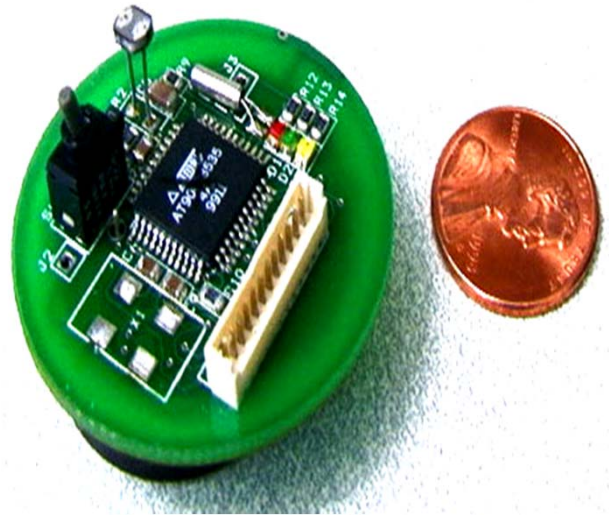
Fail-Safe Computer Systems



Presented by:
Kennteh Booker

EECE499 Computers and Nuclear Energy
Electrical and Computer Engineering
Howard University
Dr. Charles Kim

Summary

Many failure detections fail-safe systems have been proposed for techniques by the use of sensors for the networks of todays technical world. But, considering the resource constraints of sensors and the different ways of detection a good solution should have a overall detection mechanism that can be used in any situation.

Basic Concept

What is a Sensor

- a device that detects/measures a signal or stimulus
- acquires information from the "real world"
- Contains a large number of self-sufficient nodes
- **Input:** stimulus or measurand (temperature pressure, light intensity, etc.)
- **Ouput:** electrical signal (voltage, current frequency, phase, etc.)

Applications for Sensors

Applications

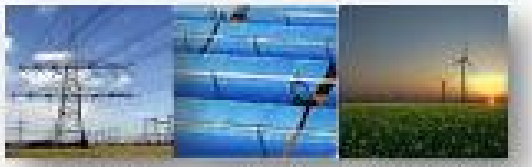
- Environmental
- Military/Industrial
- Commercial

Remote Monitoring

Sustainability

Industrial Measurements

Air/ Climate | Water/ Soil | Indoor Monitoring



Power Quality and Consumption Monitoring | Solar Monitoring | Wind Farm Health

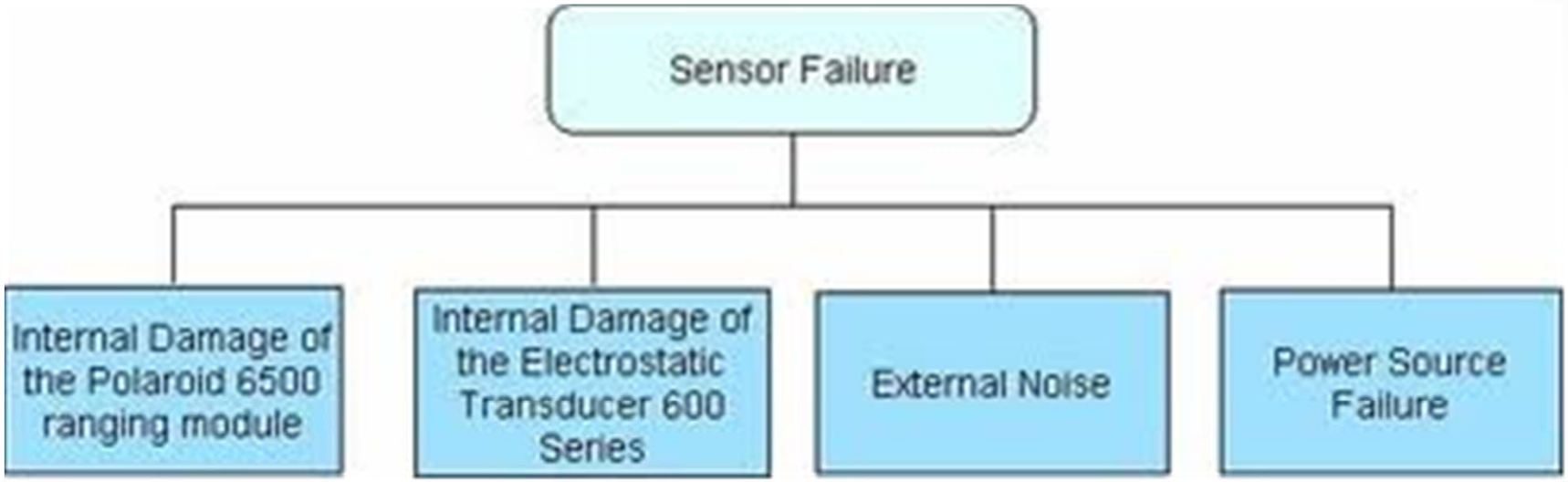
Structural Health Monitoring | Machine Condition Monitoring | Process Monitoring

