Bachelor of Engineering in Information Technology

ITM301 Professional Practices in IT

Unit VI: Errors, failures and risk (computer Reliability Issues and Liability)

Mr. Yeshi Jamtsho
Lecturer

Overview

- What is Computer Reliability?
- Classification of Computer System Failure
- Categories of Computer Reliability
- Effects of Computer Errors & Examples
- Error Cases and Ethical Analysis
- Who is Responsible for Errors
- Reliability Enhancement: Software Quality

What is computer Reliability?

- Computer Reliability is how well the computer system performs its required functions that it has
  - been designed for, and
  - to do them without failure

- One of the important **non-functional requirements** of the Software/computer system

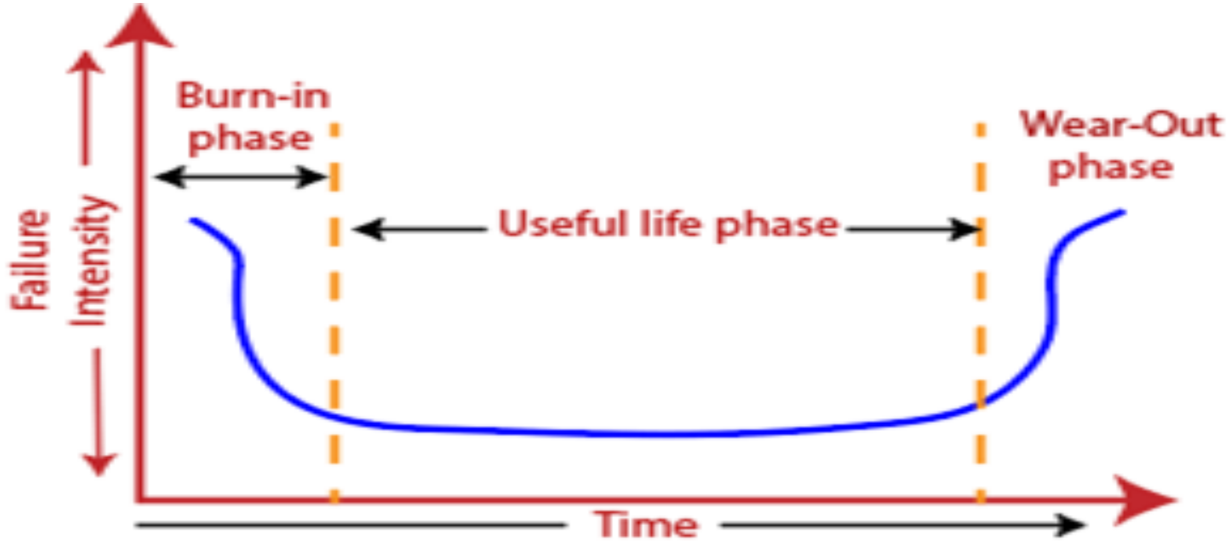
What is computer Reliability?

- Classification of Computer Failures:
  - Hardware Failures
  - Software Failures
  - Specification Failures
  - Malicious Failures
  - Human Errors

- Two main categories of Computer Reliability
  - ➢ Hardware Reliability
  - ➢ Software Reliability

