EECE 692

Practical Design of Safety-computer System

Author William R. Dunn

Chapter 6

Design of Fail-Operate computer System

Present by *kidanmariam Fenta*

Sp*ring 2011*

Design of Fail-Operate computer system

- A fail operate system is one that can tolerate one or more component failures and yet continue to operate or function.

Safety Requirements

Mishap

- Mishap can occur when control system is in hazardous operating region and it fails to operate.

Mishap Risk

- Mishap risk is the combined probability that the system is operating in that region and that it has failed to operate.

Design Overview

- Hardware and /or software must be able to first detect the existence of failures before the offending component can be isolated and system reconfigured to a safe, operable state.

Fail-Operate system Requirements

- Reliability –can be defined as the probability that an item will operate correctly for a specified continuous period of time and under specified conditions.
  - Unreliability (of the item) =1-reliability(of the item)
- Reparability- a commonly used term for describing the ease and speed which a failed system can be restored to its original condition.

Redundancy

- If a component failure can render the basic system in operable, it becomes necessary to add something to the system that will allow it to continue to operate in spite of failure.
  1. Operable backup system
  2. One or more redundant system

Component and system failure rate

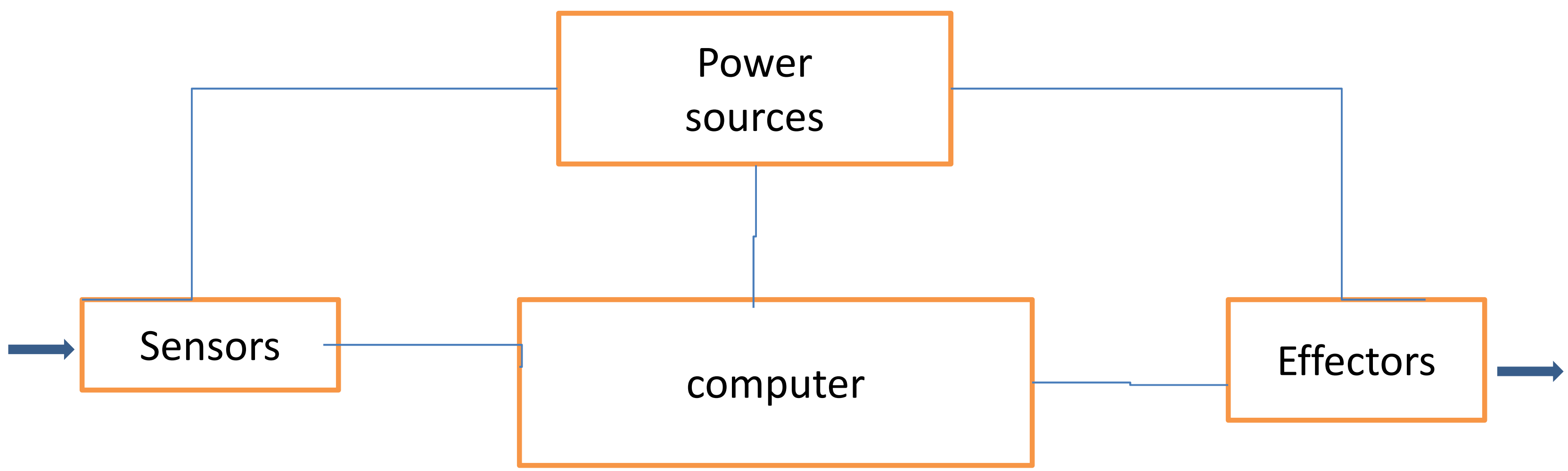
- **λ**= failure rate
- **Nsim** = simple system the sum of total number of failures , t= time
- Nsim /t = λsim
- **λsim**= λ + λ+ λ+ λ….. , λ k
- K components experienced n1,n2,n3…..,nk failures
- λsim= λs + λ E+ λ C+ λ I+λ P
- Where s= sensor, E= effector, c= computer ,I= interconnects, P= power sources.
- Critical failure rate
- If a component has total failure rate λcom, the failure rate concern is λ’com, where

λ‘comp= f x λcomp

and f is equal to the fraction of total failures that could make the simplex system inoperable.

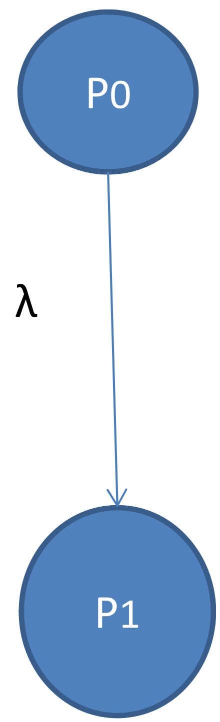
Simplex Computer System Architecture

•



Markov Model –simplex system –No Repair

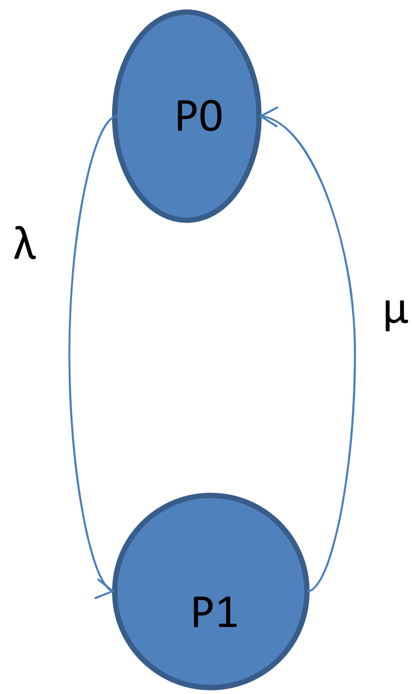
- Figure 6.2



- The simplex system can be only one of the two states, operating or not operating.
- Node P0 represent the probability that the system will be operating correctly; P1 is the probability that it will not.

Markov Model –simplex system with Repair

- Figure 6.4



- μ= repair rate
- λ= failure rate

Software Redundancy

- Backup software
- Dissimilar version of software or n-version programming

- disadvantage
  - multi-version programming is that operation on backup software development **cost** is much higher than that involved in developing primary and backup programs.

Fail-operate devices

mechanical

- Aircraft landing on an aircraft carrier increases the throttle to full power at touchdown. If the arresting wires fail to capture the plane, it is able to take off again.
- Elevator cabins have a safety mechanism that wedges securely onto the guide rails to arrest a fall if the hoist cables were to fail.

Electrical and electronics

- Many devices are protected from short circuit with fuses. The destruction of the fuse will prevent destruction of the device.
- Traffic light controllers use a *Conflict Monitor Unit* to detect faults or conflicting signals and switch an intersection to all flashing red, rather than displaying potentially dangerous conflicting signals, e.g. showing green in all directions
- The automatic protection of programs and/or processing systems when a computer hardware or software failure is detected in a computer system. A classic example is a watchdog timer.