Chapter 4: Design of Fail-Safe Computer Systems

Sections 4.3 & 4.4

Phathom Donald
Electrical and Computer Engineering
Howard University

EECE499 Computers and Nuclear Energy –Dr. Charles Kim

Topics

- 4.3: Fail-Safe Computer Systems - Dual Redundant Architecture
  - 4.3.1: Simplex System Limitations
  - 4.3.2: Dual Redundancy - Sensors
  - 4.3.3: Dual Redundancy - Computer Hardware
  - 4.3.4: Software in the Dual Redundant Hardware System
  - 4.3.5: Dual Redundancy and Independent External Safety Devices
- 4.4: Reliability and Quality Improvements
  - 4.4.1: Reliability Improvements
  - 4.4.2: Quality Measures

4.3.1: Simplex System Limitations

- Fail-Safe System: One that in the event of a failure will revert to a non-operating state that will not cause a mishap.

- The simplex computer system can be made fail-safe and suitable for use in a large number of potentially hazardous applications.

- Potential weaknesses in two areas: sensor failure detection and computer fault detection

4.3.1: Simplex System Limitations

- Sensor Failure Detection:
  - Failure of a single sensor can be detected only if software can estimate what the correct sensor value should be.
  - Cannot always know in advance what the sensor value should be at any given time.
- Computer Hardware Fault and Failure Detection:
  - Fault and failure diagnostics cannot detect all possible hardware faults.
  - Redundant computers may be required.

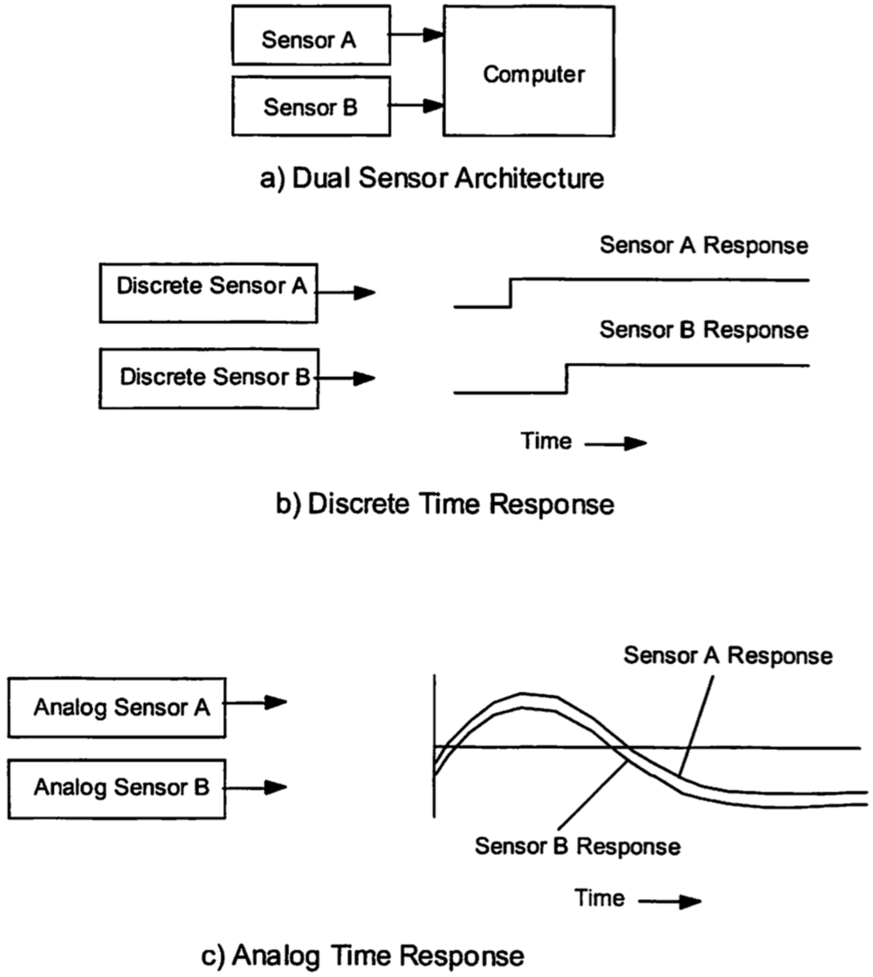
4.3.2: Dual Redundancy - Sensors

- Duplicate sensors using one for monitoring and control and the second as a reference that provides the “known” value for use in failure detection.

