EECE-692

Practical Design of Safety-computer System

Author William R. Dunn

Chapter 6-2

Design of Fail-Operate computer System

Present by *kidanmariam Fenta*

Sp*ring 2011*

Redundancy

- Definition :

  - Redundancy is the provision of two or more components or systems which are each capable of performing the same necessary function such that the **loss of any one** component or system **does not result** in the loss of the required function as a whole.

Redundancy

- Operating the same component or system in parallel
- Multiple input or output selected to operate
- Redundancy provides **protection against independent single failures** and **prevents a random independent failure** in one component or system from disabling the desired function.

Redundancy Management FDIR

- Redundancy management involves three distinct process
  1. Detection of failure when they occur
  2. Isolation of the failed element
  3. Reconfiguration of the system so that overall system operation will continue.

Dual Redundancy

- A brute –force approach to simply duplicate computer system.
- Computer A fails switch to Computer B.
- The operating computer A can be primary system and the computer B or second can be standby redundancy.

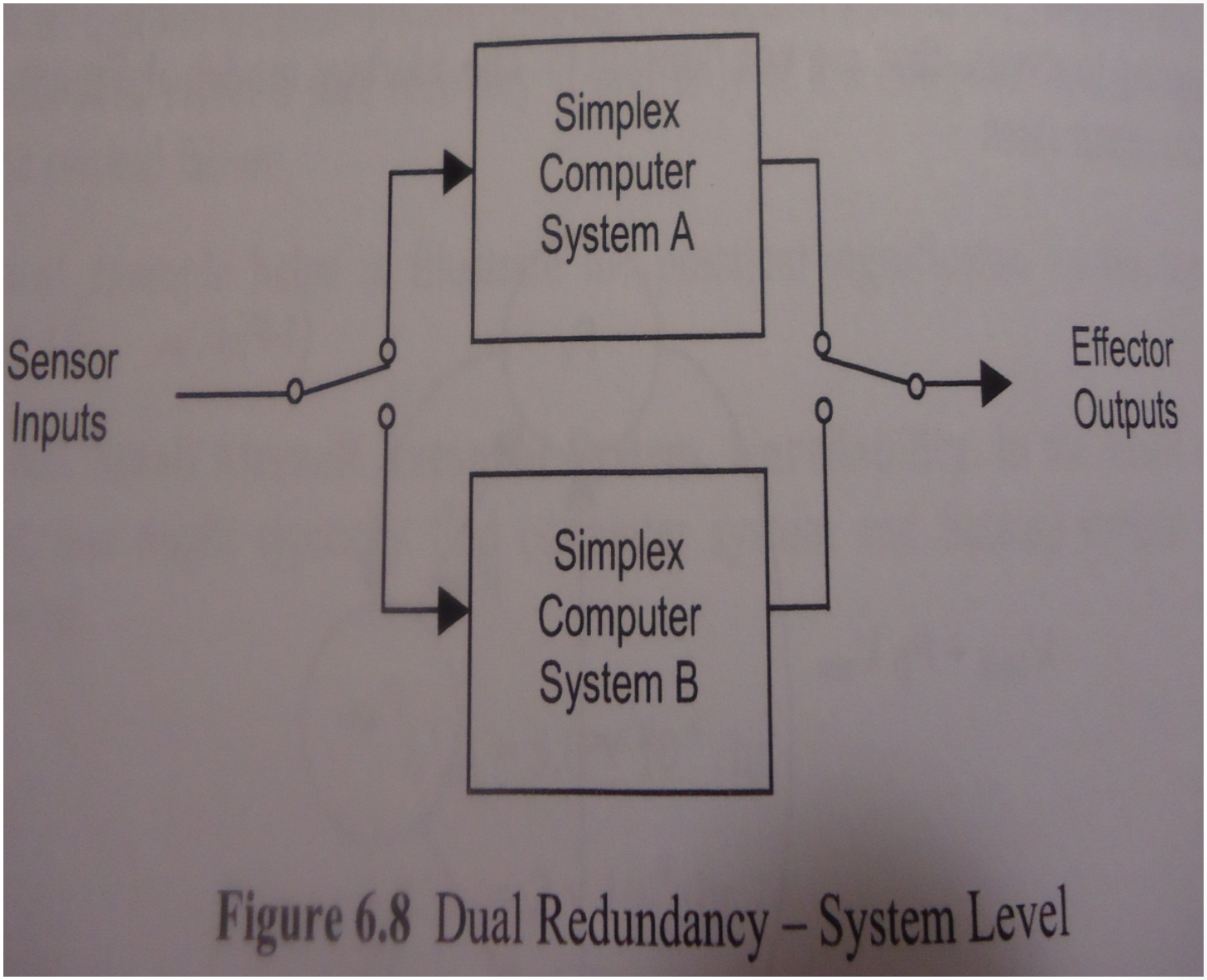


Figure 6.8 Dual Redundancy – System Level

Dual –Redundancy

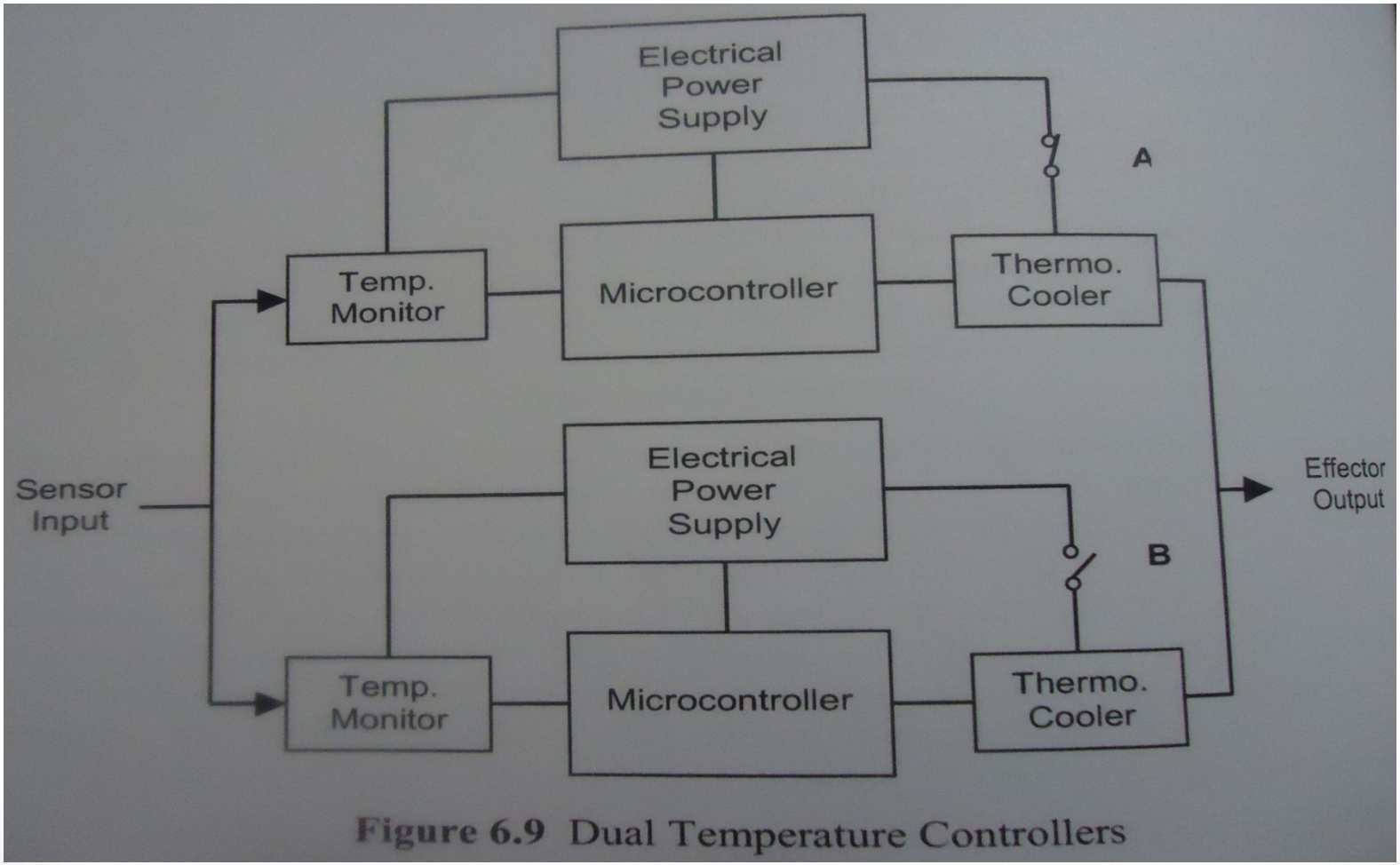


Figure 6.9 Dual Temperature Controllers

Dual Redundancy

Advantage

- The primary and the secondary (standby) computer system are physically separate, hardware failures in one system having no influence on the integrity of the other.

Disadvantage

- One way to improve the detection coverage is to allow the two computers to communicate with each other.

