INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

From Marvels to Disasters: Flaws in Requirements Engineering and Design

Sapna Grover
Assistant Professor, University of Delhi, India
Aditya Pancholi
Assistant Professor, University of Delhi, India

Abstract:
The notion of 'software engineering' was first proposed in 1968, defining best practices for software development, grounded in the application of engineering. Though, the key areas of software engineering process are identified as specification, development, validation and evolution by every process model, little attention is paid to specification and designing as compared to development, testing and maintenance. In this paper, we consider few case studies where negligence during requirements engineering and faulty design led to heavy causalities.

Key words: *Software engineering, Requirements engineering, Design flaws, Hindenburg fire disaster, Machhu dam-II disaster, Al Ayyat rail accident, Mississippi river bridge collapse, Assam ferry sinking*

1. Introduction

Software engineering is the process of developing and maintaining software systems. It involves a structured set of activities required to develop software. An in-depth study and analysis of mind-sets of end-users of the software and the surroundings where the software will be used, is needed to successfully accomplish the development task. For this, there are a large number of process development models which can be applied in development of different kinds of software.

Software process models represent an abstract series of steps that must be followed during the development process. These steps are described from a particular perspective and are therefore, abstract in nature. Software process models are broadly classified in two categories: Plan-driven and Agile. In plan-driven process, all the process activities are pre-planned and development progress is measured against this plan. The traditional waterfall model follows this approach. However, in agile process model [6,7], planning is incremental and it is easier to change the process to reflect changing customer requirements. In practice, a combined approach of these models is followed. Incremental model, Spiral model and RAD (Rapid application development) model are some of the models which follow this amalgamated approach.

In general, a software process model specifies four things in order: first, what is the system supposed to do; secondly, the structure of the system [3] and its implementation details; third, verifying the objective with which it was developed; and lastly, changing and adapting the system in response to the dynamic environment and needs of the customer. All these steps stipulate the activities of a process model.

One of the key aspects of development process is to determine what the software system is supposed to do. The process of identifying the services which a customer demands from a software system and the constraints under which the system will operate is called Requirements Engineering [2,4]. However, this part of development has always been considered the least significant in history. Much of the research work has been done on verification and validation process of a software system, and less on specification and analysis part. However, verification and validation is the last step in development process. Thus, systems suffer in terms of grade and quality.

Due to the above mentioned reasons, we carry out certain case studies in which we not only highlight the significance of requirements engineering but also suggest certain good and bad practices that must be followed during the development process. The presented case studies are analyzed from the point of view of flaw in development or design due to misinterpretation of requirements or imprecision and inconsistency in requirements statement. We, then, list out certain suggestions and improvements which must be carried out while developing the system.

The rest of the paper is organized as follows: Section 2 describes certain real life scenarios; section 3 analyses the reasons behind causalities happened due to faults in requirements engineering and design; section 4 presents the conclusion.

2. Case Studies

The ideas of software engineering not only apply to computer software but to every engineering field. In this section, we present few case studies where requirement and design flaws led to the loss of lives of many people. We also analyze them in the subsequent section.

2.1. Hindenburg disaster, 1937

LZ 129 Hindenburg, the lead ship of the two-ship Hindenburg class, was a large commercial passenger-carrying rigid airship, the longest class of flying machine and the largest airship by envelope volume, built in Germany during the time span 1931-36. The Hindenburg [15,16,17] was the first airliner to provide regularly scheduled services between Europe and North America. During the 1930s, airships like the Hindenburg class were widely considered the future of air travel. But the fire caught by the Hindenburg airship on May 6, 1937 during its second season of service bought an abrupt end to such expectations.

Of the 97 people (including passengers and crewmen) in the airship, 35 died (again including both), out of which 26 died in the fire only whereas others died while jumping from the airship at an excessive height, or as a consequence of smoke inhalation or burns a few hours later.

2.2. Machhu dam failure, 1979

Morbi, an industrial city in Gujarat, is situated on the 130 km long north-flowing Machhu river, (whose origin is Madla hills) 22 miles (35 kilometres) from the Arabian Sea and 60 kilometres from Rajkot. The Beti, Asoi, Machhori and Maha, the four important tributaries, together account for nearly 42.52% of the total catchment area of Machhu.