  a) Two sensors measure same stimulus and generate identical outputs.

  b) Outputs of two sensors are skewed in time.

  c) Sensors generating analog outputs can also be expected to differ. Threshold must be established.



a) Dual Sensor Architecture

b) Discrete Time Response

c) Analog Time Response

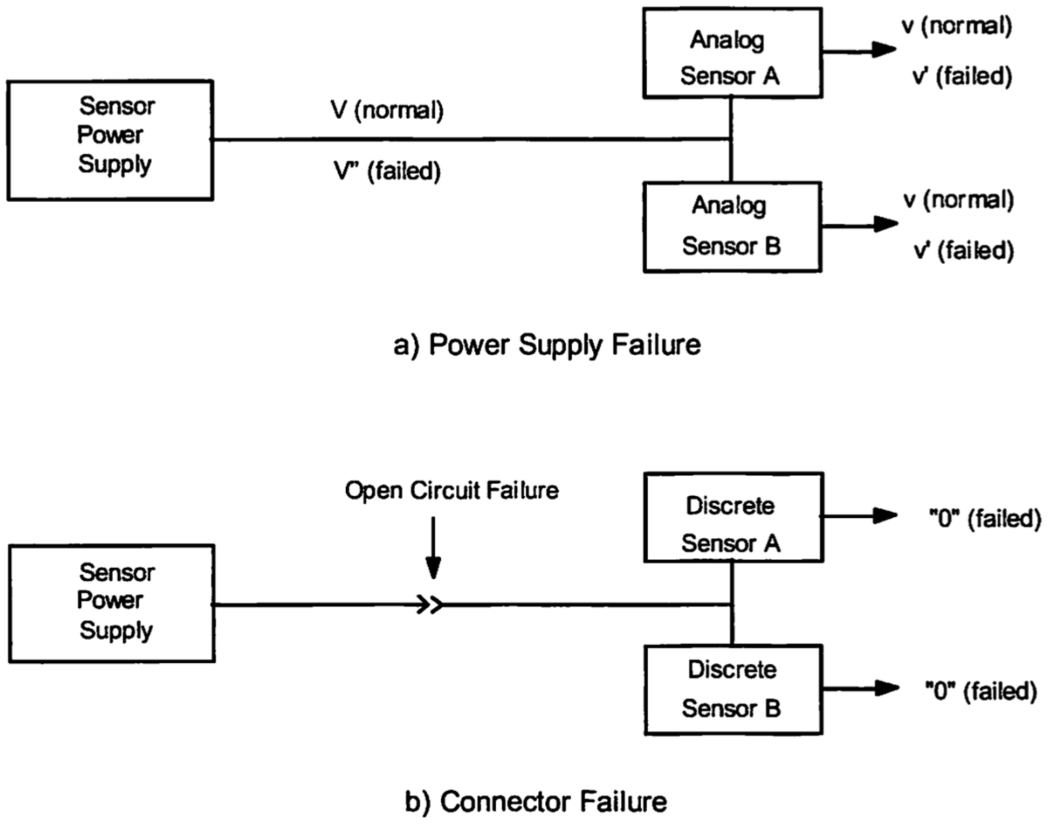
Figure 4.16 Dual Sensor Architecture and Responses

4.3.2: Dual Redundancy - Sensors

- **Single-Points-of-Failure**: simplex components can have single failures resulting in the sensors generating matching, but incorrect results.

  a) Dual sensor outputs will match, whether correct or incorrect.

  b) A single open-circuit failure in the connector can leave both sensors generating the same unchanged level regardless of input stimulus.



a) Power Supply Failure

b) Connector Failure

Figure 4.17 Dual Redundancy Single-Points-of-Failure

4.3.3: Dual Redundancy - Computer Hardware

- **Dual computer redundancy** is employed where hardware single-points-of-failure are unacceptable and where failure detection speed is important.
- Hardware and software in each of the two computers will function identically when there are no failures.
- Matching Outputs = No Failures
- Just compare the two computer outputs

4.3.3: Dual Redundancy - Computer Hardware

- Computer hardware, system power supplies, interconnects, and sensors are duplicated.