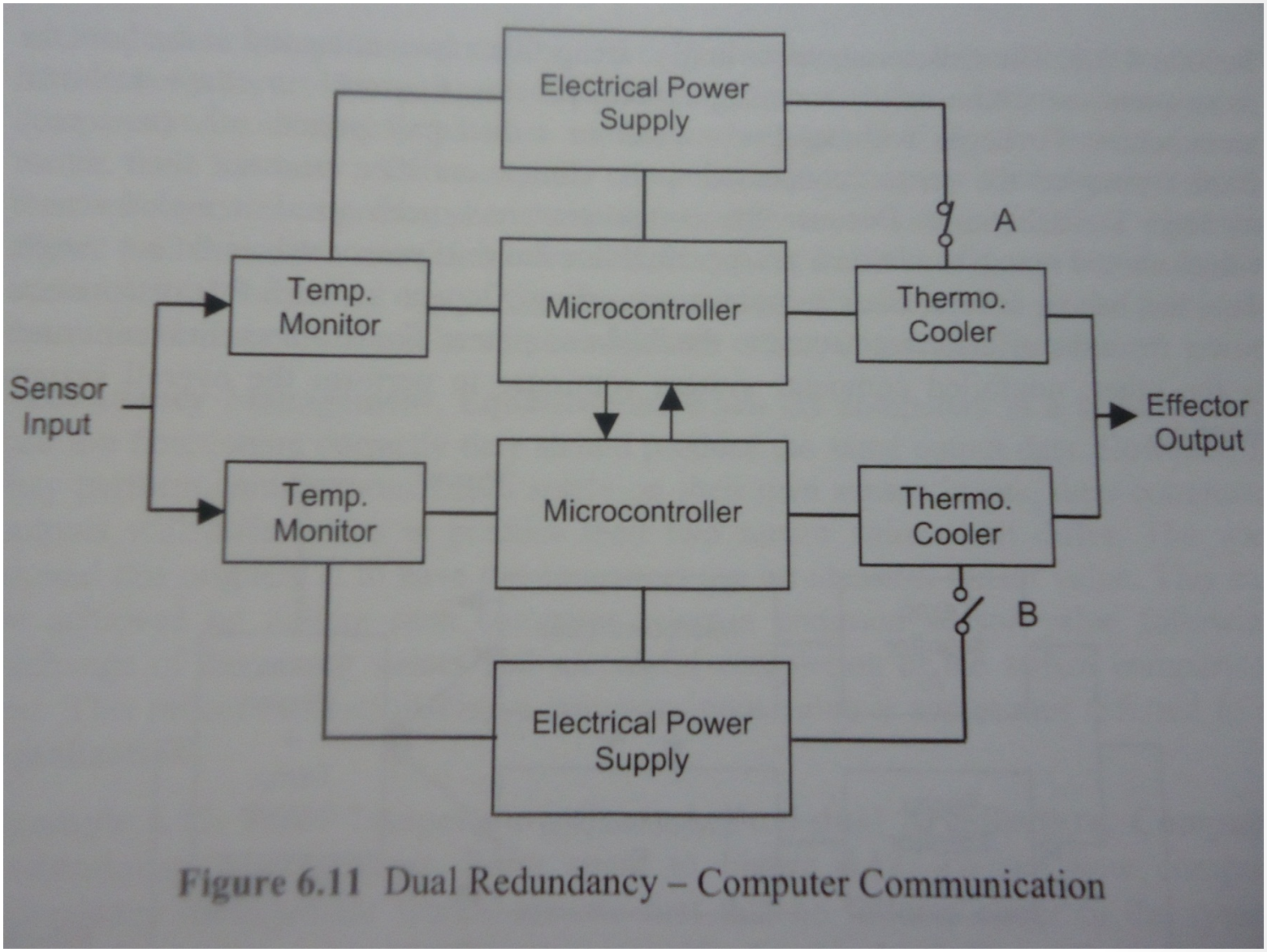


Figure 6.11 Dual Redundancy – Computer Communication

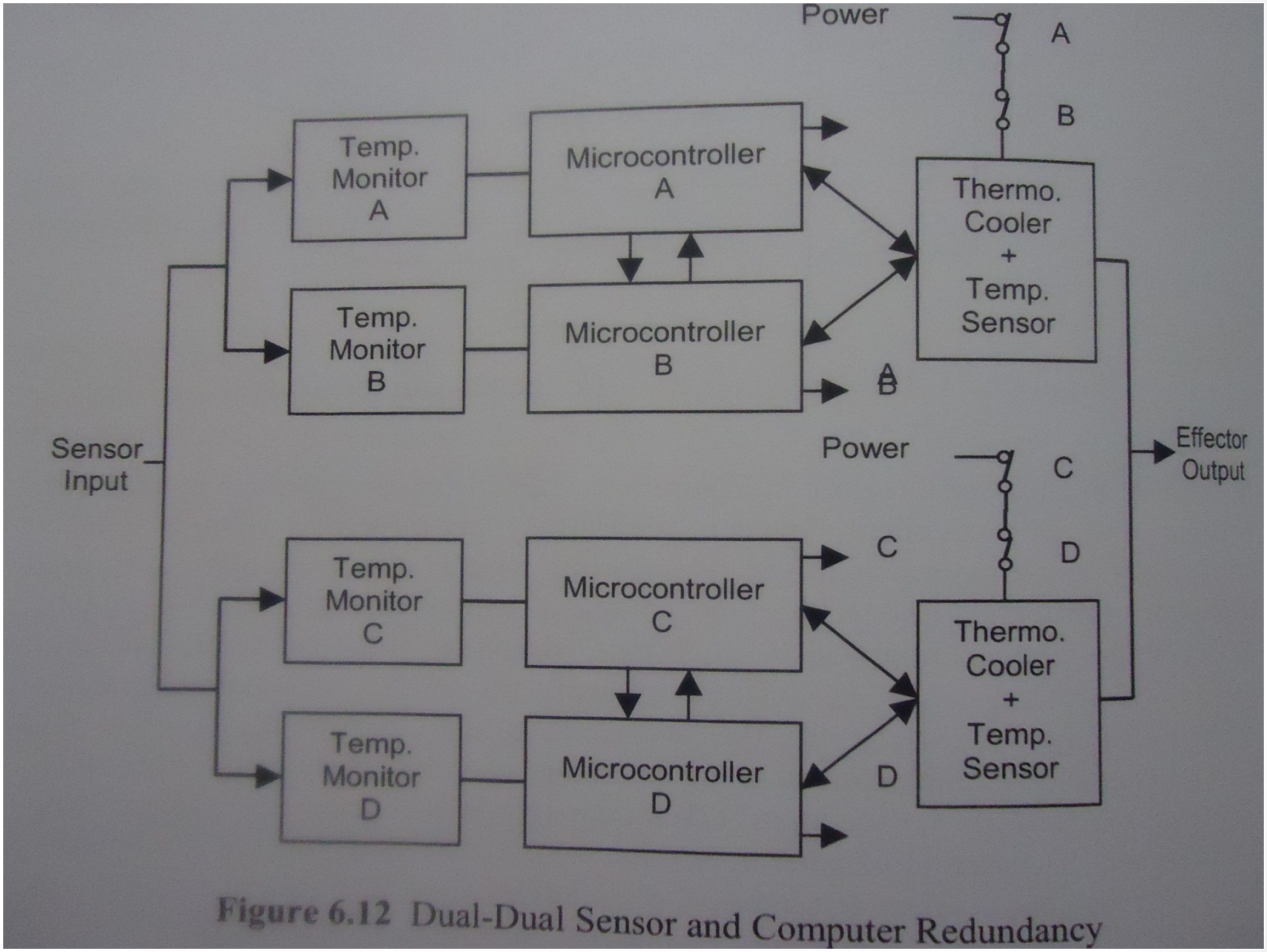


Figure 6.12 Dual-Dual Sensor and Computer Redundancy

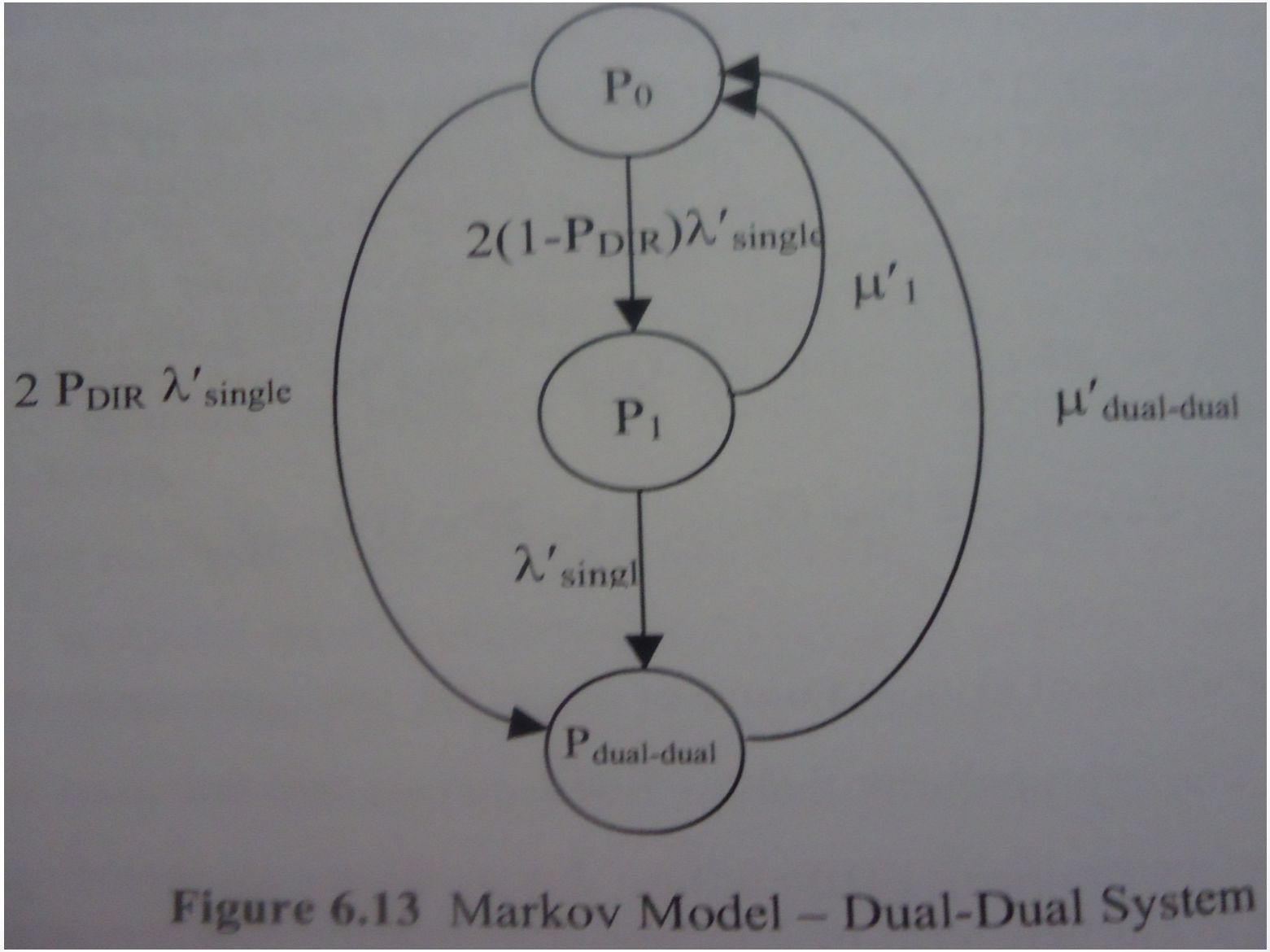


Figure 6.13 Markov Model – Dual-Dual System

Markov Model-Dual-Dual system

- P DIR –probability that the FDIR (Failure Detection Isolation Reconfiguration) process will fail.
- P0 –probability that no critical failures have occurred in the system.
- P1- probability that one of the computer s has failed and that the failure has been successfully detected, isolated , and the system successfully reconfigured.
- P dual-dual is the probability that there has been
  1) An Undetected critical failure
  2) An independent failure of both computer system
  3) Both of these events

This architecture is widely used in aerospace system.