Machhu Dam, the water source for the city, was built under the Machhu River in August 1972, for people of Morbi. Machhu Dam-I is located on the river Machhu near Jalsika village and Machhu Dam-II is placed near village Jodhpur in Morbi taluka of Rajkot District. Machhu Dam is an awesome and one of the most famous place in Gujarat.

On August 11, 1979, the earthen walls of the four-kilometer long Machhu Dam-II [9,10,11,12,13,14] had disintegrated, sending a wall of water through the town of Morbi in the Rajkot district of Gujarat. The incident occurred because of the 10-day long excessive rains. According to the estimates, the number of people killed varied, greatly ranging from 1800 to 25000 people, which led to a place for this incident in Guinness Book of Records.

2.3. Al Ayyat railway accident, 2002

In Egypt's' Al Ayyat [18,19,20], many people were returning home to their villages via a passenger train of eleven carriages, travelling from Cairo to Luxor, to celebrate the Eid-al-Adha, the largest Muslim festival of the year marking the annual pilgrimage, or Hajj, to Mecca in Saudi Arabia. However, in the fifth carriage, a cooking gas cylinder exploded at around 02:00 in the morning of February 20, 2002 and created a fire which spread as the train ran. Seven of its carriages, all third class, were burnt almost to cinders. More than 370 people, all Egyptians, were killed in this worst ever rail disaster of Egypt.

2.4. Mississippi River Bridge Disaster, 2007

Bridge 9340, official name of the Mississippi River Bridge [21,22,23,24], is built on one of the chief river of North America, Mississippi river. The eight-lane, more than one thousand feet long steel truss-arch bridge was constructed in 1964 and inaugurated for use in November 1967. The bridge was Minnesota's fifth busiest bridge and a part of Interstate 35W (I-35W) Highway in the Minnesota state of U.S, passing through downtown Minneapolis.

During the evening rush hour on August 1, 2007, the bridge experienced a catastrophic failure in the main span of the deck truss and suddenly collapsed, with about 456 feet of the main span falling 108 feet into the 15-foot-deep river. A total of 111 vehicles were on the portion of the bridge that collapsed. Of these, 17 were recovered from the water. As a result of the bridge collapse, 13 people died, and 145 people were injured.

2.5. Assam Ferry Sinking, 2012

A land of plains and river valleys, Assam, has three principal physical regions out of which the Brahmaputra River valley in north is the largest. Annual monsoon in Assam, which arrives in June, stays through September, is not only the highest in the country but also ranks among the highest in the world; it often causes widespread and destructive flooding. Boats are a common mode of transport in such an area, which is dotted with small islands and villages along the banks of the Brahmaputra River.

A ferry [25,26,27] carrying approximately 350 passengers capsized in the Brahmaputra River in Assam state of Northeast India on April 30, 2012. The ferry was touring from Dhubri, some 300 kilometers from Guwahati, to Fakirganj. According to the reports, the incident happened because the ferry was caught in a storm and thereby, it overturned into the river. The disaster killed at least 100 people and over 100 went missing.

3. Requirements Engineering and Design: Critical Flaws

In this section, we analyze the case studies described above in order to identify the flaws in requirements engineering and design.

3.1. Flaws in Hindenburg airship

The biggest, fastest and highest capability, Hindenburg airship was named after the German president of 1925. It was build to provide world class air travel services between Europe and North America. However, many issues were not addressed during the requirement engineering and design phase of Hindenburg.

The airships' designers had decided to fill it with helium gas instead of hydrogen. Helium, unlike hydrogen, does not burn, making the travel safer. However, it did not elevate as much as hydrogen, so the extra volume Hindenburg had for gas was a crucial attribute. But Hindenburg was never filled with helium because it was tough to produce and U.S had a monopoly in its manufacture. The officials decided to purchase the required amount of gas but Americans did not gave it because they feared Hitler, in Germany, would use the gas for military purposes. Thus, the Zeppelin Company, Manufacturer of Hindenburg, was forced to redesign the ship for hydrogen and make changes to minimize the possibility of fire.