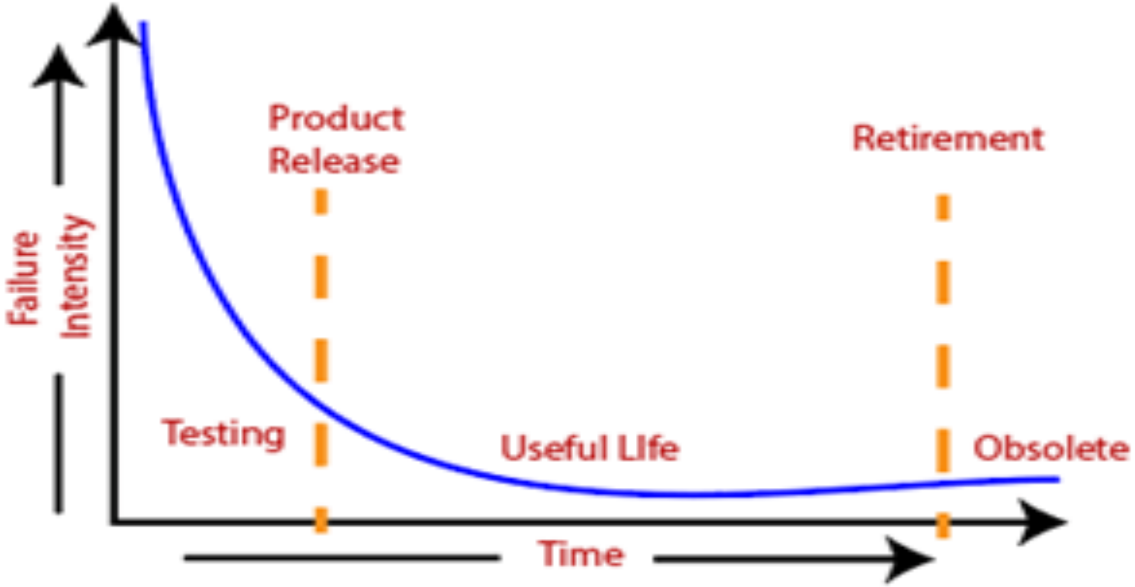
Hardware reliability

- Hardware Errors are mostly physical faults although design faults exist
- Hardware component fails are generally wear and tear.
- Hardware Product exhibits failure features as **Bathtub curve** (has 3 phases of life)



Software Reliability

- Software Errors are design faults, which are difficult to detect and correct
- Software fails due to some bugs



Human Errors in Computer Systems

- Besides software errors from design faults, there are some Human Errors while dealing with the computer system

  - Erroneous information in databases due to **Data Entry Error**

  - Misinterpretation of database information due to **Data Retrieval Error**

Human Errors in Computer Systems

- Computer databases track many of our activities

- What happens
  - ➢ When a computer is fed erroneous information?

  OR

  - ➢ When someone misinterprets the information retrieved from the computer database?

- What happens when a computer program contains a bug that leads the computer system malfunction?

Errors in Computer Systems

Effects of Computer Errors:

- Causes a real Inconvenience
- Poor/bad Business Decision and Financial loses
- Resulted in Fatalities

Example of Data Entry **or** Data Retrieval Errors

- **Example1**: Disenfranchised Voters:
- In the November 2000 general election, Florida in USA **disqualified thousands of voters**.
- ***Reason**:* People identified as felons. As results voters had been charged with misdemeanors and were forbidden from voting.
- ***Main Cause**:* Incorrect records in voter database.
- ***Consequence**:* May have affected election’s outcome

Example of Data Entry or Data Retrieval Errors

Example2: False Arrests in USA

Due to Record **Inaccuracy** in the databases of National Crime Information Center(NCIC):

- Ms. Sheila Jackson Stossier, Airline flight attendant mistaken for Ms. Shirley Jackson,
  - Arrested by Police at the New Orleans Airport and
  - Spent 1 night in jail and five days in detention

Example of Data Entry or Data Retrieval Errors

Example3: False Arrests in USA

Due to Record **Inaccuracy** in the databases of National Crime Information Center(NCIC):

- Roberto Hernandez mistaken for another Roberto Hernandez
- Both have same height, brown hairs & eyes, tattoos on the left arm, same birthday and also SSN# but differs by a single digit

  - California Police arrested him twice and spent 12 days in jail as a suspect in a Chicago Burglary case

Example of Data Entry or Data Retrieval Errors

- **Who should be responsible to ensure accuracy of such important information?**
- **Privacy Act of 1974**: “*Each agency … shall … maintain all records … with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individual in the determination*”
- Privacy Advocates:
  - Number of crime records is increasing (> 40 mil) in the NCLC databases
  - Accuracy of records is more important than ever
  - Government must fulfill its responsibility to ensure
    - No American citizen is being falsely arrested due to erroneous records are put into the databases.

