EECE 692

Practical Design of Safety-computer System
Author William R. Dunn

Chapter 3
How Computer Systems Fail

Present by *kidanmariam Fenta*
Sp*ring 2011*

How computer systems fail

3.1.1.Computer system failure and failure causes

Definition :

- Failure is defined as a failing to perform a duty or expected action.

How Computer System Fail

3.1.1computer system Failure and Failure causes

- Hardware
- Software
- systematic

Failure causes

- **Hardware faults**

➢ the inherent defects that are found in any manufacturer hardware item.

e.g. defects on physical item.

- **Software faults**

  ➢ The inherent defects that can reside in software as the result of software programming.

  e.g. defects on programing

- **Systematic faults**

Systematic Fault

- Personnel error : human action that leads to computer system failure.
- Environmental condition: system failure caused by temp, humidity,shock,vibration and electromagnetic interferance.
- Design adequacies
- Procedural deficiencies

3.1.2. Determining component Failure Mode

- Vendor data
- Facility records
- Publish database
- Technical literature
- Analysis
- Worst-case hypothesis

Component Failure Modes

- Vendor data-based on actual field history of a given component.
- Facility records-maintenance and operating records kept on past use of the system will include failure mode information on these latter components.
- Publish database-FMD-91.Failuremode/ Mechanism Distributions published in 1991 by the Reliability analysis center (RAC),Rome,NY
  - IEEE std 500in 1984

Component Failure Modes cont.

- Technical literature–conference and journal articles
- Analysis– sometimes FM data are not available but engineering analysis can yield some of the component's failure modes based on the failure modes of its parts.
- Worst–case hypothesis – component failure modes as obtained either from available data source or as determined from analysis.

3.2 Computer System Failure Modes and Effects

- Application failure
- Sensors failure
- Effectors
- Data communication link
- System power/interconnect
- Operator failure
- computer failure

3.2.2.Application Failure Modes

- The application under goes a failure resulting in an unplanned harmful release of energy or substance. e.g. collision, fire, and explosion.
- **End User**–is made up of people who will take possession of the system at the end of the development cycle. e.g. engineering, operator, maintenance etc.
- **Documentation** –operating logs, maintenance logs are often available and should be viewed by designers and analsis.
- **Formal safety analysis report**–formal reports detailing the hazards associated with the application.

3.2.3. Sensors Failure

- Sensor converts a physical stimulus into a corresponding electrical signal.
- Sensor failure effect- by them selves are usually quite harmless.
- Sensor failures can be dangerous when they can directly or indirectly influence operator action.

3.2.4 Effectors

- Effector converts an electrical signal into physical stimulus.
- Opposite to sensor.
- Effector failures can be dangerous and causes of mishaps.

3.2.5 Data Communication Link

- **Failures in data communication Link**
  - Failure of receipt of transmission of data.
  - Alteration of received or transmitted data.

3.2.6 System Power/Interconnect

Component	Failures mode
Electronic power supply	Incorrect voltage/no output
Hydraulic accumulator	Leaking. nonoperation. Stuck closed
Hydraulic pump	Leakage. Improper flow.no flow
Interconnect electrical	Open. Shorted. Intermittent
Interconnect pneumatic	Leak
Interconnect hydraulic	leak
Public utility power	No out put
Uninterruptable(backup) power supply	Fail transfer on demand

3.2.7 Operator Failure

- Operator failure can arise in the form of operator error or procedure inadequacies.
- The operator can fail to follow the procedures in a number of ways that includes:
  - Omitting of required actions
  - Performing of nonrequired actions
  - Failing to recognize needed action(s)
  - Responding poorly (too early, too late, incorrect)
  - Failing to communicate.

Monitoring Failures

- There are three types
  - **Perception failure**- (hear and see) an output
  - **Cognition failure** –perceiving and understanding it
  - **Decision failures**- decide to take appropriate action

Control Task Failures

- Control tasks involve operator actions that ultimately produce effector outputs and corresponding changes in the physical processes in the application.
- This also three types
  - **Activation of built-in command sequences**
    - Permanent part of the system cannot be changed by operator
  - **Operator-programmed** sequences-operator develop his own set of sequence offline to executed in real time.
  - **Closed-loop manual control**-the operator use an input device via computer move one or more effectors

How Computer Systems Fail

- **3.3.Computer hardware failure mode and effects**
  - **Digital integrated circuits-** pins, chips or wires
  - **Electronic support/interface components-** connector, clock and DC power etc.
  - **Memory and CPU**-fail to stored data, return valid stored data or instruction or both.
  - **CPU Failure** -can generate incorrect output

3.3.Computer hardware failure mode and effects

- **Sensor input modules**- A/D, Discrete/Digital and D/D converter
- **Effectors output** modules-A/D, Discrete/Digital and D/D converter
- **Operator input/output devices**-keyboard assembly, potentiometer ,switch and trackball.
- **Communication modules**-failing to transmit and/or receive data, transmitting data, and distorting data.
- **Peripheral units**- disk or tape driver, printers and event records ,etc.

How Computer Systems Fail

3.4 Software Faults and Failures

Definition :

- occurs when software does not produce a correct response given a set of inputs and internal states.
- a software faults Is a defect that resides in the software as a result of programming the software requirements.

Software Faults and Failure

- **Fault-free software and complexity**
  - The instruction don't fail. E.g microwave oven, VCR and modern automotive systems .
- **Software faults and failures and effects**
  - System software
  - Development software
  - Application software e.g computer virus
    - ❖Misinterpreted requirement-incorrect understanding of the requirment.
    - ❖Incorrect software design or implementation- using wrong variable, function , subroutine and finite loop . Etc.
    - ❖Clerical error- typographical error(.) use instead of comma(,)
  - the computer virus is an other form of people-related malicious that can produce software failures.

Design Faults and Failures

Design Faults and Failures–Basic System

- Design requirements and design faults
  - personnel error
  - Limited Engineering knowledge–
- Design Faults and Failures–Safety–Critical systems
  - Added Complexity– add requirement can make simple design.

Question ?