- **Channel**: groupings of sensors, power supplies, computers, and interconnects.

- Channels are independent; communication path is electrically isolated.

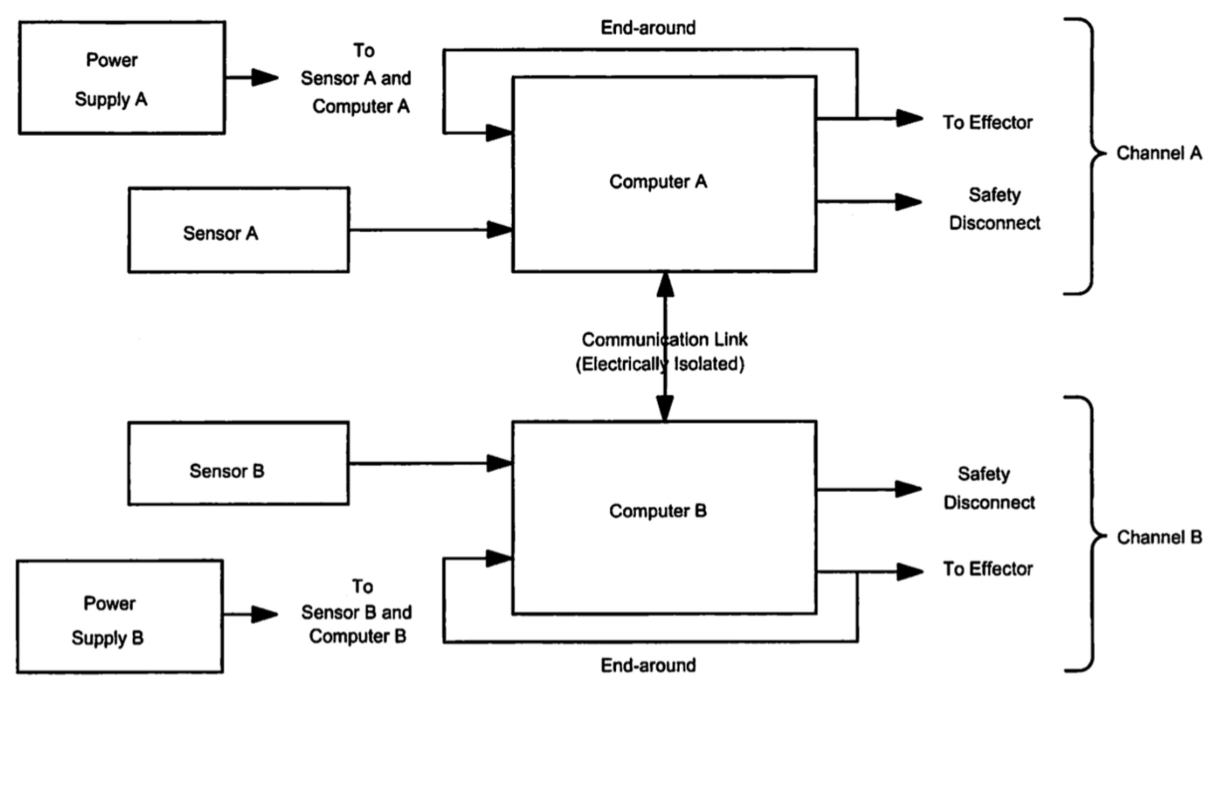


Figure 4.18 Dual Computer Architecture

- Computers execute exactly the same sequence of instructions.

- Two basic functions: normal control/monitoring and hardware failure detection

4.3.3: Dual Redundancy - Computer Hardware

- Computer A and Computer B exchange sensor values which are compared
- Mismatch = Declared Failure
- **End-Around Test** conducted to cover failures that might occur.