Justice Depts's Position

- **Impractical** for FBI to be responsible for data's accuracy:
  - ➢ **Much information** provided by other law enforcement and intelligence agencies are **hard to verify**
  - ➢ If full accuracy is required, much less information would be in NCIC, making it less useful
- *In March 2003: Justice Dept. announces that*
  - FBI not responsible for accuracy of NCIC records;
  - Exempts NCIC from some provisions of the Privacy Act of 1974.

Examples of Software Errors

- **Example1:** In 1996 a Software error at the U.S Postal Service **resulted to returns 50,000 mail** (addressed to Patent and Trademark Office) to all senders.
- **Example2:** In 2001, A bug in the Billing Software of Qwest Company in U.S had **led to send incorrect bills** to 14,000 cell phone customers (i.e about 1.4 % of a total customers).
  - ✓ This bug caused to charge those customers more than $600 per minute for the use of their cell phones
  - ✓ One customer received a phone bills for $57,346.20 through email

Examples of Software Errors

Example3: In March 2003, a software error led it to post wrong price.

- Amazon.com in Britain offered **iPad for £7 instead of £275**;
  - ✓ Some customers ordered 10 iPad
  - ✓ Amazon.com shut down site,
  - ✓ refused to deliver unless customers paid true price (2003)
- ***Question:*** **Was Amazon wrong to refuse to fill the orders?**

Amazon Case Analysis

- ***Rule Utilitarian Analysis**:*

  - ***Proposed Rule**:*
    - A company must always honor the advertised price.
  - ***Cost/Harms**:*
    - Companies would spend more time proofreading advertisements materials, and may take out insurance policies
    - Higher costs for doing these tasks and thus lead to higher prices for all consumers
  - ***Benefits***:
    - Only few customers would benefit from errors
  - ***Conclusion**:*
    - Rule has more harms than benefits
    - Amazon.com did the right thing

Amazon Case Analysis (cont.)

- ***Kantian Analysis:*** *What is your view on buyer's action? Right or Wrong?*

- Buyers knew 97.5% mark-down was an error
- They attempted to take advantage of Amazon.com's stockholders
- They were not acting in "**good faith**"
- Buyers did something wrong

System Failure - Patriot Missile System

- Originally designed by U.S Army to shoot down airplanes.
- They used it to defend against Scud missiles launched at Israel and Saudi Arabia in 1991 Gulf War
- Most **significance failure** of this missile system was
  - one battery failed and never even shoot down any incoming Scud missile fired from Iraq
  - Scud hits US army place in Saudi Arabia and killed 28 soldiers

- ***Cause:***
  - Designed to operate only a few hours at a time
  - Kept in operation > 100 hours
  - Tiny truncation errors added up
  - Clock error of 0.3433 seconds → tracking error of 687 meters

Scud Missile
(wikipedia photo)

Patriot Antimissile Defense System
(wikipedia photo)

Summary of failure cause

- **Summary of Failure Cause of Patriot Missile System:**

- Equipment was not operated to its exact specifications.

- ***Was it Operator Error*** **or** ***Design Error*** ???

Other Notable System Failure Cases

- Therac-25 (1985-86)
- Airbus A320 (1988-92)
- AT&T long-distance network (1990)
- **Patriot missile (1991)-“Anti-Missile Defend System”**
- Denver international airport (1993)
- Ariane 5 (1996)
- Robot missions to Mars (1999)

Summary of Failure Causes in General for other cases

- ***Technical :***
  - Use of very new technology, with unknown reliability and problems
  - Reuse of software, without adapting to new conditions
  - Lack of clear, well thought out goals and specifications
  - Lack of thorough testing

- ***Managerial (Project Management)**:*
  - Poor management and poor communication among customers, designers, programmers
  - Pressures that encourage **unrealistically low bids** and **underestimates of time requirements**
  - Refusal to recognize or admit project problems

Who is Responsible for Failures?

