ECE544: Fault-Tolerant Computing & Reliability Engineering (Fall 2022)

Homework #1 Solution (65 points)

1. Some systems are designed for reliability, some are designed for availability, and others are designed for safety. Based on your understanding of the three concepts explained in Lecture#1 and their difference, give an example of an application requiring high reliability, one requiring high availability, and one requiring high safety. Please justify your answer.

Solution (18 points, 6 each):

Reliability: the conditional probability that a system performs correctly throughout an interval of time [t0, t], given that it was performing correctly at time t0. Reliability is most often used to characterize systems in which even momentary periods of incorrect performance are unacceptable, or in which it is impossible to repair the system.

Examples of applications requiring high reliability:

- Operation systems in hospitals
- Life support systems, patient health care systems
- DC-AC converter (in aircraft applications)
- Spacecraft, long-term unmanned space mission systems
- Satellite system
- Personal computer
- Onboard computers in satellites
- Radar systems

Availability: the probability that a system is operating correctly at the instant of time t. Availability differs from reliability in that reliability depends on an interval of time whereas availability is taken at an instant of time. A system can be highly available yet experience frequent periods of inoperability as long as the length of each period is extremely short. In other words, the availability of a system depends not only on how frequently it becomes inoperable but also on how quickly it can be repaired.

Examples of applications requiring high availability:

- Banking systems
- Stock exchange systems
- Airline reservation systems
- Telecommunication services
- Mobile networks
- Retail web page
- Customer services

Safety: the probability that a system either performs correctly or discontinues its operations in a "safe" manner, specifically in a manner that does not disrupt the operation of other systems or comprise the safety of any people associated with the system. Safety is a measure of the fail-safe capability of the system; if the system does not operate correctly, you at least want the system to fail in a safe manner.

Examples of applications requiring high safety

- Nuclear power plants
- Electrical outlets in houses
- Railroad / auto traffic control systems

- Medical applications
- Drill press
- Chemical plants
- Elevators
- Missile guidance systems
- Smoke detectors
- Aircraft flight control systems
- Computer storage system (needs to crash safely to save contents stored)

2. Devise an original example (different from the lecture examples) to illustrate the difference between faults, errors, and failures. As you illustrate these concepts, relate them to the three-universe model.

Solution Hints (15 points):

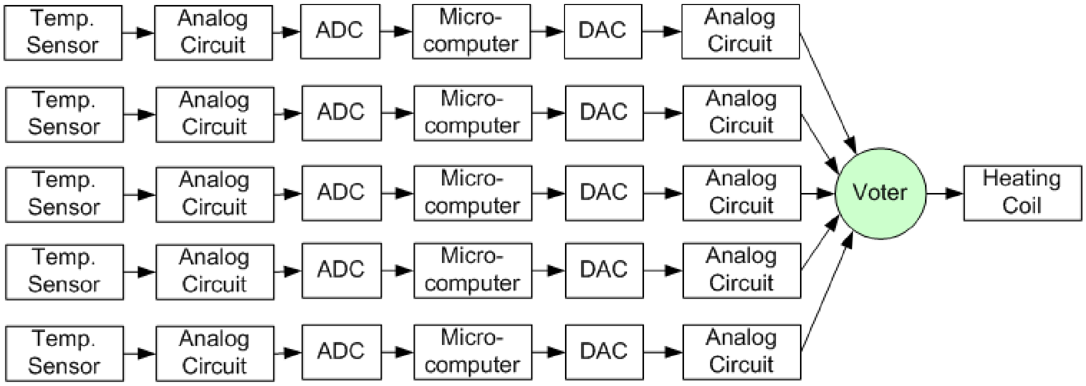
- Program execution: logical error in a line of code
- Sink of Titanic ship
- Damaged temperature sensor inside the car engine
- Printer fails to print documents
- Campus Center Student Package Pick-up
- Broken backpack zipper
- Open circuit in Radar systems
- Damaged gas indicator
- Car timing belt errors
- Watertight seal with a grain of sand
- Columbia space shuttle accident
- Banking transaction systems
- Library systems
- Heart attack of human
- Promotion system in some organization
- Electric power systems
- An ATM with malfunctioning keypad
- Damage on the teeth of the shifting gear of the car

