

Defect Prevention Methods

Traci Kanzawa
Thomas Ko
Matt Moon

Defect Prevention Methods

- **Introduction**
 - Definition of Defect Prevention
 - Real-life software errors
 - ▣ Airbus A320
 - ▣ Therac-25
- **Defect Prevention Methods**
 - Quality Function Deployment
 - Cleanroom
 - Joint Application Design
 - Participatory Design
- **Conclusion**
 - Airbus 320 and Therac-25 revisited

Software Errors

- **fault:** an anomaly in the source code
- **failure:** an unexpected output according to what the user desired
- **error:** that part of the software system which is liable to lead to failure

Definition of Defect Prevention

- **def:** "...an activity of continuous institutionalized learning during which common causes of errors in work products are systematically identified and process changes eliminating those causes are made."
[Eickelmann]

Effects of Software Errors

- unreasonable added cost
- lost time and effort
- inconvenience and annoyance
- death

Real-Life Software Errors

- **Airbus A320**
 - January 20, 1992
 - Example: 4th crash since the plane's debut in 1987
- **Therac-25**
 - April 11, 1986
 - Example: 5th reported overdose between the 1985 and 1987

Airbus A320

- 87 died, 9 survived the crash in 1992
- A320 was designed to be entirely computer controlled
- The pilot had to enter the flight data into the computer with multiple entry displays that looked similar
- The similarities of the “flight-path-angle” and the “vertical-speed” displays confused the pilots
- The result was the plane ended up descending at 3300 feet per minute instead of 800 feet. (The plane was initially cruising at 5000 feet.)

Therac-25

- 6 reported accidents involving massive overdoses to patients
- out of the 6, 4 of them resulted in deaths
- The East Texas Cancer Center on April 11, 1986 is the 5th reported accident

East Cancer Texas Center

- a patient was scheduled to receive an electron treatment for a skin cancer on the side of his face
- “Malfunction 54” showed up on the machine when the technician attempted to treat the patient
- The patient developed a fever and a coma and died 3 weeks later due to radiation overdose of the brain

Could these incidences of software errors been prevented?

YES!

Defect Prevention Methods

- Quality Function Deployment
- Cleanroom
- Joint Application Design
- Participatory Design

Quality Function Deployment (QFD)

- Originated from Mitsubishi’s Kobe shipyards in the 1970’s.
- QFD is a requirements solicitation technique that solicits and defines critical customer requirements.

QFD Technique

- **Step 1:** Record the customer requirements for the software system.
- **Step 2:** Requirements statements are converted into technical and measurable statements.
- **Step 3:** Completion of a correlation matrix by the customer.
- **Step 4:** Develop the technical product specification priorities.

Benefits of QFD

- customer satisfaction
- the correlation matrix mathematically prioritizes the customer specifications

Cleanroom

- introduced by Harlan D. Mills in 1987
- Cleanroom is an engineering and managerial process with the goal to prevent the introduction of defects before the completion of the product.

Cleanroom Technique

- Step 1: Record the customer requirements for the software system.
- Step 2: Develop an implementation-free formal specification that clearly and correctly describes the desired system.
- Step 3: "Functional Verification"
- Step 4: Coding and Walkthroughs
- Step 5: Statistical Test Planning
- Step 6: Code execution

Benefits of Cleanroom

- high quality without the high price tag
- minimizes development cost
- utilizes development time more efficiently

Joint Application Design (JAD)

- developed by IBM Canada in the 1970's
- JAD has evolved from being a technique to gather the views of both the developers and users to a structure for how to run a meeting.

4 Building Blocks for a Well-Fun JAD Meeting

- Facilitation
- Agenda Structure
- Documentation
- Group Dynamics

Costs and Benefits of JAD

- increased software quality
- reduced costs
- reduced life cycle time
- However...
 - because JAD is structure-based, it does not fully encourage creativity.
 - Also, because a JAD meeting includes managerial workers, the non-managerial workers might be less likely to participate.

Participatory Design (PD)

- originated in Scandinavia in the 1980's during the Scandinavian workplace democratic movement
- PD is a movement to improve the quality of work life and the work place by studying and analyzing the social dimension of work.

The Three Tenets of PD:

- The goal is to improve the quality of work life.
- The orientation is collaborative.
- The process is iterative.

Costs and Benefits of PD

- a rapid and inexpensive process
- However...
 - it can be viewed as intrusive
 - Also, some may view the lack of structure of the PD approach as a downfall

Defect Prevention Methods with respect to Software Qualities

- Learnability
- Usability
- Expandability
- Verifiability

Airbus A320 and Therac-25 Revisited...

- Lessons learned are:
 - the importance of safe versus “user-friendly” operator interfaces
 - the importance of providing fail-safe designs

“No Silver Bullet”

- “Undoubtedly, the most efficient way to produce quality software is to prevent the injection of defects in the first place.” [Williams]
- However, Frederick P. Brooks, Jr. would argue otherwise...
- “There is no single development, in either technology or management technique, which by itself promotes even one order-of-magnitude improvement within a decade in productivity, in reliability, in simplicity.” [Brooks]

References

- Frederick P. Brooks, Jr. **The Mythical Man Month.** Published By: Addison Wesley Longman, Inc. 1995. Pages 178-203. 26 pages
- Eickelmann, N.S. **Empirical Studies to Identify Defect Prevention Opportunities Using Process Simulation Technologies.** Software Engineering Workshop, Proceedings. 26th Annual NASA Goddard. 2001. Pages 22-25
- Williams, L. **Instilling a Defect Prevention Philosophy.** Frontiers in Education Conference. 1998. Pages 1308-1312