www.mwttr.com
EECE499 Computers and Nuclear Energy
Howard University
Dr. Charles Kim

Chapter 6: Design of Fail-Operate Computer Systems

By: Venessa Woodson

Overview

- 6.3.3 Simplex Computer System with Operable Backup
- 6.3.4 Dual Redundancy – Independent Systems

Purpose of Operable Backup

- If the Simplex computer system fails to operate, it is possible to retreat to a more primitive low-risk system in order to continue overall operation.

Safety Failure Analysis

- Most important safety concern is that the system will fail and place incorrect, possibly dangerous forces onto the manual system that the operator will not recognize or cannot overcome.

Table 6.2 Simplex Computer System Self-Test Summary

Components	Self-Tests
Sensors	State estimator, reasonableness tests, informational redundancy, dependent sensor values, and analytical redundancy.
Computer	Watchdog timer. CPU: self-tests. CPU hardware diagnostics. Memory: Checksums. "Checkerboard " test. Parity check (if implemented). End-around tests.
Effectors	Wraparound tests.
Power sources	Compare electrical, hydraulic, pneumatic power levels to normal range of values.

Redundancy Management

To detect failure, the computer conducts hardware and software tests. When a failure is detected, the system signals the operator, disengages it and assumes manual control using the backup system.

Example Backup System: Autopilot

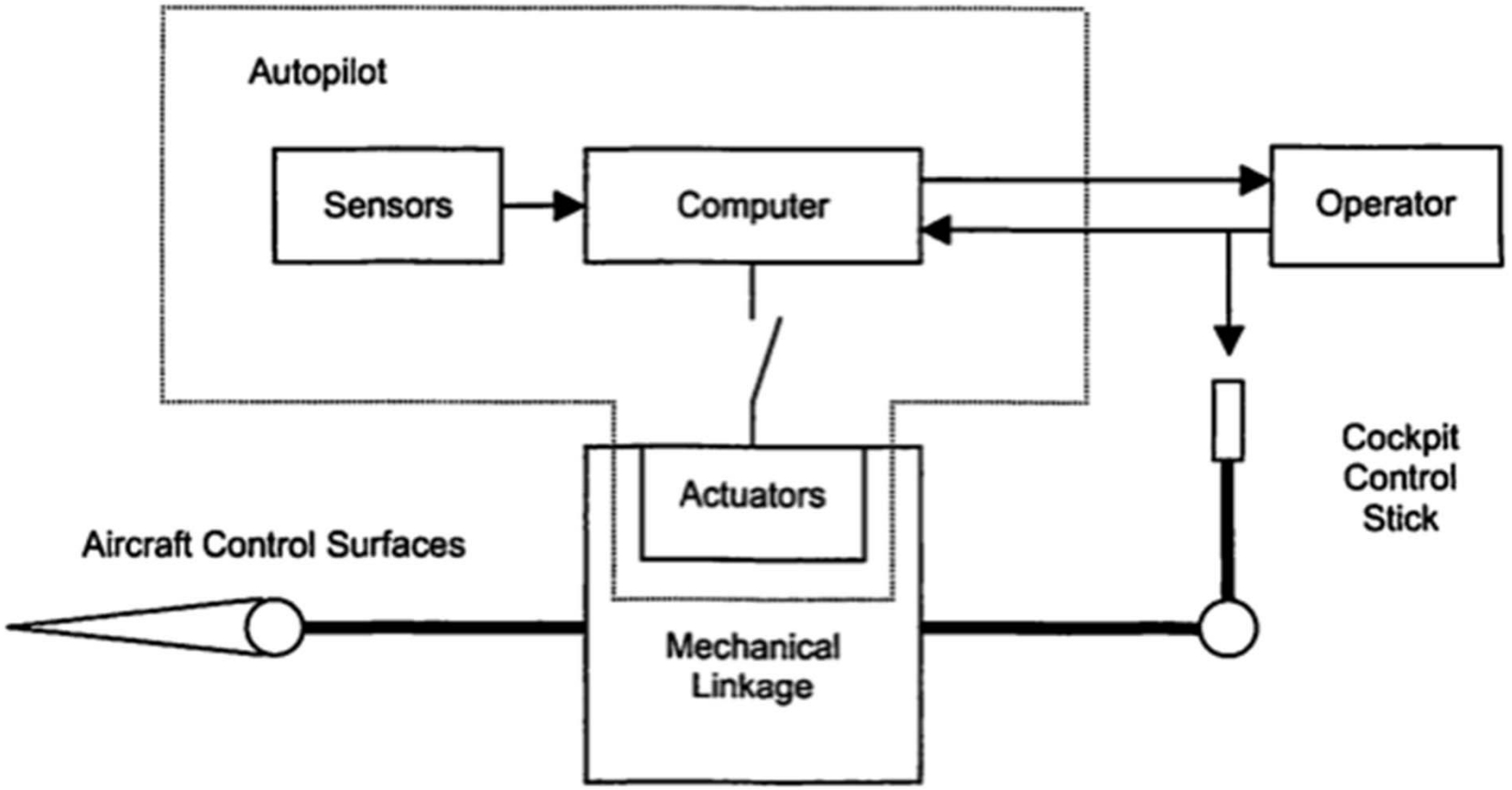

Figure 6.6 Aircraft Autopilot Detailed Mechanization

Hardware Unreliability Analysis

- Unreliability: The probability of the backup system having critical failure and/or the simplex computer system having critical failure is denoted by $Q_{simback}$.

$$Q_{simback} = Q_{sim} \times P_D \times (1-Q_{back}) + Q_{back}$$

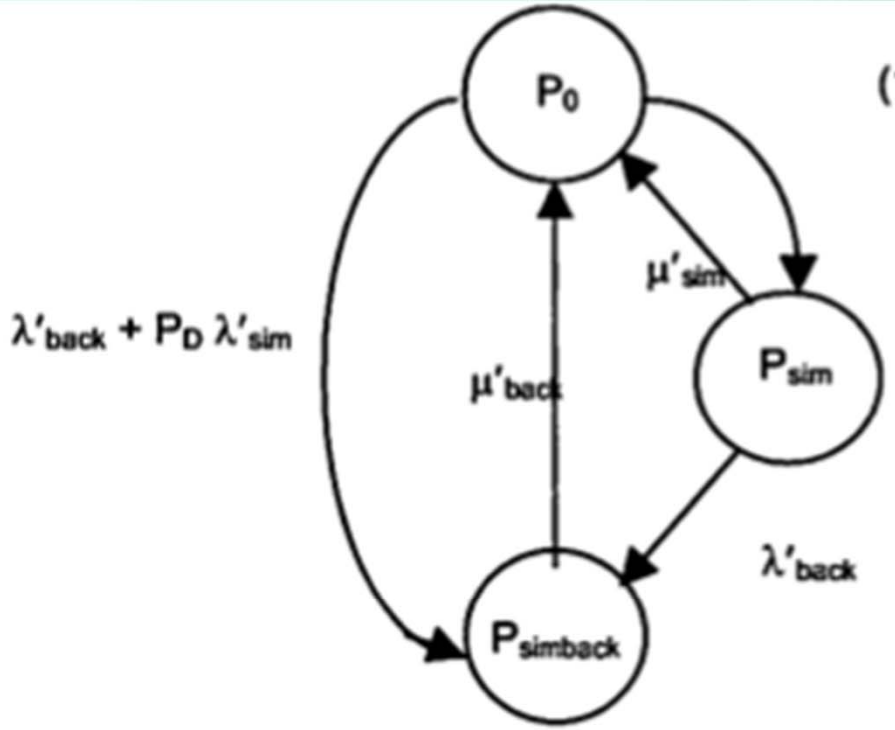

Figure 6.7 Markov Model – Simplex System With Backup

Markov Model

Another way to analyze unavailability and unreliability.

6.3.4 Dual Redundancy – Independent Systems

To avoid a degraded performance, the backup system is a standby duplicate system (Standby Redundancy).