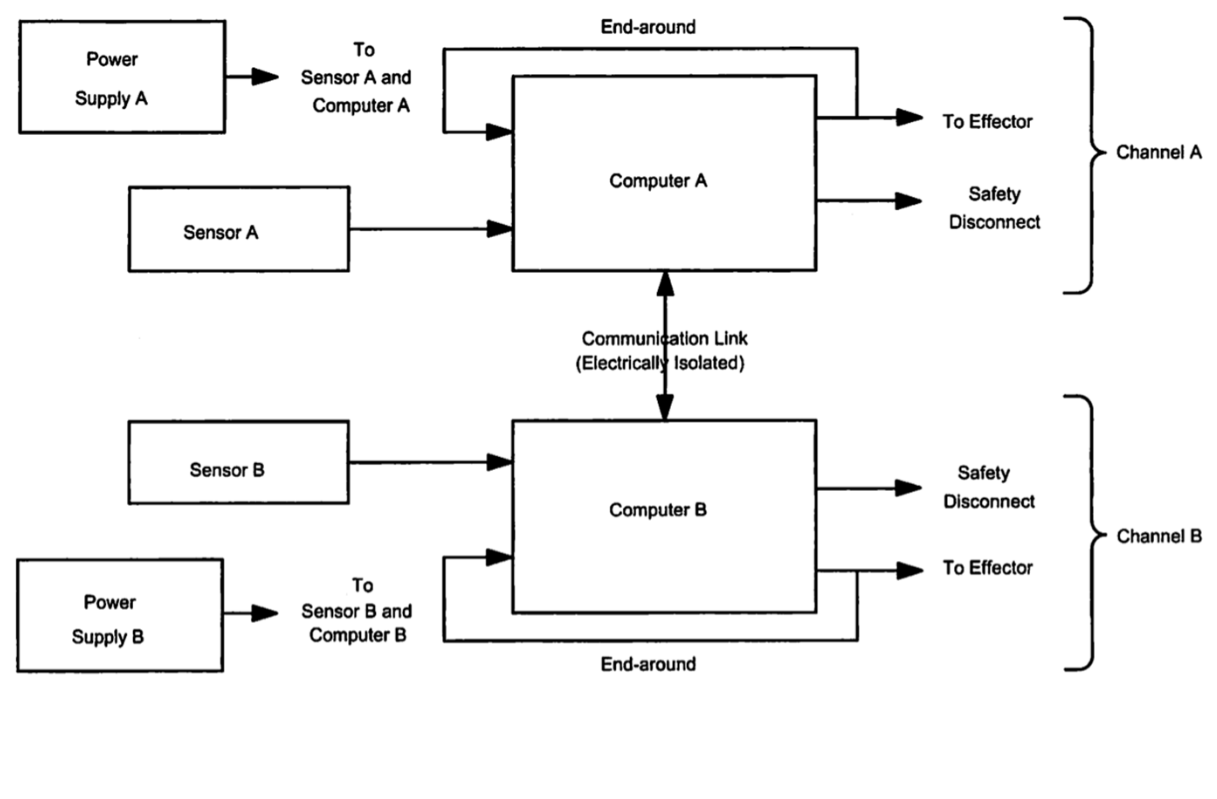


Figure 4.18 Dual Computer Architecture

- When a failure is detected, the computer software generates a disconnect output that must reconfigure the system to a fail-safe condition.

4.3.3: Dual Redundancy - Computer Hardware

- The frame of the two computers need to be synchronized for the hardware and software in the two channels to function identically when there are no failures.

- Computer B is synchronized to Computer A.

- As a crosscheck on Computer B, Computer A samples Computer B's frame pulse to verify that it matches its own.

