Fault Tolerance in Control Systems

PURDUE UNIVERSITY

Overview

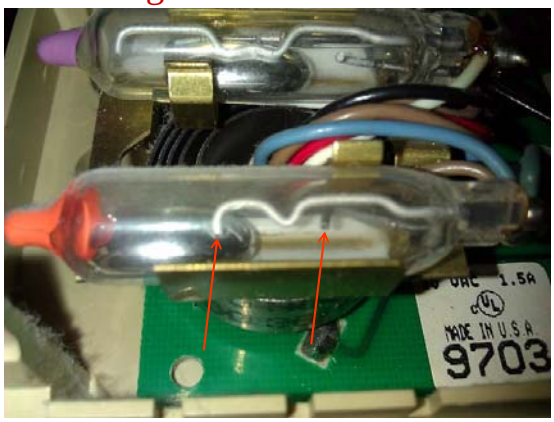
- Basic control hardware
- Operating under fault conditions
- Faults in autonomous systems

- This presentation is an overview of my personal experience in control systems and a survey of some papers

PURDUE UNIVERSITY

Control Hardware Basics

- Control systems, in general, may be analog, switch/relay based, or computer operated, or some mixture of the two
- Analog Control: Thermostat



- The tubes rotate on a metal strip that lengthens/shortens with temperature.
- When the tube's angle makes the mercury connect the probes, the heater turns on
- Setpoint is controlled by rotating the metal strip's base
- All faults in this system are mechanical

Control Hardware Basics

- Sensors measure the process variable (PV) (position, temperature, etc)
- Humans or autonomous systems make set points (SP) for these process variables
- Control variables (CV) can change the process variables (motor, heater, etc)

- Control systems, such as PID loops, measure the PV, compare it to the SP, then adjust the CV
- Faults in all 3 stages, sensing, control processing, and actuation/control may disable the system

Fault Tolerant Sensors

- Triple Modular Redundancy (TMR) approach:
  - 3 sensors inputs are voted on, and if 2 agree there is no fault
- TMR with 2/3 versions:
  - Different manufacturers are used to make the 3 sensors
  - Eliminates some common design problems
- Sensor data fusion:
  - Can fuse information from different sensor types into a common state
  - Norbert Schmitz; Jan Koch; Martin Proetzsch; Karsten Berns; , "Fault-Tolerant 3D Localization for Outdoor Vehicles," *Intelligent Robots and Systems, 2006 IEEE/RSJ International Conference on* , vol., no., pp.941-946, Oct. 2006

PURDUE UNIVERSITY

Sensor Data Fusion

- Sometimes sensors can provide similar information about the same situation
  - Flow rate can be determined by the rate of change in level on a tank
  - Air pressure may give some sense of altitude
  - Accelerometers can provide velocity

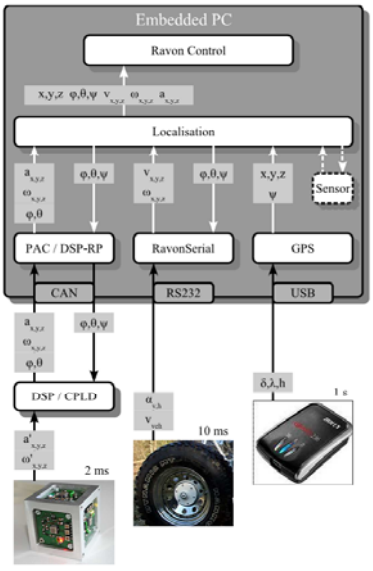
PURDUE UNIVERSITY

Sensor Data Fusion

- One way to improve accuracy is with a state estimation technique
- Kalman filters take a state equation, such as an equation of motion (x=x0+x1*t+x2*t^2/2) and determine the coefficients x0,x1,x2 from repeated processing of measurements (position/velocity/acceleration)
- Multiple sensors can provide inputs to the filter to build this state
- The sensor data fusion will tolerate multiple sensor faults at the cost of accuracy

