AAS 01-074. 2001.
[8] NASA. Mars Climate Orbiter Mishap Investigation Board Phase I Report. November 10, 1999.
[9] Mars Polar Lander. NSSDC Master Catalog: Spacecraft. Retrieved on Feb 7, 2007.
[10] United States of America, General Accounting Office, Patriot missile defense: Software problem led to system failure at Dhahran, Saudi Arabia. Technical Report of the U.S. General Accounting Office, GAO/IMTEC-92-26, GAO, 1992.
[11] United States of America, Department of Defense, "Formal Investigation of the Circumstances Surrounding the Downing of Iran Air Flight 655 on 3 July, 1998", http://www.dod.mil/pubs/foi/reading_room/172.pdf
[12] Larry Seese, AT&T's director of technology development.
[13] Brennan TA, Leape LL & Laird N. (1996). Incidence of Adverse Events and Negligence in Hospitalized Patients. *New England Journal of Medicine*. 32(5), 5-28.
[14] Bates DW, Reducing the Frequency of Errors in Medicine using Information Technology, *Journal of the American Medical Informatics Association: JAMIA*. 2001; 8: 299-308.
[15] FDA Preliminary Public Health Notification*: Guidant VENTAK PRIZM® 2 DR and CONTAK RENEWAL® Implantable Cardioverter Defibrillators http://www.fda.gov/cdrh/safety/071405-guidant.html
[16] Meier B. (2005, May 25). Maker of Heart Device Kept Flaw from Doctors. N*w York Times on the Web* [Online]. Retrieved January 19, 2007, from http://query.nytimes.com/gst/fullpage.html?res=9803E4D71239F937A15756C0A9639C8B63&sec=health&spon=&pagewanted=print
[17] Leveson, Nancy G. SAFEWARE System safety and Computers: a Guide to Preventing Accidents and Loses Caused by Technology. Addison Wesley Publishing Company Inc. 1995.
[18] Leveson, Nancy G and Clark S Turner. 1992. "An Investigation of the Therac-25 Accidents". Technical Report #92-108. *Department of Information and Computer Science*, University of California, Irvine.
[19] Roberts K. Risk, Regulation, Litigation and Organizational Issues in Safety High-Hazard Industries. Position paper for *Workshop on Organizational Analysis in High Hazard Production Systems: An Academy/Industry Dialogue*, MIT Endicott House, NSF Grant No. 9510883-SBR. April 15-18, 1997.
[20] Sagan SD. *The Limits of Safety*. Princeton: Princeton University Press. 1993.
[21] Kopec D & Michie D. Mismatch between machine representations and human concepts: dangers and *remedies. Report to the EEC under subprogram FAST (Forecasting and Assessment in Science and Technology)*, Brussels, Belgium. 19.
[22] Reason J. *Human Error*. Cambridge. Cambridge University Press. 1990.
[23] Gornick CC, Hauser RG, Almquist AK, Maron BJ. Unpredictable implantable cardioverter-defibrillator pulse generator failure due to electrical overstress causing sudden death in a young high-risk patient with hypertrophic cardiomyopathy. *Heart Rhythm.* 2005; 2(7): 681-3.