Chapter 6: Design of Fail-Operate Computer Systems

BY: ALEXIS WELLS
COMPUTERS & NUCLEAR ENERGY
NOVEMBER 14, 2013

Overview

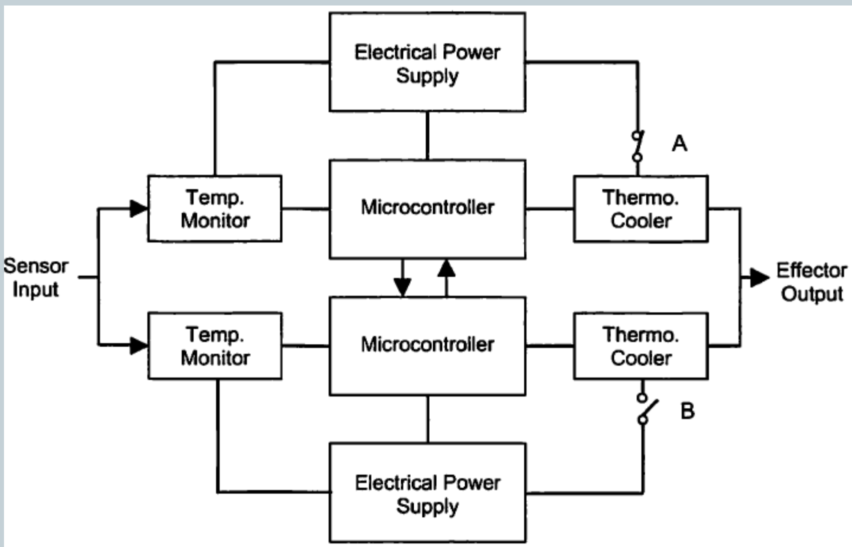
- Section 6.3.5: Dual Redundancy
- Section6.3.6: Triplex Architecture
- Section6.3.7: Quadruplex Architecture
- Section 6.3.8:Defining Custom Hardware

Dual Redundancy

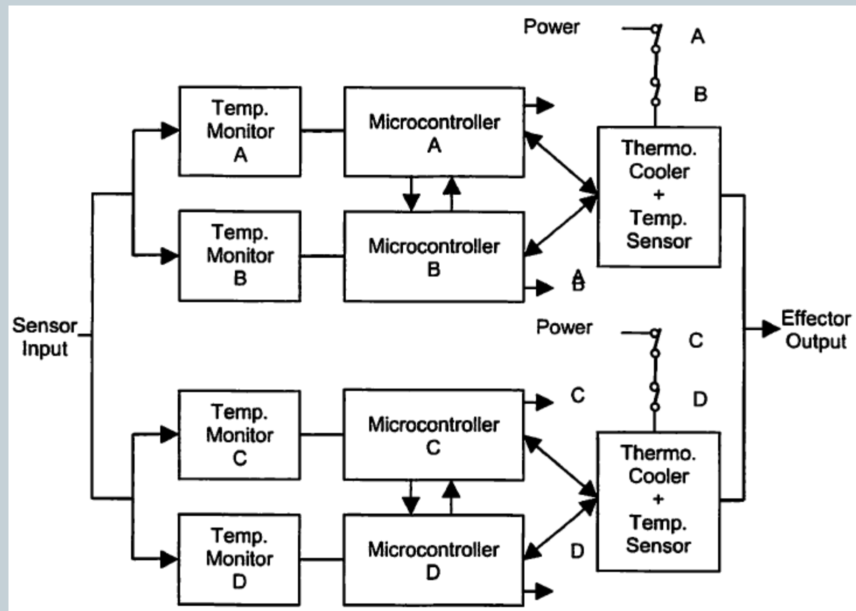
Dual Architecture	Dual-Dual Architecture
• Primary and Back-up computers are physically separated • Computer Communicate with one another to check for failures within sensors and data	• combining two dual systems • Both Systems are active and operating