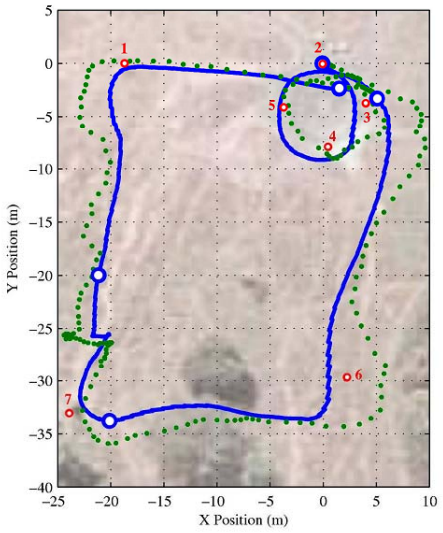
Sensor Data Fusion

- Example: Robot Position
  - Input of Acceleration/ Angle (Gyroscope)
  - Input of velocity from speedometer
  - Input of position from GPS
- Fusion of sensors of different measurement classes



Sensor Data Fusion

- Green dots are GPS indicated position
- Blue line is filter indicated position
- Red dots are obstacles
- Accuracy of the filter based approach is approx. 2m

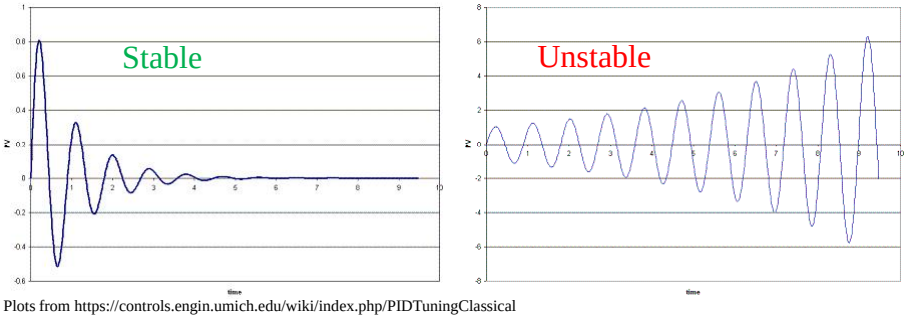


Controllers

- Once the process variable is reliably monitored, a controller can process the input to drive an output
- Programmable logic controllers (PLC's) are usually rugged embedded systems based on ARM or Intel Atom or similar low power, typically fan-less systems
- Deployed systems today may be from the 1970's or 2012

Controllers

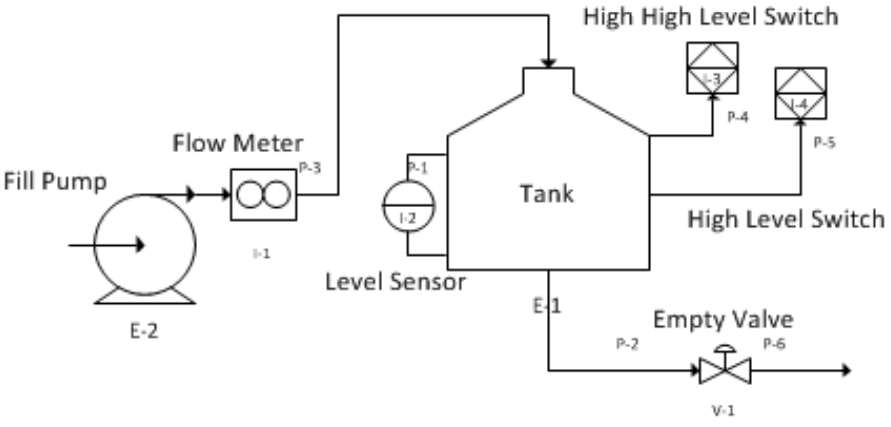
- Digital/PID Control
- Proportional–integral–derivative (PID) loops compare a process variable (temperature) to a set point and provide an output (control variable) that is proportional to the difference in input/set point.