Fluid Temperature control- Triplex System

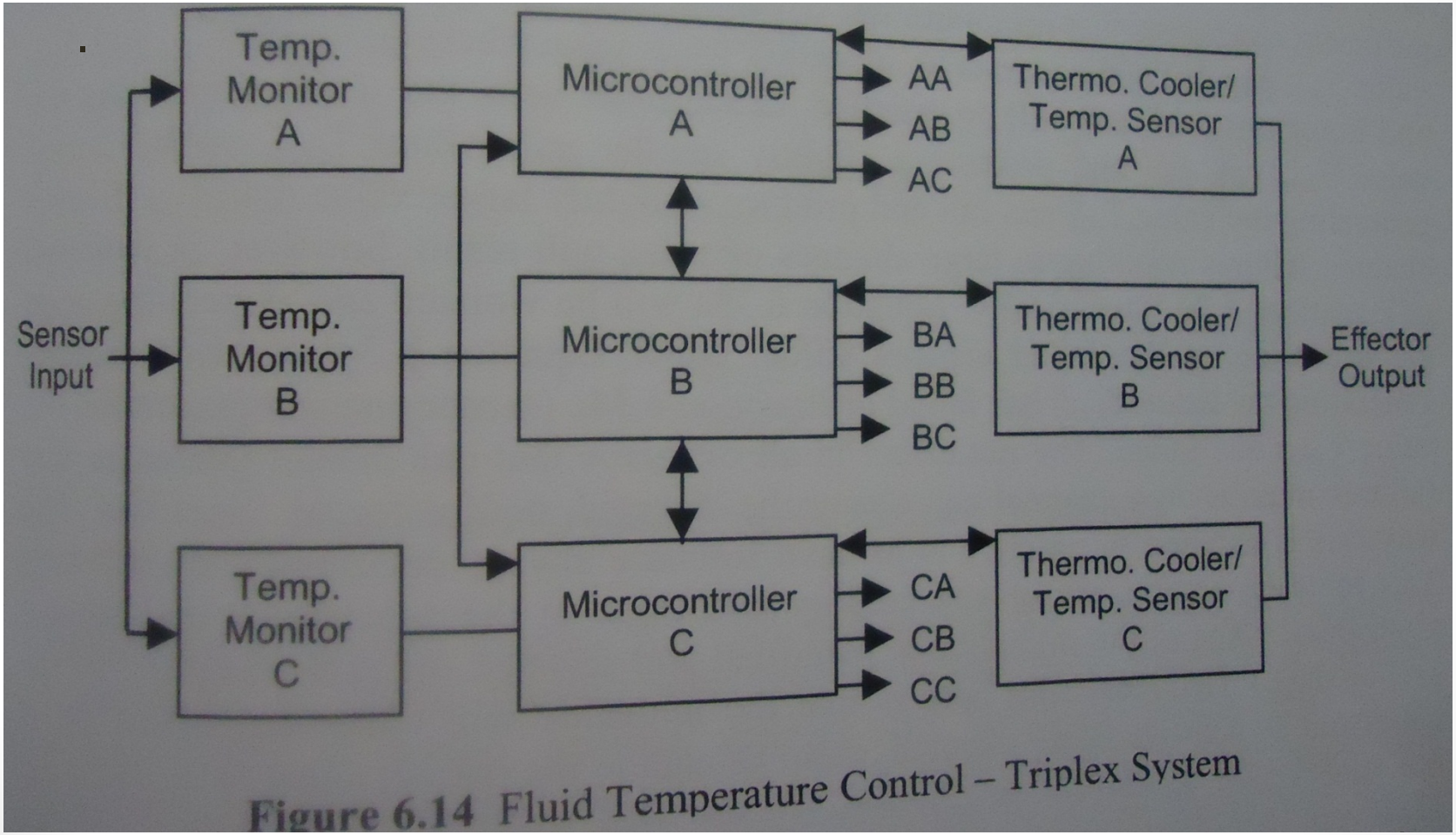


Figure 6.14 Fluid Temperature Control – Triplex System