- Software developers?
- Software vendors?
- System administrators

- ***Question:*** If you were a judge who had to assign responsibility in the particular case, how much responsibility would you assign to the

✓ programmers,

✓ manufacturer, and

✓ System Administrator (Army who operate the Missile machine)?

How to Improve Reliability?

- ***Difficulties:***
  - **Software complexity**
  - Software is only part of a system
  - Formal verification tools still immature
- ***Directions:***
  - Solid software engineering practice
  - Regulation on safety-critical applications
  - Professional licensing

Software Complexity

- ***Examples**:*
  - Linux kernel 2.6.0 – 6 million lines of code
  - Redhat Linux 7.1 – 30 million lines of code
  - Windows XP – 40 million lines of code
- ***In comparison (hardware):***
  - Boeing 747 – 3.5 million parts
  - Space shuttle – 10 million parts
- ***The main point:*** Formal Methodology is needed for software development
- **Note:** Software is Only a Part of the large & complex System

Software is Only a Part of the large & complex System

- ***Computer simulations***
  - *replace physical experiments in many fields:*
    - ✓ Experiment is too expensive/time-consuming
    - ✓ Experiment is **unethical**
    - ✓ Experiment is impossible
  - Can model past and current events, and predict the future

- ***However**, accuracy and reliability is only as good as the weakest link:*
  - ○ **Verification:** Does the model accurately represent the real system?
  - ○ **Validation**: Does program correctly implement the model?

Software Quality is still improving

Standish Group tracks IT projects in USA:

- Situation in 1994
  - 1/3 projects cancelled before completion
  - 1/2 projects had time and/or cost overruns
  - 1/6 projects completed on time on budget
- Situation in 2002
  - 1/6 projects cancelled
  - 1/2 projects had time and/or cost overruns
  - 1/3 projects completed on time on budget
- Situation in Bhutan ???

Software Warranties

- Many are "shrink-wrapped" – can't read software license clauses before purchasing.

- *Question: Are "shrink-wrapped" agreements legally enforceable?*

- Most say you accept software "as is". None will accept liability for harm caused by use of software.

- *Question: Can software manufacturers choose any warranty terms they want on their products?*

Scenario

A software vendor sell some buggy software. Later the bugs are fixed……………..and the fixes are incorporated into next version.

The new version is available, but to get it, the users must purchase it.

Is it ethical for the company to force users to purchase a new version in order to get their bugs fixed?

Consumer Protection Law

- Magnuson-Moss Warranty Act (1975) in USA:
  - Requires manufacturers/sellers to provide consumers with detailed information about warranty coverage.
  - It defines the rights of consumers and the obligations of warrantors under written warranties.

***Problem**:*

Only applicable to *full* warranties. Yet, no requirement on what type of warranty manufacturers use.

Uniform Computer Information Transactions Act (UCITA) for USA

- A proposed law to create a uniform set of rules to govern transactions in computer information (e.g. software licensing and online access).

- Under UCITA, software manufacturers can
  - License software
  - Prevent software transfer
  - Disclaim liability
  - Remote disable licensed software
  - Collect information about how software is used

- For more about UCITA, Ethical Issues and Software Contract Law: https://cs.stanford.edu/people/eroberts/cs201/projects/2000-01/ucita/index.html

Discussion Questions

- Have you been the victim of a software error?
    - Whom did you blame?
    - Now that you know more about the reliability of computer systems, do you still feel the same way?

- Assume you are in-charge of developing a software system that controls the traffic lights.
    - Its main purpose is to adjust the timing of the lights to improve traffic flow at rush hours.
    - List some technical requirements that you would put in the design for safety.

Discussion Questions

- Should software manufacturers be responsible for harmful consequences of defects of their products?

- Software companies sometimes release bug-fixes on their product to their customers free of charge. However, they often stop doing it when a new version of the product is released.
  - Do you think this practice is fair?

    Or
  - should companies keep fixing bugs in older versions?

Thank you