The system is not connected but stands by as a spare unit ready to pick up the primary system's duties.

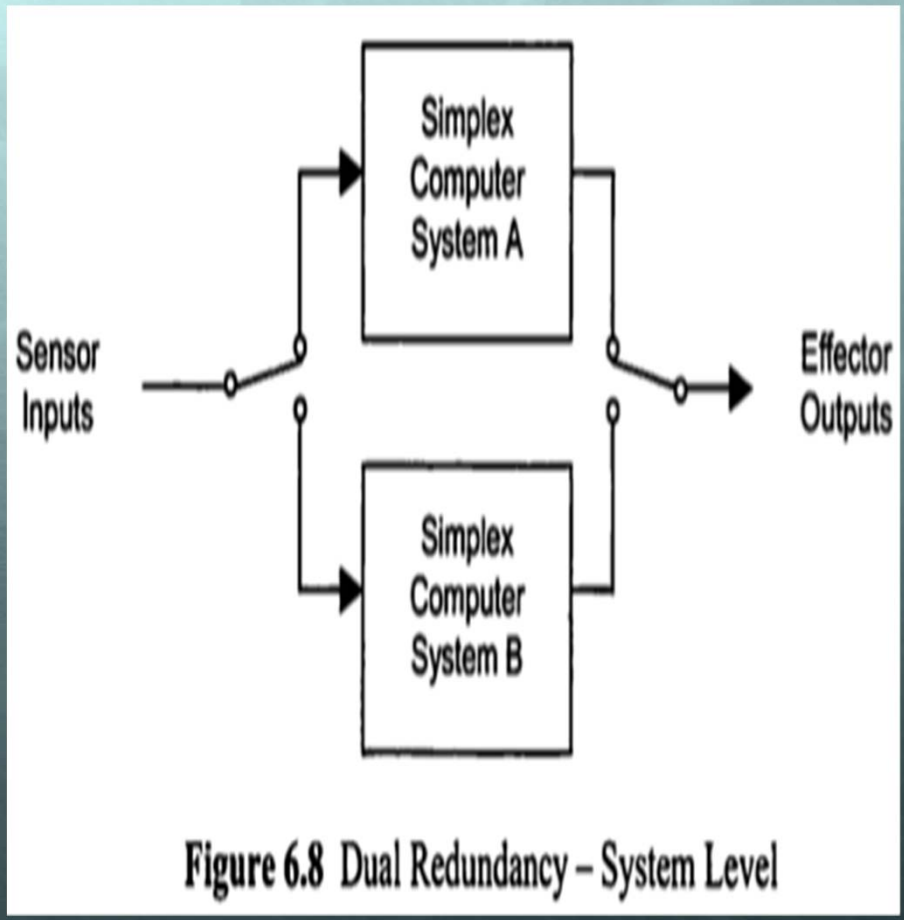

Figure 6.8 Dual Redundancy – System Level

Practical Considerations: Hot versus Cold Standby

Hot

- Has the advantage of being immediately available should the primary unit fail.

Cold

- Has the advantage of minimizing power consumption.

Practical Considerations: Synchronization

The primary and standby computers will have slightly different frame rates, meaning that any common computation employing pure counters, such as timers, will yield different results in the two computers.

Hardware Unreliability Analysis

- Unreliability of the dual system: One or both of the systems failing is denoted by Q_{dual}.

$$Q_{dual} = Q_{pri} \times Q_{sby} \times (1-P_{DS}) \times Q_{pri} \times P_{DS}$$

Figure 6.10 Markov Model – Dual System

Markov Model – Dual System

Another way to analyze unreliability and unavailability.

Common-Cause Failure

- Dual Redundancy must take Common-Cause Failure into consideration.
- With two of the exact same systems, the rate at which they would fail in common is

$$\lambda_{cc} = f_{cc} \times \lambda_{nom}$$

The Simplex Computer System with Operable Backup and the Dual Redundancy system are both good ways of designing Fail-Operate computer systems but no system is perfect!

Any Questions?