Problem of Detecting Failures

Movement Assisted Sensor Placement

- In real life, sensors are unable to detect or measure the event's effect below certain threshold. So, diffusion curve has finite tail
  - - Lack of sensitivity of sensor device(s)
- Erroneous reading of malfunctioning sensors
  - - Due to calibration errors or obstacle
    - Cause local maxima or minima
- Environmental noise

Example Chart



Fault Detection

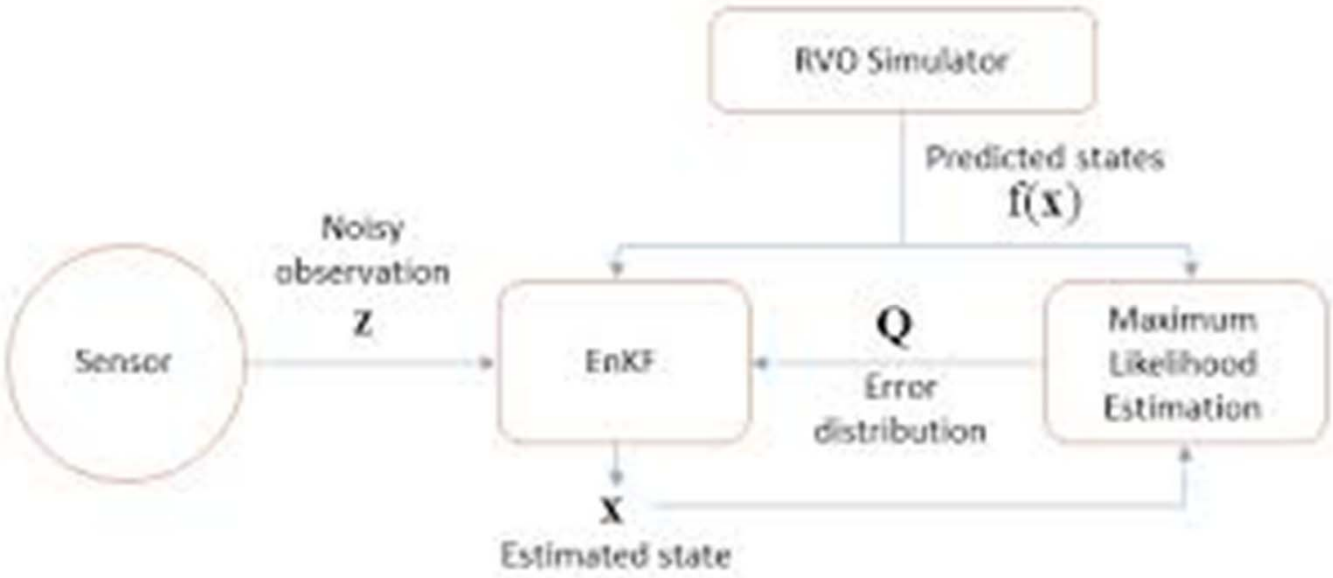
What is a Fault Detection?

There are four types of Faults:

1. Fault in connection between flow and switch
2. Fault within discrrete/digital converter
3. CPU fault
4. Memory Fault
5. Software Fault

What should it have

- Thresholds
- Persistence Counters
- State estimator



Fault Tolerance

- Simplex System : A single fault results in the loss of protection and/or unnecessary shutdown.

- Redundant System : A single fault will result in an immediate alarm but will not result in loss of protection nor in an unnecessary shutdown.