During its travel on May 6, 1937, when Hindenburg arrived USA, the weather was worrisome. Strong winds were accompanied by heavy rains and frequent lightning. Rain water tended to cling more to the rear end of the ship than the front, making it heavier. Thus, the airship was losing trim and the tail section was dropping. Also, the wind was constantly changing direction, so the captain was forced to make sharp "S" turns in order to land. The final turns taken in order to land were too sharp and they caused a support wire to snap inside the ship tearing open one of the hydrogen gas cells.

One of the other design flaws that contributed to the disaster was the doping solution used to stretch and waterproof the hull. It was made from a layer of iron oxide covered with coats of cellulose butyrate acetate mixed with powdered aluminium; the compound is very similar to a mixture used to power solid fuel rockets. This solution ignited Hindenburg within seconds. In short, the Hindenburg was literally painted with rocket fuel.

3.2. Reasons behind Machhu dam failure

Machcohhu River originates from Madla hills (Jasdan) and meets in little Rann of Kuchchh. Its length is 130 km. & 2515 sq.km. catchment area. Jamburee, Benia, Machchhori, Maha are right bank tributaries of river Machchhu. Betti and Asoi are left bank tributaries of Machhu River. The Machhu Dam-II near the city of Morbi, India, burst on August 11, 1979 allowing the Machhu River to flood the city. The flood took lives of thousands of people.

Officials claim that the dam failure was an “act of God” but we highlight the structural and communicational failures that resulted in such a huge disaster. Firstly, the geographical location of Machhu Dam-II is just 4 miles above the Morbi city. Construction of a huge dam, just few miles from the city was the biggest error, putting the lives of thousands of people on sake. Exactly, the same happened on 11th August 1979, when water of the rain-weakened dam came crushing, sweeping and obliterating dozens of villages and the city of Morbi. The water reached the city within minutes giving no time to cope up with this sudden disaster.

Second major cause was the ignorance and negligence of the management. Due to constant rains, all rivers in Saurashtra were flowing way over the danger mark. The spillway capacity of Machhu Dam-II was provided for 5663 m^3/s. The actual observed flow following the intense rainfall reached 16,307 m^3/s, thrice of what the dam was designed for. Despite of all these, no action was taken by the government officials to release the water to prevent the dam from collapsing. Apart from serious design flaws, there was little or no training given to the officials to deal with such situation.

3.3. Faults in Al Ayyat railway accident

The Egyptian railway system is by far the second oldest railway services in the world and the oldest railway network in Africa and the Middle East. Cairo, the capital of Egypt and the headquarters city of Egyptian rail transport services, has a number of trains originating from it and travelling to different parts of the country. One such passenger train, Al Ayyat, was heading towards Luxor and had eleven carriages. Fire began in a small cooking stove in its fifth carriage. It tore through the end of the train due to a number of design flaws.

When the fire broke out, the electricity failed, leaving many passengers struggling to escape in darkness. According to the reports, each carriage was packed with at least double the maximum carrying capacity of 150, making it further more difficult to escape in the presence of bars over the windows. Also, there was no means of communication between the driver and the rear carriages, and thus, the passengers could not inform the driver about the fire until about two hours after the fire had begun, because of which, so many people who attempted to flee from the overcrowded carriages were killed when they tried to jump. Besides this, the people who were rescued told that there were no emergency brakes in the train, which they could utilize. Fire extinguishers were also far less in number as compared to the quantity required. And, the available extinguishers were so far beyond their reach that they could not access them.

3.4. Mississippi River Bridge Disaster and causes

The Mississippi River, the chief river of the largest drainage system of North America, rises in northern Minnesota and curves slowly southwards to the delta at the Gulf of Mexico. However, the 1000 feet long bridge collapsed into the river at about 06:00p.m. on August 1, 2007.

The National Transportation Safety Board (NTSB), which was given the responsibility of investigating the possible causes behind such a malady, announced that the steel gusset plates used in the bridge's design were undersized (0.5 inches or 13 mm thick) and inadequate to support the intended capacity of the bridge; a load which had increased over time. Also, 2 inches (51 mm) of concrete was added to the road surface over the years, increasing the dead load by 20%. During the wreckage recovery, investigators discovered that the gusset plates at eight different junctures in the primary middle span were corroded. The NTSB also concluded that

the inspectors, who were supposed to review the bridges' functioning at regular basis, did not routinely check the status of safety features.