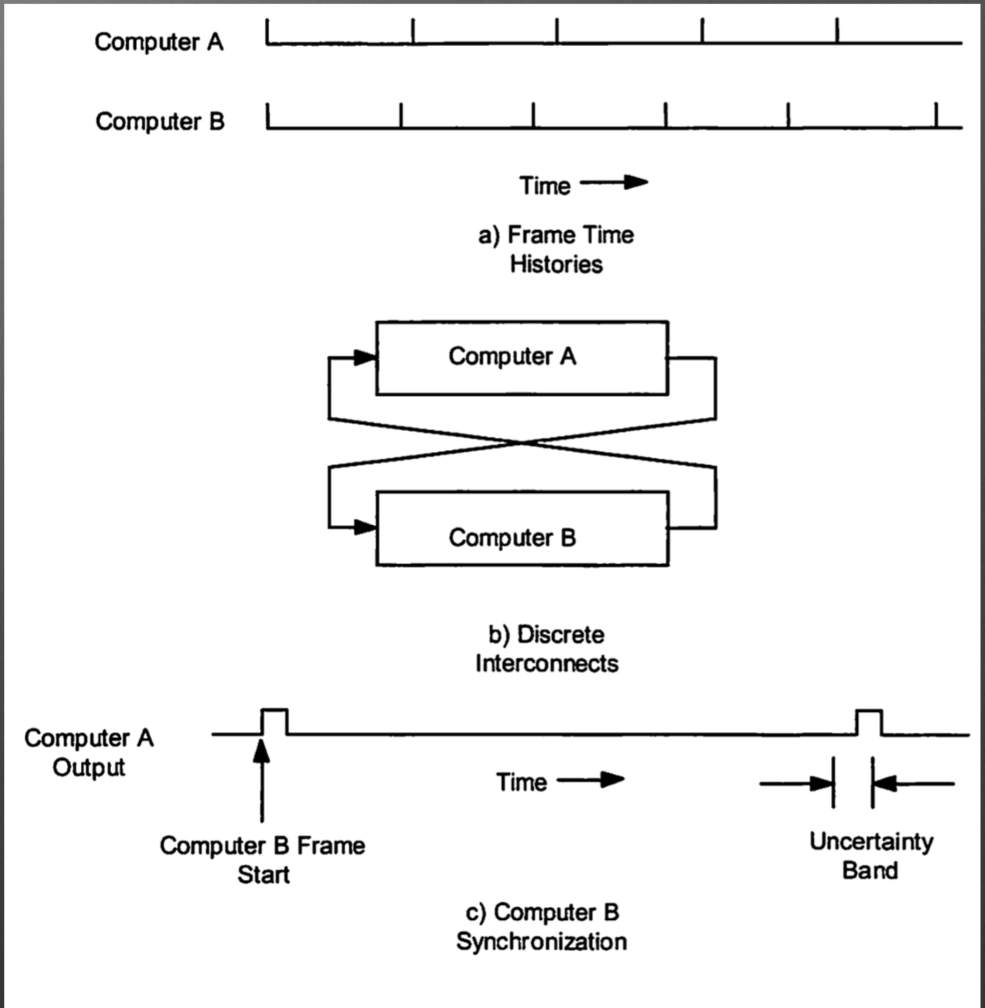


Figure 4.19 Dual Computer Synchronization

4.3.3: Dual Redundancy - Computer Hardware

- Dual redundancy is usually employed where required speed of failure detection exceeds human reaction times.

- Dual-sensor/Dual-Computer architecture eliminates speed and coverage limitations of the simplex system’s failure detection process.

- Two failed components can produce identical but incorrect outputs.

- Dissimilar components can be used to counteract **common-cause hardware failures**.

- Dual redundant architecture eliminates undetectable single-points-of-failure.

4.3.4: Software in the Dual Redundant Hardware System

- Common-cause failures may surface from the use of identical software in dual redundant hardware channels — eroding the safety benefit gained by using redundant hardware.

- Each computer in the dual channel system should be equipped with a separate hardware watchdog timer.

- The use of dissimilar software can be considered when software faults cannot be detected.

4.3.5: Dual Redundancy and Independent External Safety Devices

- Independent external safety devices and safety interlocks should always be employed since faults can still reside in the operational system.

- An emergency stop provision should be incorporated to include unplanned events (earthquakes, fire, etc.)

4.4.1: Reliability Improvements

- Employing higher-grade components and improving reliability will do little to reduce mishap risk to an acceptable level.

- Improvement in Reliability = Increase in Cost

- Employ redundancy when high component reliability is required for functionality.

4.4.2: Quality Measures

- One should, in theory, be able to design software that is fault-free.
- However, it must be assumed that, like hardware, software will contain faults.
- Internal and external safety devices must be employed to protect against them.