

EECE 692

Practical Design of Safety-computer System

Author William R. Dunn

Chapter 4

Design of Fail-Safe computer System

Present by *kidanmariam Fenta*

Spring 2011



Designing the fail-safe system

- The three mitigation measures has to be taken concurrently,
 1. Incorporate internal safety and warning devices
 2. Incorporate external safety devices
 3. Improve component reliability and quality



Designing the fail-safe system

Fail-Safe

- System as being one that in the event of failure will revert to a **nonoperation state** that will not cause a mishap.
- Able to detect faults or failure and reconfigure itself to the safe state.

Fail Operate

- System must Detect fault or failure and isolate the offending component and reconfigure itself so that safe operation **will continue** with out noticeable operation.



Fail-safe system Design Guidelines

- Inherent fail-safe system-in designing a system using discrete electromechanical (and some electronic) components, it is common practice to select and interconnect the components so that the failure of any component will automatically cause the system to revert to a fail-safe state.
- Fail-safe design approach-is to make hardware and software modification
 1. Detect the presence of faults or occurrence of failure
 2. Upon detecting these failures, reconfigure itself to a safe state.
- Fault categories covered in fail-safe design-how fault associated fault got into the system such as hardware, software ,systematic faults and fault rising from design, installation operation and maintenance etc.



Simplex system

- System that **does not** employ redundancy
- A fail-safe system employing **no redundant components**



Application Failure-

Controlling Application Failures

- **Step1** :define the physical measurements that can be made on the application approaching a failing condition.
- **Step2** :select the appropriate sensors for making these measurements and interfaces them to the computer.
- **Step3** :select effectors that can be commended to eliminate or arrest the conditions leading to the application failure and interface them to the computer.
- **Step4** : design and install software which will continuously monitor output of the sensor selected in STEP #2. if the software detects a fault or onset of failure, it will signal one or more of the effectors selected in STEP#3 to arrest failure onset.



Sensor Failure Detection

- You noted the generate **signal differs** from it would or **supposed to generate** signal if it were failed.



State Estimator

- The foregoing software scheme for detecting sensor failures can be refined considerably by employing a mathematical concept.
- States refer physical parameter such as position, velocity, pressure and temp etc.



Sensor redundancy

- Analytical redundancy
 - Sensors that measure physical parameters which are **different** but are **analytically related** to each other through a common parameter.
 - A position sensor **PH** and its corresponding position rate sensor **RH** are an example of such pair
 - Common parameter is time
 - E.g. RH(10 degrees/second) by 4 second comparing PH is equal to 40 degrees.
- Information redundancy
 - Sensor value can be directly related through **physical laws** to other sensor values.
 - Fig 4.4

Effector Failure Detection

- **Wraparound test-** the instrument the output of the effector and feed it back into the computer where it can read by software. The software then compares actual effector output with what was commanded.
- A commonly employed approach in safety-critical design is to bring effectors to a fail-safe position by simply withdrawing effector power.



Data Communication Failure Detection

- Parity Check-a primary concern in marginal communications is that one or more **bits** in received **group of bits** will have a flipped state wherein "1" becomes "0" or vice versa.
- Checksums
 - E.g Suppose that is desired to transmit the block of integers {23,16,55}. The sum, checksum is **94** so the block plus checksum {23,16,55,**94**}.if this **checksum don't match**, there has been a **failure** somewhere in the system.
- Timeouts – the problem of a CPU to receiving no data due to hardware or software failure.
 - A schedule communication between CPUs such that failure of a CPU to **receive data** within a time window.

•

•

Handling System Power/Interconnect Failure

- Handling power source loss- when power loss the system automatically transition to a safe state.



Operator Failure Detection

the failure associated with human error.



Operator Failure Detection

- Monitoring Failure Detection
 - Perception failure- (hear and see) an output eg. design verbal command
 - Cognition failure - perceiving and understanding it . eg Failure to follow correct operating procedure
 - Decision failures- decide to take appropriate action



External Safety Device and Control

- Are used to in **conjunction** with computer control system and internal safety devices and to provide further risk reduction. eg. Gas station emergency switch
- The purpose is to prevent failures that escapes internal safety devices from causing a mishap.
- Safety interlocks- are commonly used in home appliances: the door switch on the microwave oven and washing machine prevent operation.



Fail-Safe computer systems- simplex Architecture

- Hardware safety features
- Software safety features- this software is supplemented with software functions for **detecting failures** and **safely reconfiguring** the system.
- Maintenance Diagnostics software-provide the operator (or the system peripheral devices) with not only the indication of failure but clues as to their origin.