Plots from https://controls.engin.umich.edu/wiki/index.php/PIDTuningClassical

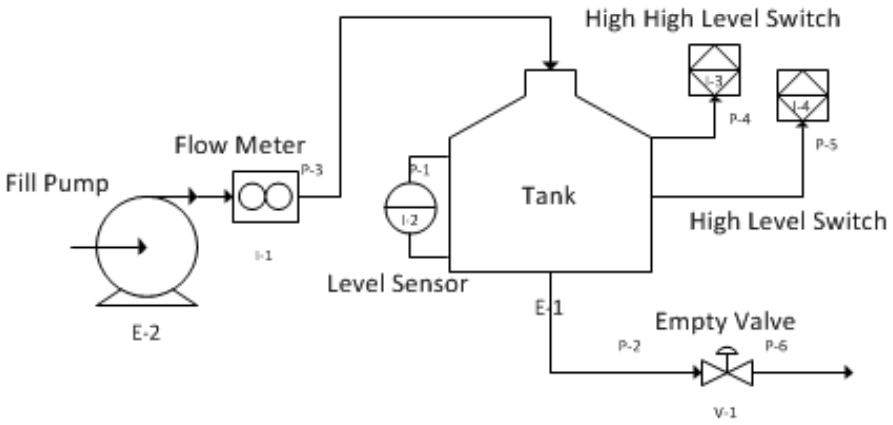
Fault Tolerant Control Loop Example

- PID controller operates the pump to fill the tank
- It has a set point of a full tank and a specified flow



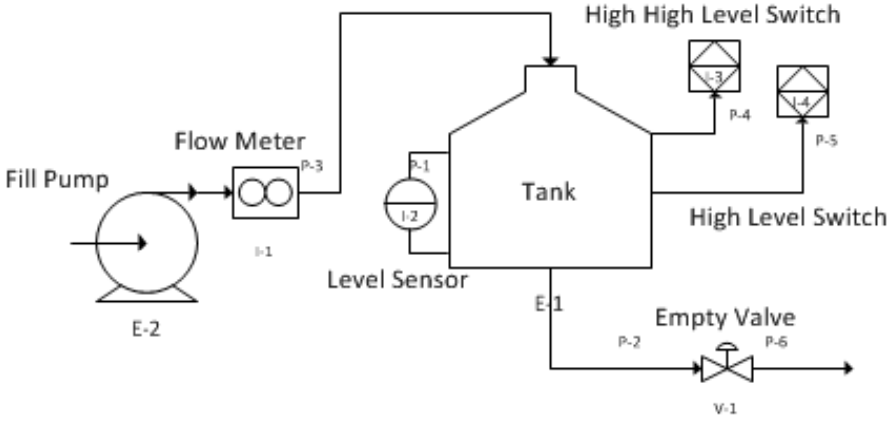
Fault Tolerant Control Loop Example

- The pump speed is the control variable
- The flow meter provides the primary PV to the loop



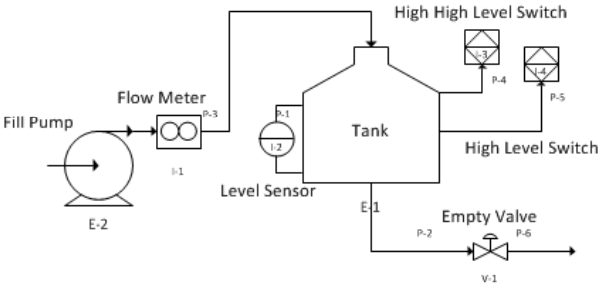
Fault Tolerant Control Loop Example

- The tank level is the secondary PV to the control loop
- If the tank is full, the control system is programmed to stop the pump



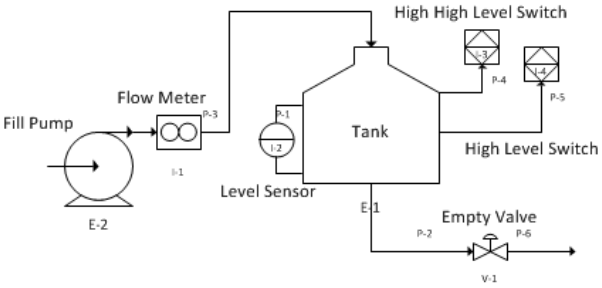
Fault Tolerant Control Loop Example

- Fault: Failed Flow Meter (reads 0 or infinity)
  - Fault can be tolerated by using a differential on the level sensor
- Fault: Level Indicator
  - An integration can be used on the flow meter
  - The level switches can be used to stop the pump when the tank is full



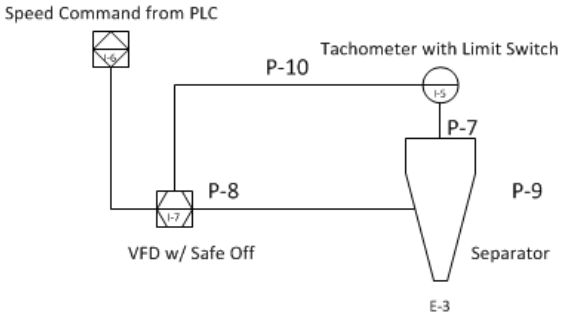
Fault Tolerant Control Loop Example

- Fault: PID loop unstable
  - Min/Max values on the pump speed can keep the process running
  - The PID can be flagged faulty if it never stabilizes and stop the process
  - A static pump speed can be used to safely fill the tank