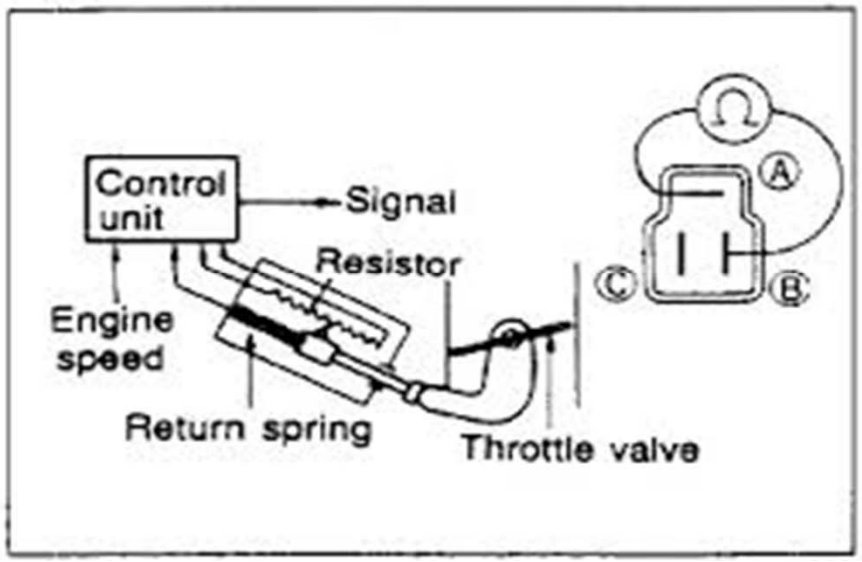
Fault Detection

- **Deviation Alarm**:
  - Value of the sensor is automatically compared with redundant sensors for validity checking.
  - If the difference exceeds a preset tolerance, an alarm is triggered.

- **Diagnostics**:
  - Real-time artificial intelligence that compares current status bits for conformance with pre-defined rules.
  - Alarms are generated whenever the rules are violated.

Effector Failure Detection

- Automatic danger
- Knows response but doesn't follow
- Wraparound Test(Precaution Software)



System Reconfiguration

- Automatic safe state

Detecting Data Com. Failures

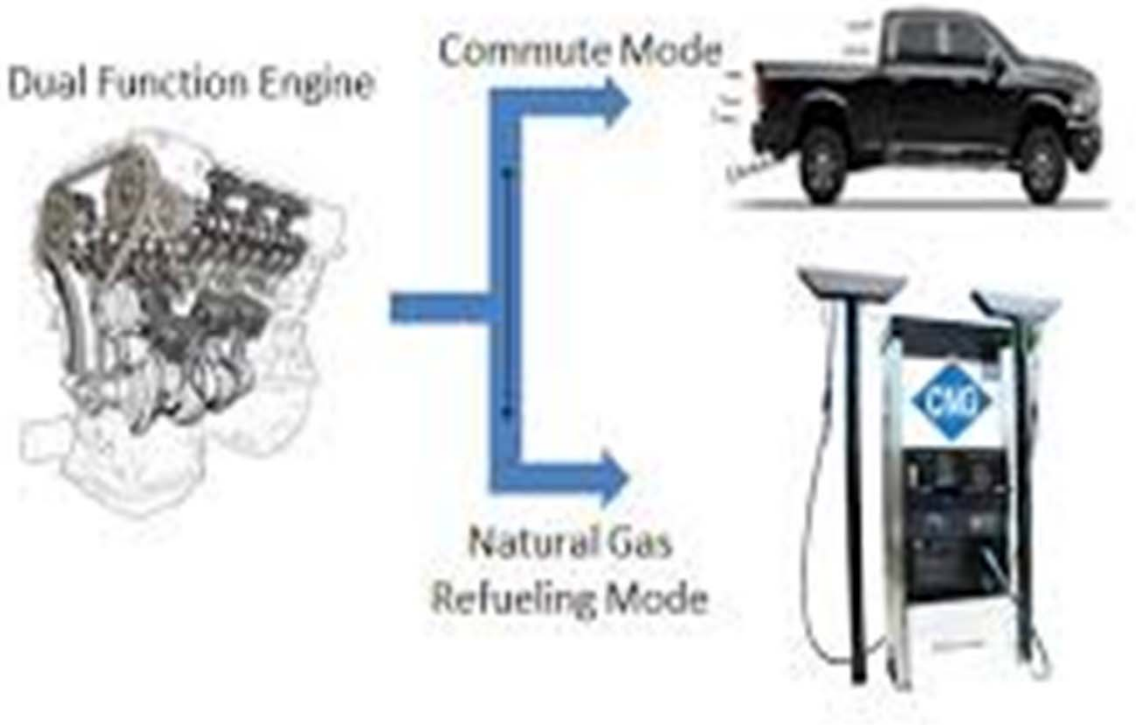
There are three ways of Detecting Communication Failures