3. The company that you work for is designing an industrial controller that maintains the temperature of a fluid during a chemical reaction. The non-redundant controller contains: (1) temperature sensor; (2) analog circuitry to process the temperature sensor's output signal; (3) analog-to-digital converter (ADC); (4) microprocessor (including hardware and software); (5) digital-to-analog converter (DAC); (6) analog circuitry to process the output of the DAC; and (7) heating coil to control the temperature. You have been asked to develop at least two alternatives for making the controller tolerant of any two faulty components. The term "component" means one of the blocks of functionality listed above, excluding the heating coil. Show block diagrams of your two approaches and compare them qualitatively. Which approach would you recommend for implementation and why?

Solution (32 points; 14 points per design; 4 points for the recommendation):

- **Design 1: passive hardware redundancy technique -- 5MR & variations**

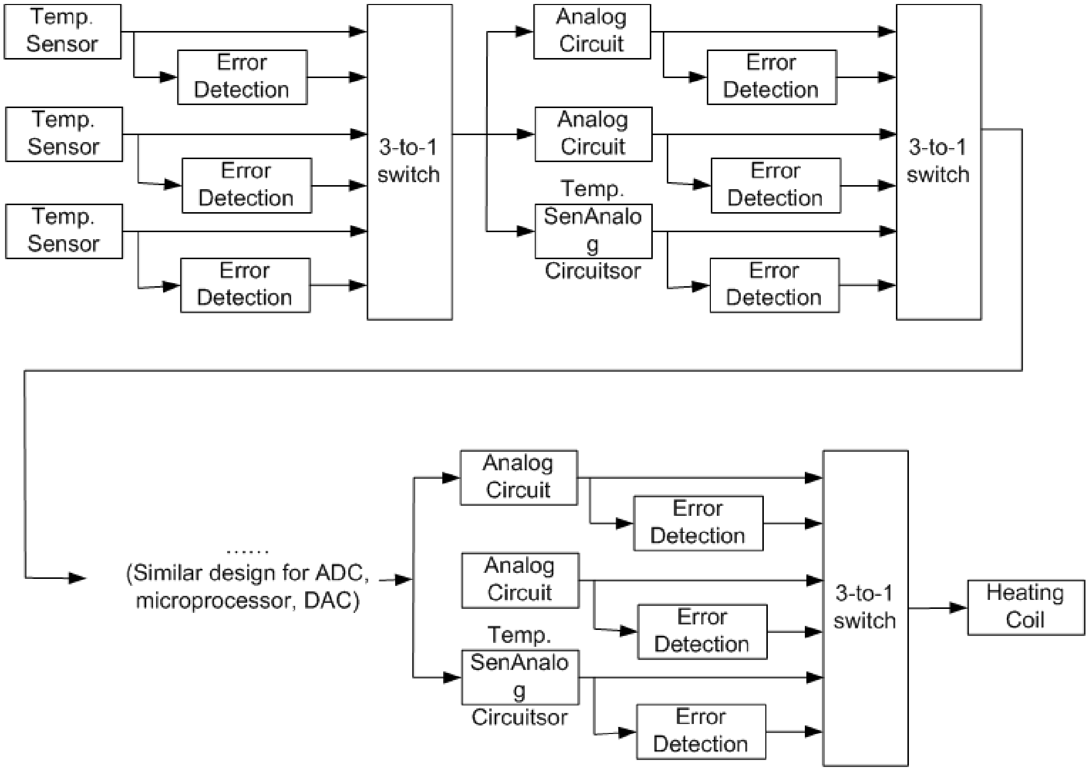
a. Original 5MR:



b. Variation 1: Multi-stage 5MR: perform majority voting after each component/stage, each voter is a single-point-of-failure