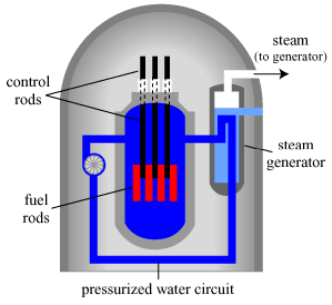
Supervisory Control

- Supervisory control loops can be used to ensure that the process runs safely
- A tachometer can be installed on the centrifuge (encoder) and programmed with a limit switch
- If the RPM is too high, then the motor drive is turned off



Fail Safe Control Variables

- Control rods in a nuclear reactor withdraw to increase power
- The control rods are held in place by an electromagnet
- If the rods do not respond to a control input, then the power to the electromagnets can be cut



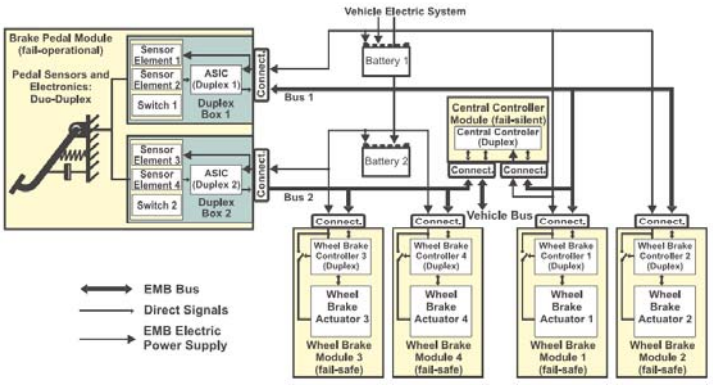
Automotive Drive-by-Wire

- Traditionally mechanical systems in vehicles are being replaced by computer controlled systems
- Examples:
  - Electronic Braking
  - Electronic Throttle Control
  - Electronic Fuel Injection
  - Electronic Ignition

Isermann, R.; Schwarz, R.; Stolzl, S.; , "Fault-tolerant drive-by-wire systems," *Control Systems, IEEE* , vol.22, no.5, pp. 64- 81, Oct 2002

Example: Brake System

- This design for a brake system uses redundant battery systems, brake pedal sensors, and independent (front/rear) wheel brake control



Move to Autonomous Systems

- Now that electronics can control the brakes, throttle, and steering in most modern vehicles, computers can easily replace human drivers as set points
- Existing sensor systems are used to drive the set points for brakes, acceleration, and steering:
  - Sonar and chirp-radar systems for ranging
  - GPS and vision systems for lane tracking
  - Navigation systems for point-to-point path finding

Example Faults in Autonomous Systems

- Airplane autopilot systems are an example of autonomous systems commonly in use today
- GPS/Radar indicated heading and wind speed are controlled by adjusting the rudder/throttle
- Pilots are still there as the backup control system and supervisors

Air France Flight 447

- Airbus A330 has three pilot tubes that indicate air speed (TMR of same-manufacturer)
- The pilot tubes became icy during flight and clogged
- The autopilot lost its PV for airspeed and gave control to the pilots
- The pilots failed to stabilize the plane with the missing airspeed indication (ultimately pilot error)

PURDUE UNIVERSITY

Air France Flight 447

- Airbus recommended the A330 pilot tubes be replaced with at least 2 from a different manufacturer
- Some lessons learned:
  - Avoid TMR with the same manufacturer
  - Human operators may not respond correctly to faulty situations, especially if the operator relies on the same process variable for control
  - Consider new ways (such as sensor fusion) to provide more redundancy in the process variables
  - Evaluate an autonomous supervisor for the human instead of the other way around

PURDUE UNIVERSITY

Conclusion

- Control systems can be designed to be fault tolerant at the component levels in ways similar to fault tolerance for software systems
- As systems become more autonomous, the human operator's ability to respond to fault scenarios may degrade