Dual Architecture vs Dual-Dual Architecture

Dual

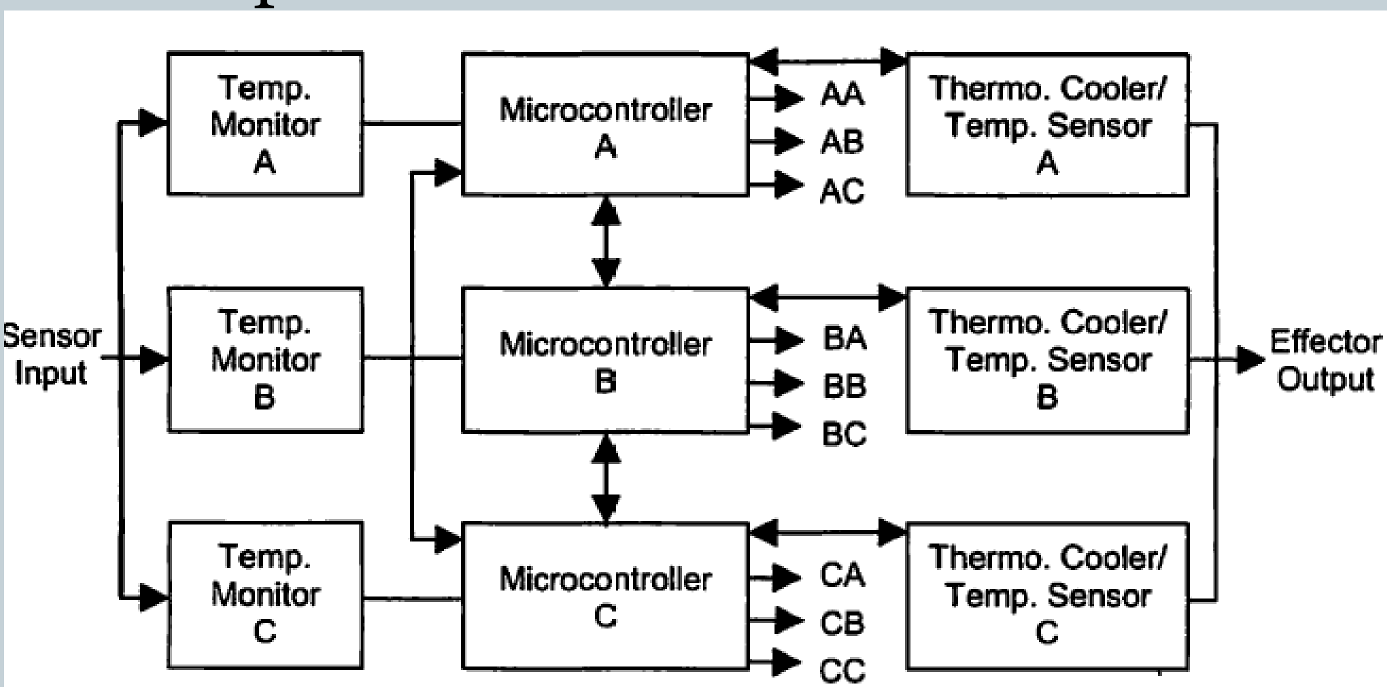


Dual-Dual



Triplex Architecture

- Three Redundant sets of components
- Less expensive, and still achieves single failure, fail-operational performance



Triplex Redundancy Management

1. Each computer controls separate Thermocooler
2. Results in 3 redundant temperature monitors
3. Computers communicate values & are synchronized