Triplex System

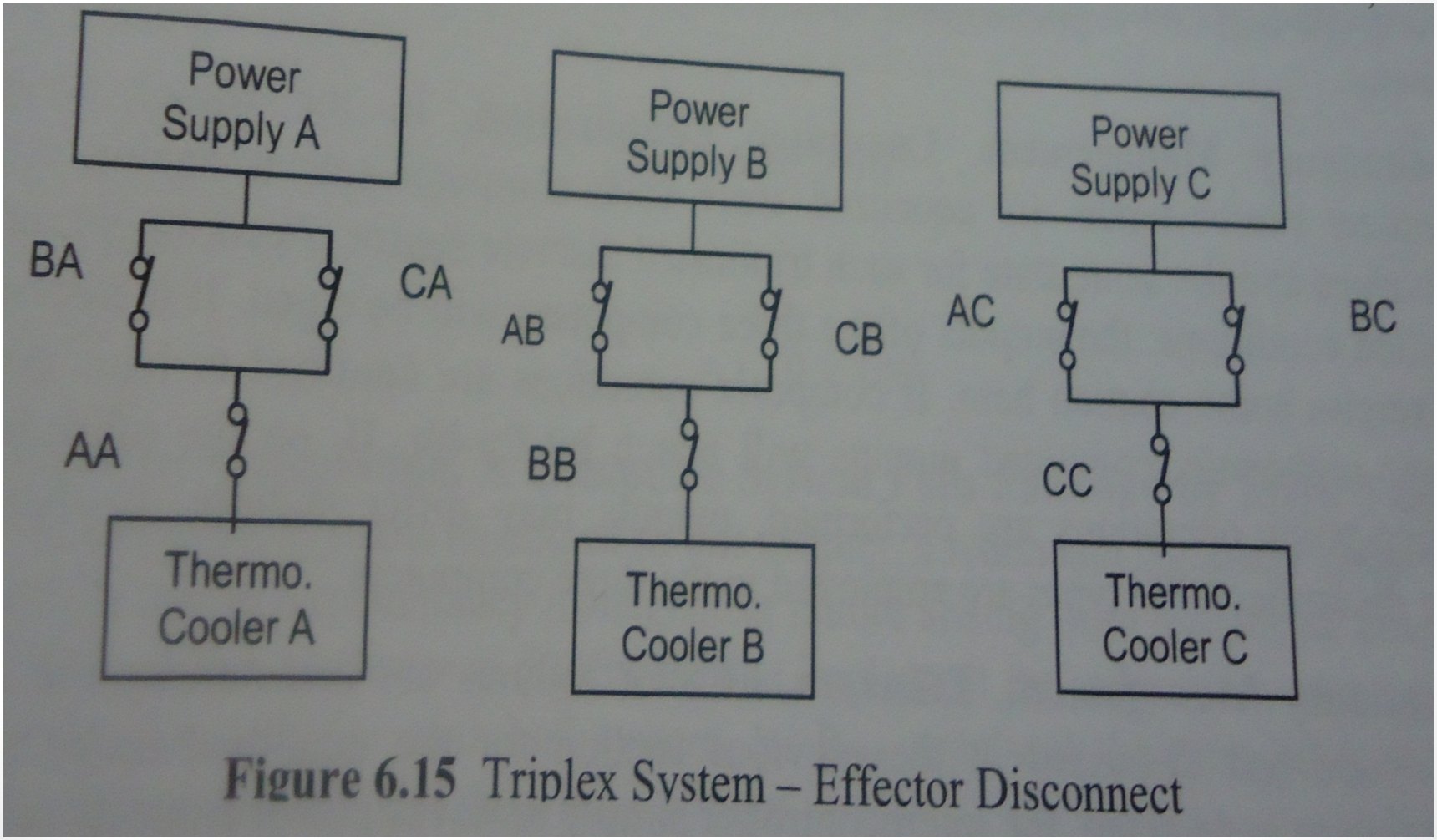


Figure 6.15 Triplex System – Effector Disconnect