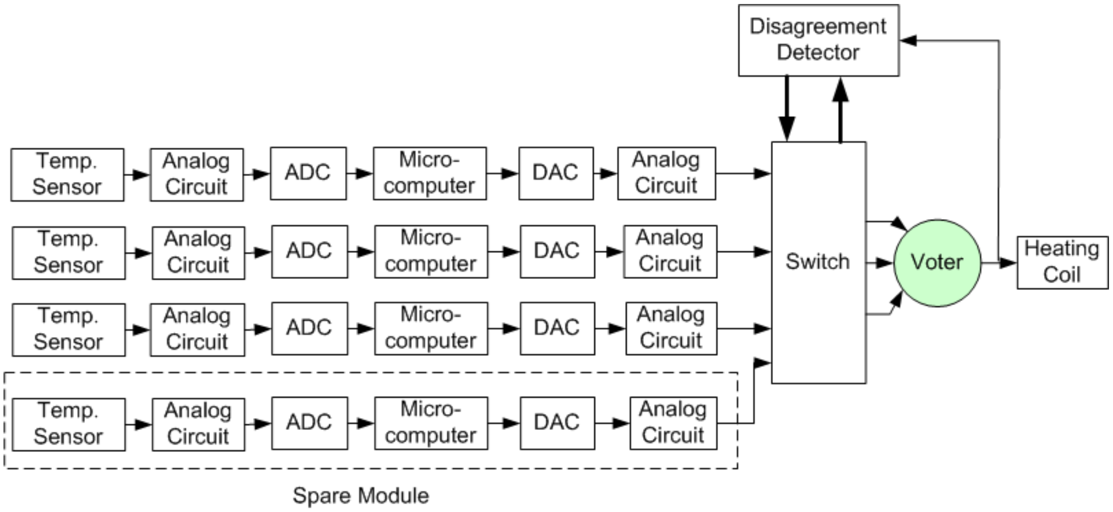
c. Variation 2: Multi-stage 5MR: use five voters at each stage to overcome the single-point-of-failure effect of the voters

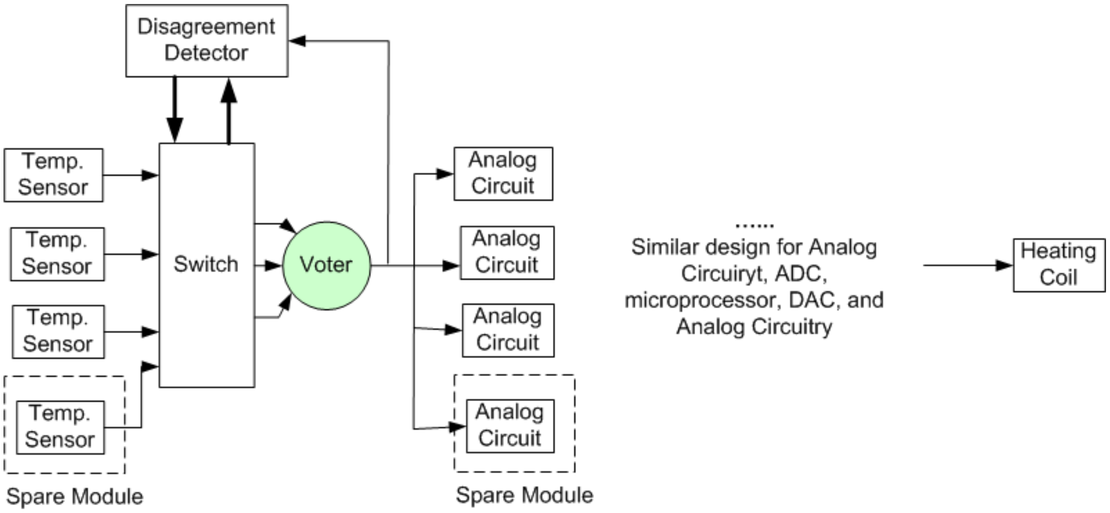
- **Design 2: active hardware redundancy technique – standby sparing**



- **Design 3: hybrid hardware redundancy technique – TMR with 1 spare**

This technique can be applied to all the components as a whole or each individual component:





The selection of the designs should consider the extra redundancy required, the complexity of the circuitry, the fault confinement capability, and the limitations on the system weight, cost, size, and power consumption, and the available resources.