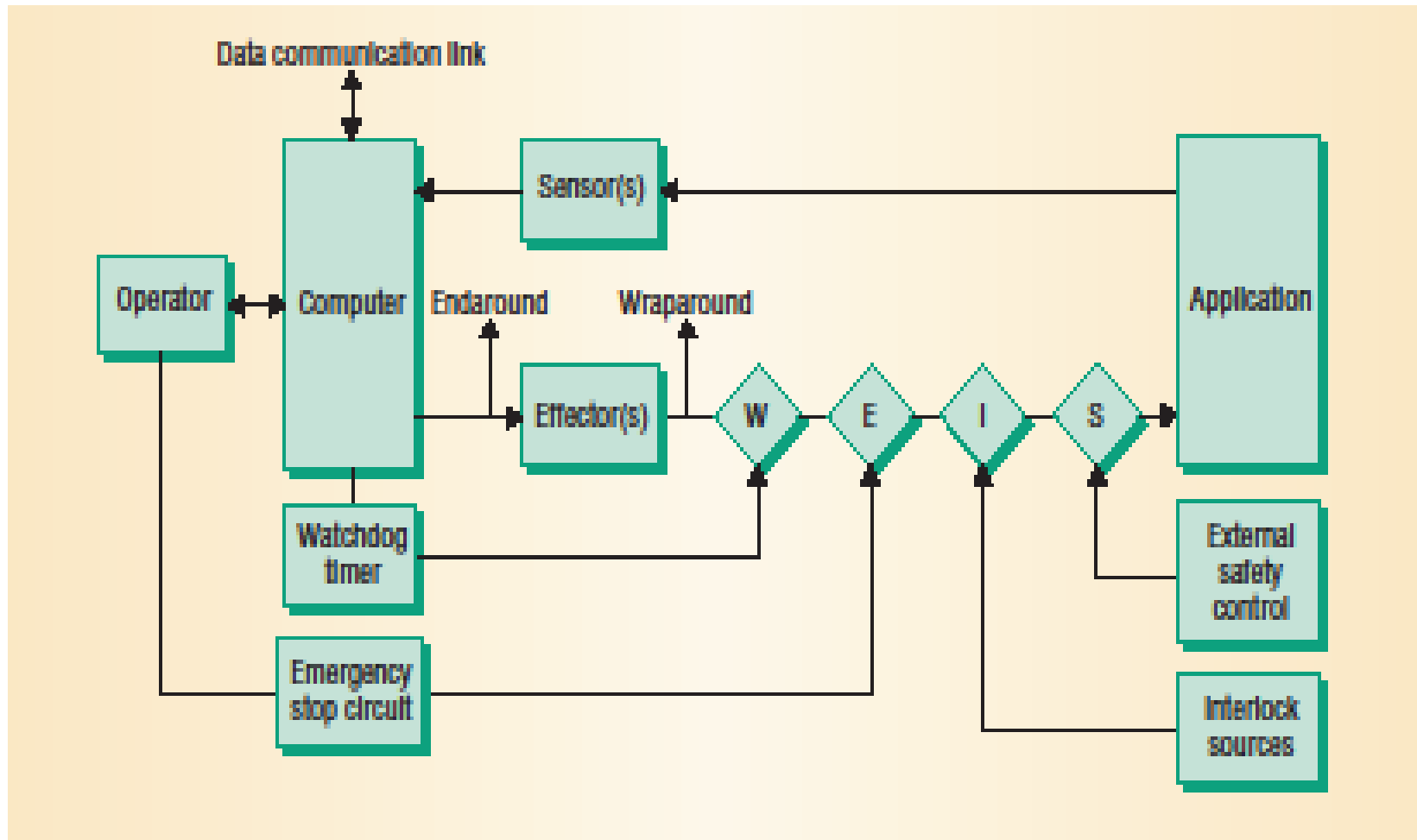


Figure 4.15 Fail Safe computer
System safety Features

Dual Redundant-computer Hardware

- The basic idea behind using **dual computer architecture** is that hardware and software in each of the two computers will **function identically** when there are no failures and will therefore **produce matching** output.
- The primary **goal choosing** a dual redundant architecture is to **eliminate** undetectable **single-points-failure**. Eg. Dual potentiometer ,or dual pressure transducer.



Fail-Safe computer system-Dual Redundant

- Failure detection
- Dual Redundancy
 - Two identical component are employed and run parallel.eg. Sensors if their output match they are assumed to be working correctly ; if they don't match there has been failure.



Reliability and Quality Improvement

- Design Internal and external safety devices to mitigate mishap risk
- Apply quality measures intended to avoid or eliminate faults in the design.



...

Thank You

•

•