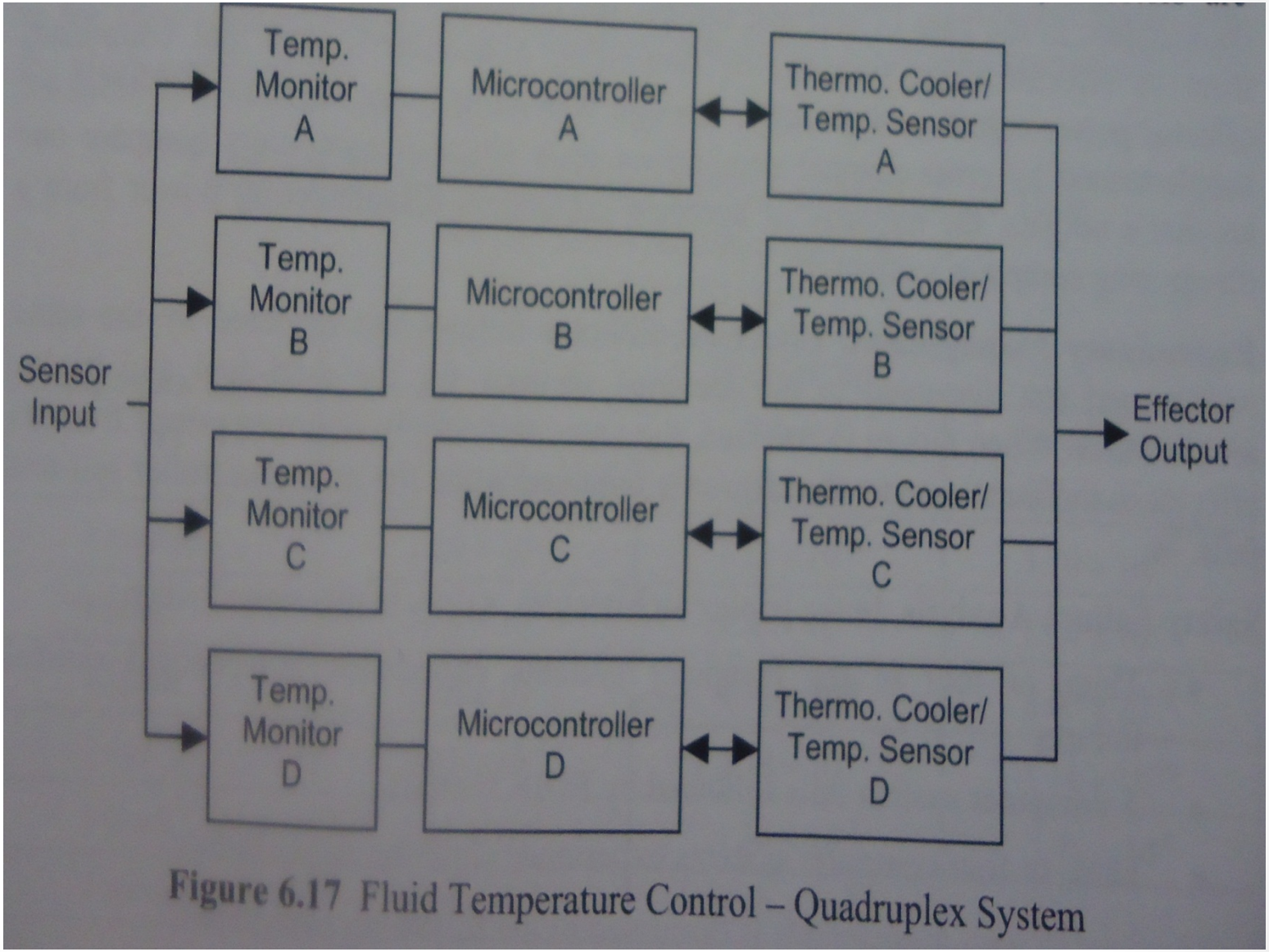


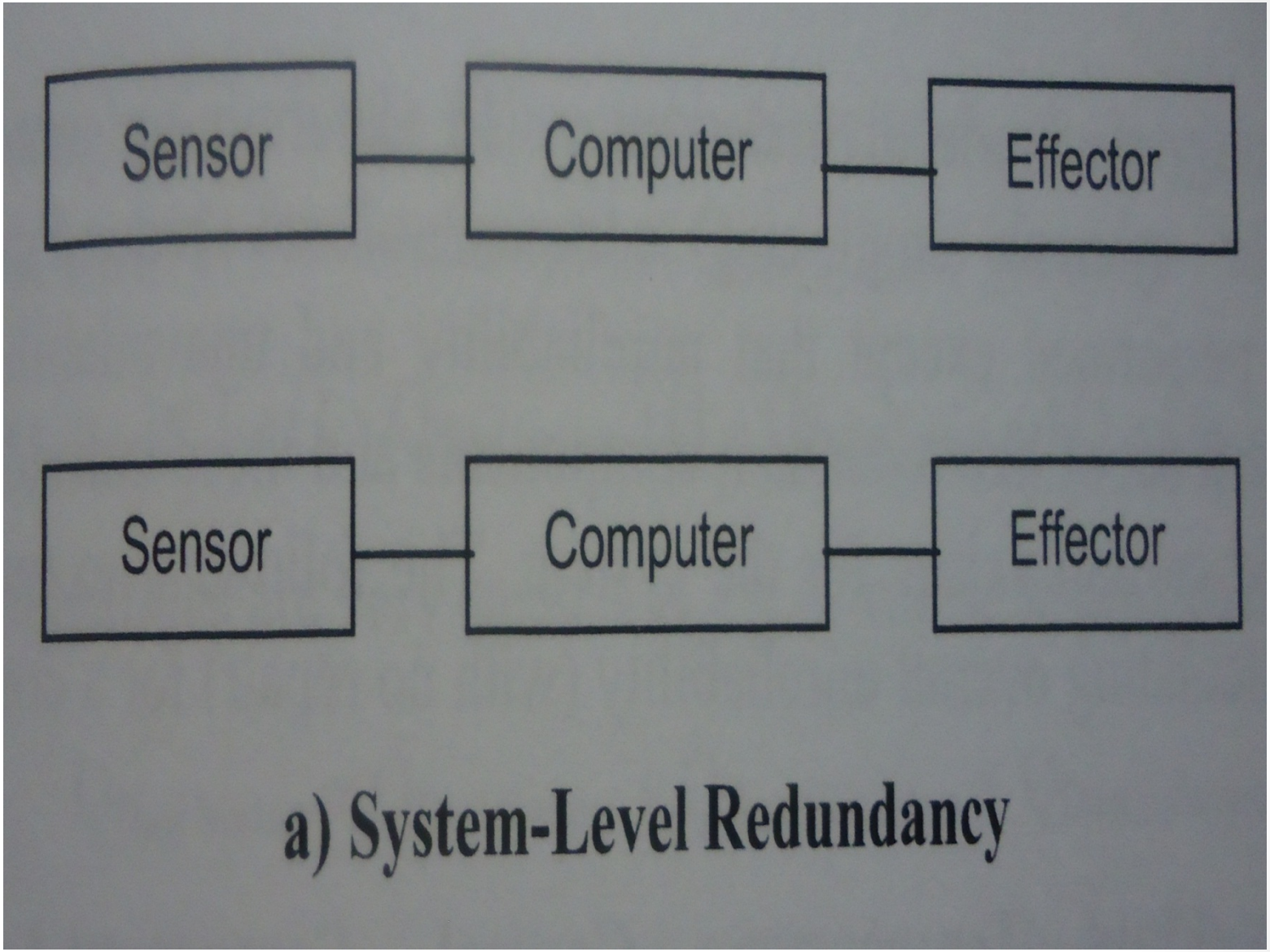
Figure 6.17 Fluid Temperature Control – Quadruplex System