- Comparison of 3 Data Sets

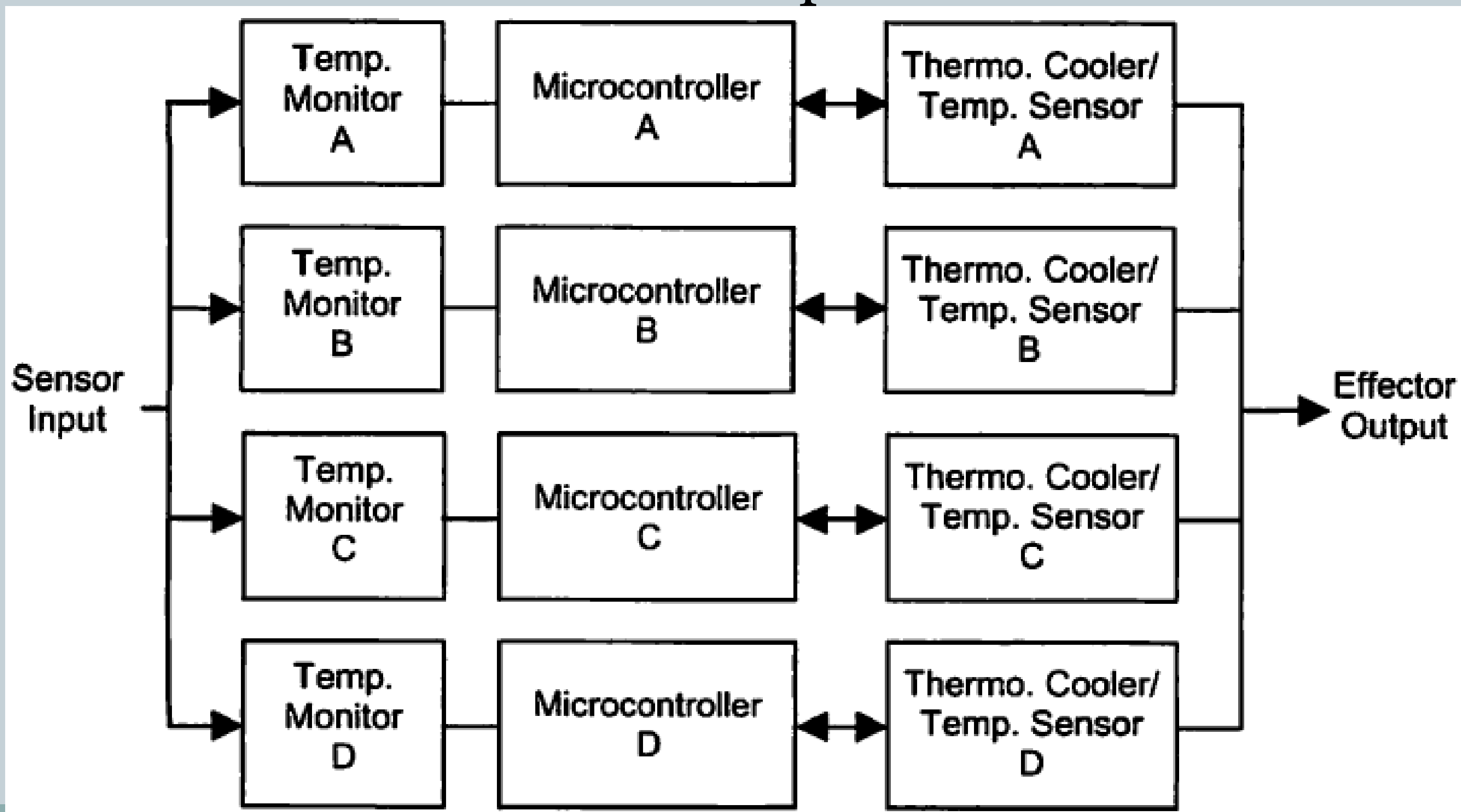
$$(T_{max} - T_{min}) \leq T_{threshold}$$

$$(T_{max} - T_{mid}) \leq T_{threshold}$$

$$(T_{mid} - T_{min}) \leq Tthreshold$$

Quadruplex Architecture

- Can tolerate two or more sequential failures



Force Vote

- Failed computers or effectors remain in failed state while other computers in the system continue to operate normally, over powering the failed systems.