- Parity Check
- Check Sums
- Advanced Techniques

1. Timeouts

Handling Power Loss

- Power loss: Electrical, Hydraulic Pneumatic Transient and Power and Signal Inter connect Failure



Prevention Operator Failures

- Cognition
- Decision
- Procedure Fail
- Human Factor
- Control Sequences
- Closed Loop Manual
- Eliminating Errors
- Relocation

Computer Failure Detection

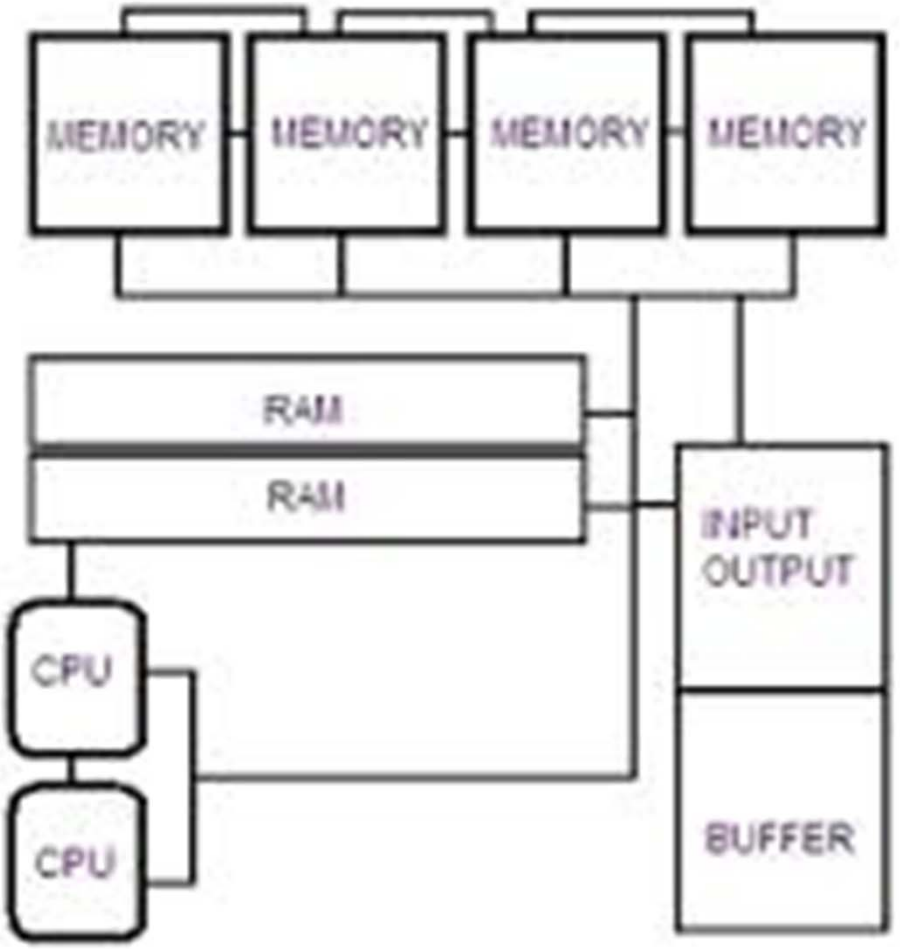
- Detecting Sensor, Effector and Operator Input/Output Device Failure
- Operator I/0 Device Failures
- Detecting Communication Module Failure
- Periphal Units

Wall Street

Computer Failure Detection
(CPU and Memory)

- Self- Tests
- CPU Hardware Diagnostics
- Memory Tests
- Memory Hardware Diagnostics
- Electronic Support/Interface Components
- Clock Failures

Example 1


MEMORY
MEMORY
MEMORY
MEMORY
RAM
RAM
INPUT
OUTPUT
CPU
CPU
BUFFER

External Safety Devices and Controls

- Independence
- Common-Cause Component Failures
- External Safety Device Hierarchy
- Layering of External Safety Devices
- Emergency Stop Circuits
- Safety Interlocks
- Latent faults

Conclusion

There are two main drivers for continuous improvement in the area of Sensor Failure Detection:

- SAFETY.
- RELIABILITY.

Thank You!