Redundancy

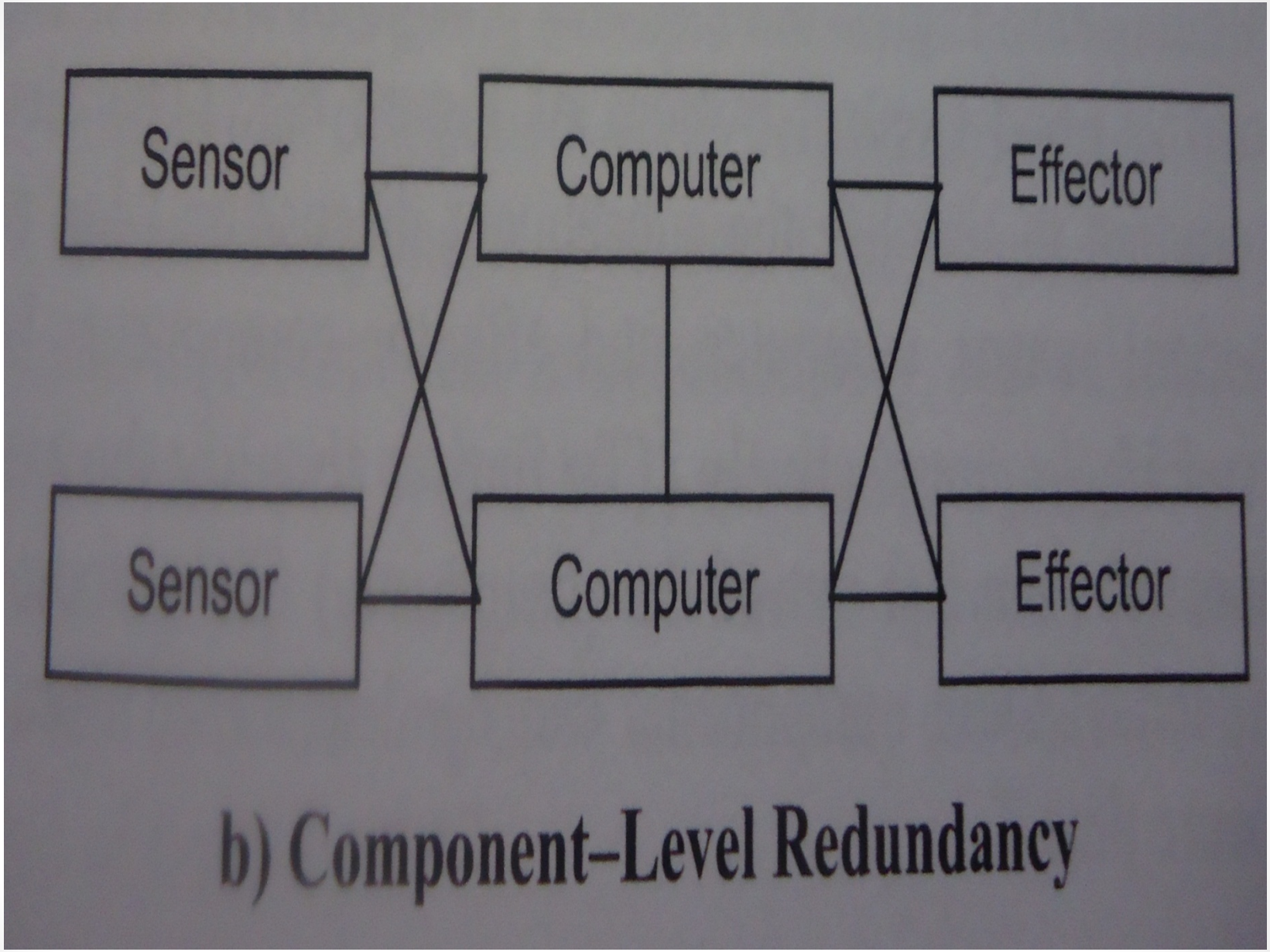
Redundancy Management

- System Level
  - The redundancy management in general involves the isolation and removal of the entire system.

- **Component Level**
  - The redundancy management operate to isolate and remove individual components, not the entire system.
  - A computer system is broken down into its individual components.
  - Each computer has inputs from all sensors and the ability to drive all effector.
  - It has **several benefits** over **system-level** redundancy.