Unreliability

- Dual

  $Q_{single} = 1.26 \times 10^{-4}$

- Dual-Dual

  $Q_{dual\text{-}dual} = [\ Q_{single}\ ]^2 = 1.58 \times 10^{-8}$

- Triplex

  $Q_{triplex} = 1.19 \times 10^{-8}$

- Quarduplex

  $Q_{quadruplex} = 4 \times [Q_{sim}]^3 - 3 \times [Q_{sim}]^4$

- Protection
  - Diversity in Component Design

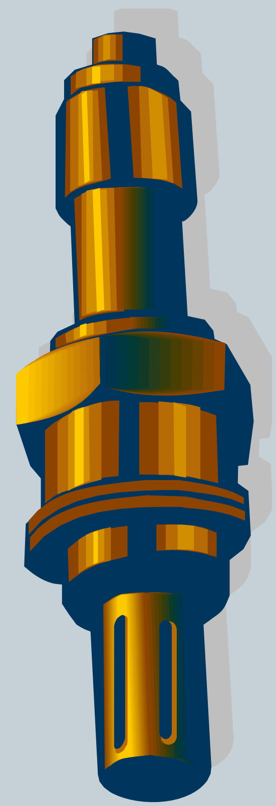
($\lambda'_{sim} = 1.26 \times 10^{-5}$/hr)

Exposure Time (T)	Unreliability		
	Simplex (Q_{sim})	Triplex ($Q_{triplex}$)	Quadruplex ($Q_{quadruplex}$)
1 minute	2.10×10^{-7}	1.32×10^{-13}	3.70×10^{-20}
1 hour	1.26×10^{-5}	4.76×10^{-10}	8.00×10^{-15}
10 hour	1.26×10^{-4}	4.76×10^{-8}	8.00×10^{-12}
1 day	3.02×10^{-4}	2.74×10^{-7}	1.11×10^{-10}
1 week	2.11×10^{-3}	1.34×10^{-5}	3.78×10^{-8}
1 month	9.16×10^{-3}	2.50×10^{-4}	3.06×10^{-6}

Redundancy Management: Sensors

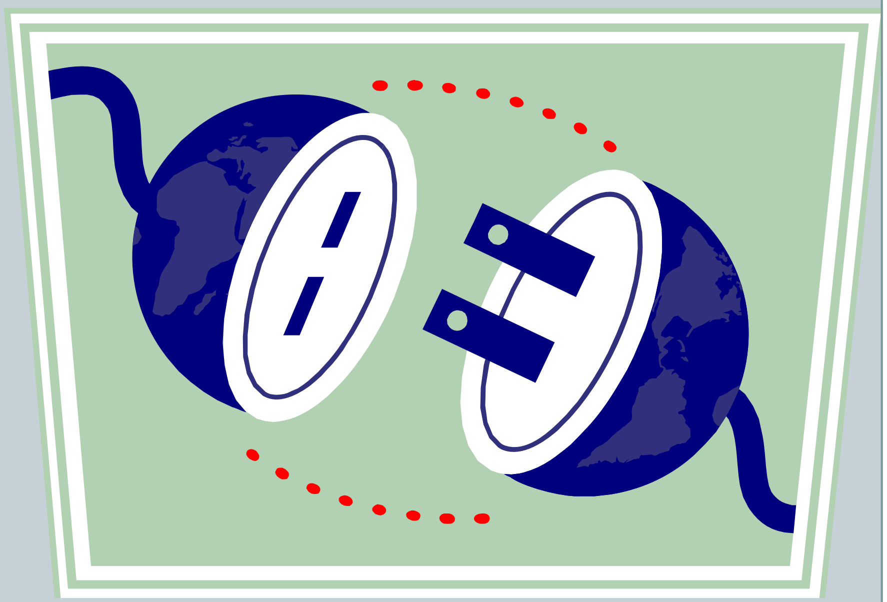
1. Each computer gathers information from sensor
2. Computers share readings
3. Compare if values are within predetermined threshold
4. Yes -> System is Functioning

   No -> System Failure



Redundancy Management: Computers

- Method of Failure Detection: Comparison of Results
  - If results do not match, computer with irregular values loses power
  - Other computer continues operation



Redundancy Management: Equalization

- Equalization: process of establishing a common input value
  - Sensors have standardized starting point
  - Computers are more likely to produce similar outputs
  - Less likely to detect errors