3.5. Causes behind Assam ferry sinking

Brahmaputra, one of the most powerful rivers in the world, enters India in Arunachal Pradesh and slows down to the plains of Assam. The average width of Brahmaputra in Assam is close to 10 kms which is the widest in the world. Because of the excessive flow and enormous width, only four bridges exist on the river over a long stretch of 1000 kms in India. Due to the unavailability of bridges, ferry is the most widely means of transport across this mighty river.

In such a situation, meeting safety and security standards while travelling such long distances across river is a must. However, there were a number of loopholes in the ferry configured for transport on April 30, 2012. According to the officials, the boat was overloaded with people, far more than its capacity of 280 people. It reported that the ferry was so overcrowded that people were seen sitting on the roof. Besides, the cargo of the ferry was also excessively overloaded with goods. Also, the boat had neither lifeboat nor life jackets, making another big safety measure a miss.

4. Conclusion

In this paper, we have studied and analyzed certain real life cases where small engineering and design flaws resulted in loss of property and many innocent lives. It can be easily concluded that the principles of software engineering apply not only in developing software, but to other engineering fields also. And, if these principles are not followed, they might lead to catastrophic failures. Hence, the principles of requirements engineering and design should not be neglected, as proper foundation leads to efficient development and maintenance of any software or real life projects.

5. References

1. Pandey D, Suman U, Ramani A.K. A Framework for Modelling Software Requirements. International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011.
2. Aranda J., Easterbrook S., Wilson G. Requirements in the wild: How small companies do it. 15th IEEE International Requirements Engineering Conference (RE 2007), 39-48.
3. Curtis B., Krasner H., Iscoe N. A field study of the software design process for large systems. Communications of the ACM, 31(11):1268–1287, 1988.
4. Cheng B.H.C., Atlee J.M. Research Directions in Requirements Engineering. Future of Software Engineering(FOSE 2007), IEEE Computer Society.
5. Cheng B.H.C, Lemos R., Giese H., Inverardi P., Magee L. Software Engineering for Self-Adaptive Systems: A Research Roadmap. LNCS 5525, 1–26, 2009.
6. Paetsch F., Eberlein A., Maurer F. Requirements Engineering and Agile Software Development. Proceedings of the Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'03).
7. Schwaber K., Beedle M. Agile Software Development with Scrum. Prentice Hall, 2001.
8. Sommerville I. (2011). Software engineering. Addison-Wesley.
9. http://en.wikipedia.org/wiki/1979_Machchhu_dam_failure
10. www.indiawaterportal.org/articles/machhu-dam-disaster-1979-gujarat-discussion-book-tom-wooten-and-utpal-sandesara
11. http://www.nrigujarati.co.in/Topic/1555/1/machhu-dam-in-morbi-gujarat-history-details-photos.html
12. https://www.prometheusbooks.com/index.php?main_page=product_info&products_id=2053&zenid=frm78kova0c86071eh6udgp244
13. http://www.timeoutbengaluru.net/books/features/flood-plain
14. http://members.optusnet.com.au/~engineeringgeologist/page21.html
15. http://en.wikipedia.org/wiki/Hindenburg_disaster
16. http://www.unmuseum.org/hindenburg.htm
17. www.airships.net/hindenburg/disaster
18. http://en.wikipedia.org/wiki/2002_Al_Ayyat_railway_accident
19. https://www.wsws.org/en/articles/2002/02/egy-f22.html
20. http://www.nytimes.com/2002/02/20/international/20CND-TRAIN.html
21. http://en.wikipedia.org/wiki/I-35W_Mississippi_River_bridge
22. http://www.mprnews.org/story/2007/08/02/inspection
23. http://www.dot.state.mn.us/i35wbridge/
24. http://www.ntsb.gov/investigations/summary/har0803.htm
25. http://edition.cnn.com/2012/04/30/world/asia/india-ferry/
26. http://www.bbc.com/news/world-asia-india-17895377
27. http://popularlogistics.com/2012/05/ferry-sinks-in-assam-india/