a) System-Level Redundancy



b) Component–Level Redundancy

Component Level Redundancy Temperature control System

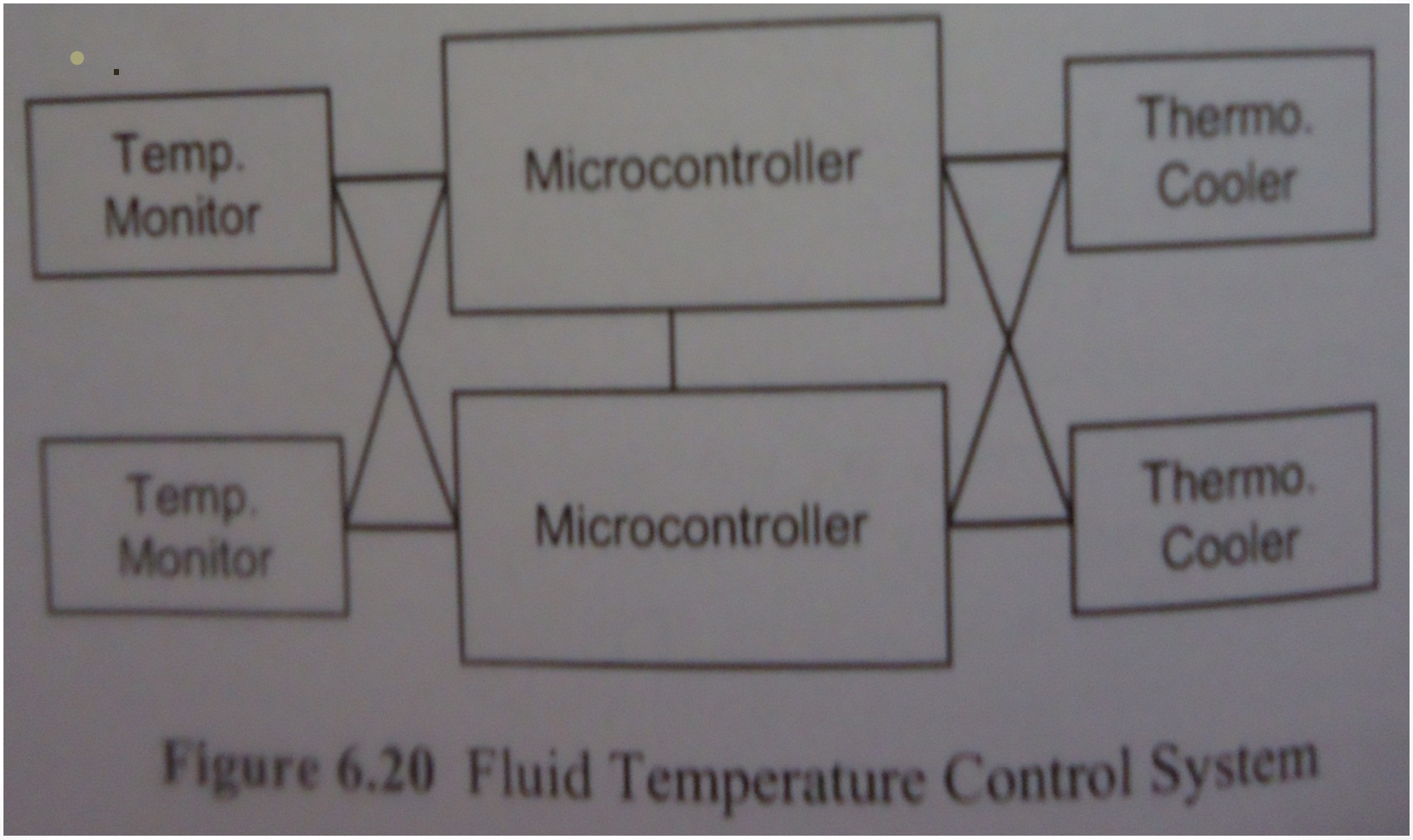


Figure 6.20 Fluid Temperature Control System

Software Redundancy

- Failure of software can lead to unsafe operation.
- The basic approach for implementing software redundancy is :
  1. Backup software may be employed to permit continued system operation in the event of primary software failure
  2. Dissimilar versions of software can be designed and implemented against a common set of functional and operational requirements.

- Disadvantage
- It is unlike to hardware redundancy because Multiple copies of a given software package will contain **the same faults and cause** simultaneous failures.

- The redundant software must be dissimilar.

Primary software Failure

Primary SW Failure Detection

- Stand alone real time software test s, which are hardwired to run every computational frame, can detect incorrect system responses that might be the result of primary software failure.
- Detected by the computer's **watchdog timer.**

Primary SW Failure Isolation

- Watchdog timeout can result from software entering an **endless loop** or failure of program counter hardware in computer CPU.
- If the failure has not altered program flow in each computer, computers can cross communication and agree that a **common failure** event has occurred.

Markov- model Triplex System with Backup Software

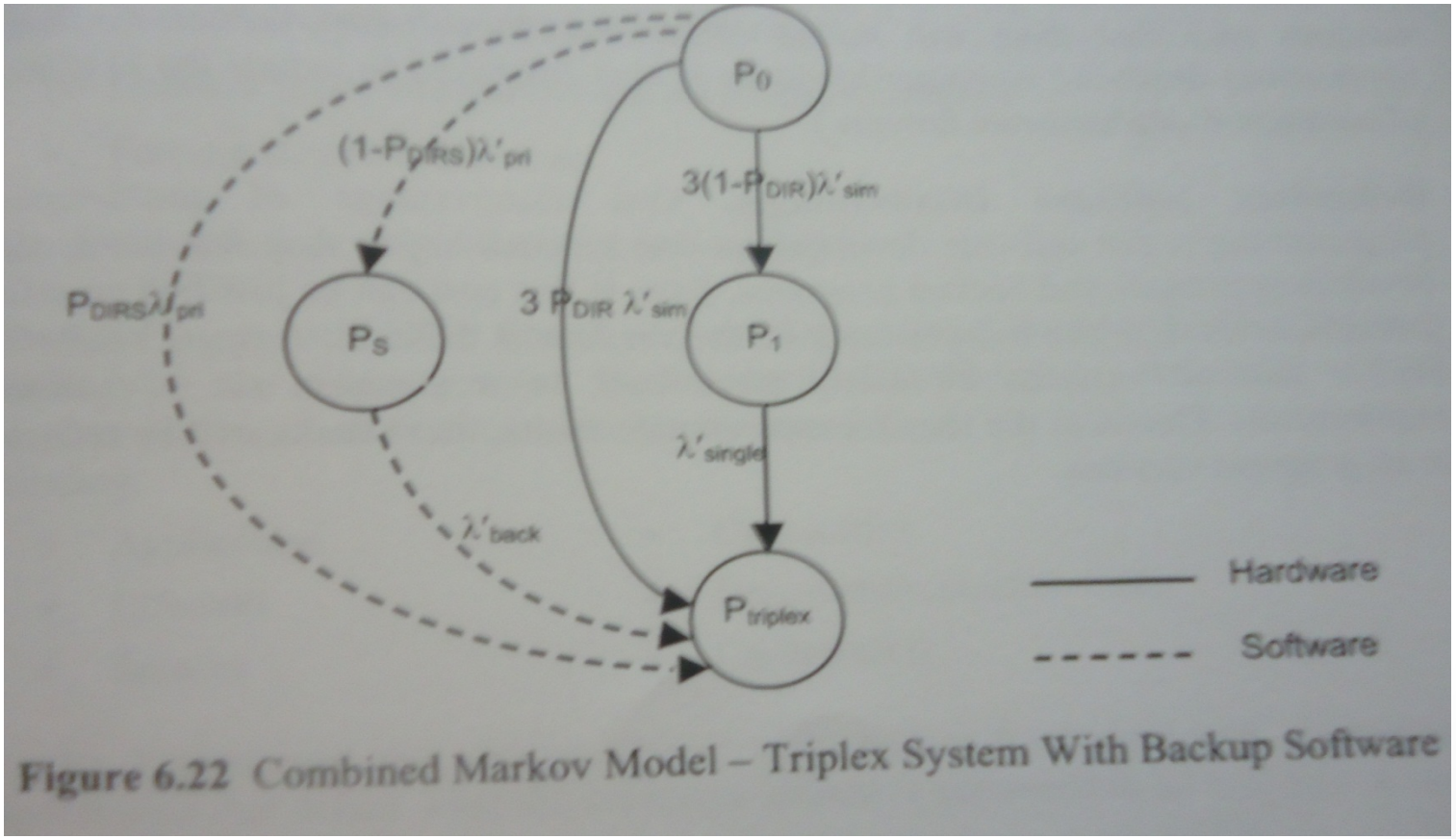


Figure 6.22 Combined Markov Model – Triplex System With Backup Software

Thank you