Redundancy Management: Effectors

- Temperature decreases when Microcontroller command is on
- Temperature increases when Microcontroller command is off
- Temperature Value lies within pre-specified Range

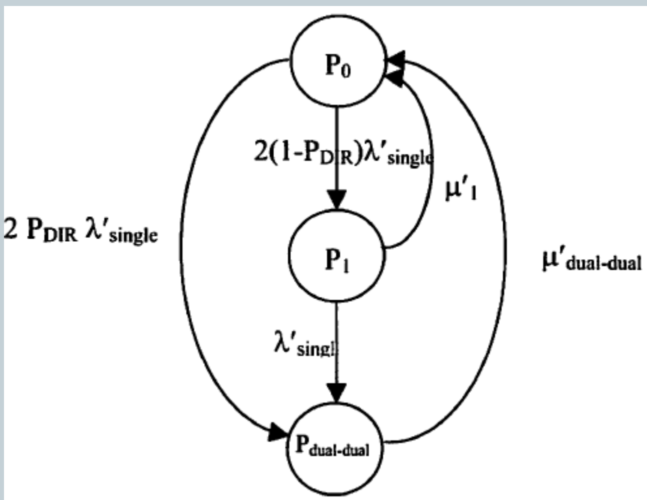
Safety Failure Analysis

- Both computer systems experience independent critical failures
- Computer System Fails followed by FDIR failure
- Common-Cause Failure

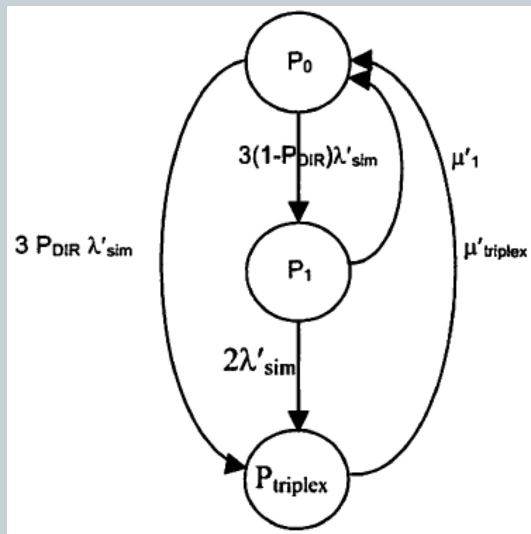
Markov Models

Probability Theory: Models system with random variable through time

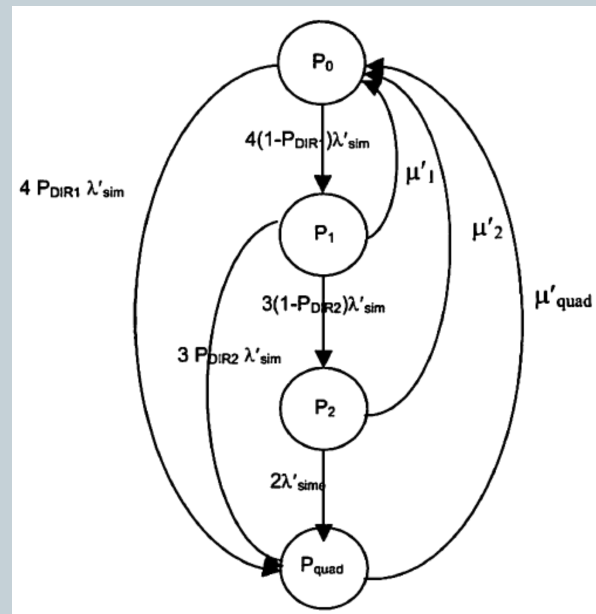
- Dual-Dual



- Triplex



- Quadraplex



- P_0 = No Critical Failures
- P_n = Probability n computers have failed, detected fault, isolated, and reconfigured
- μ_n = Average Rate Failures P_n are repaired

Defining Custom Hardware

- System Level Redundancy
- Component Level Redundancy
- System Decomposition
- Independent Safety Back-ups