Risk and Designing Against Failure

Risk

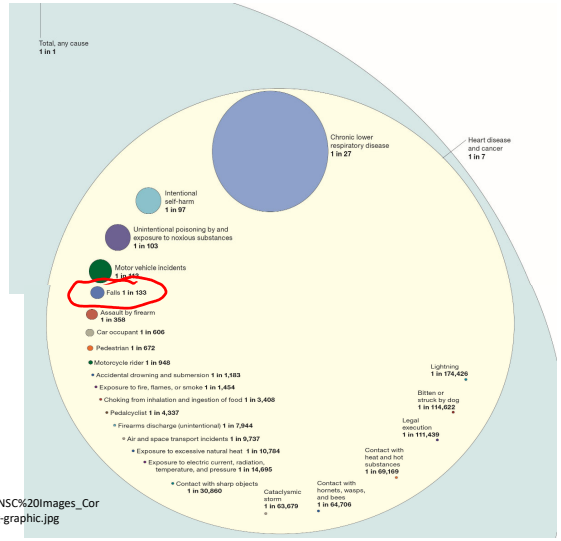
- = Severity x Occurrence
- Severity = Hazard Level – well understood
- Occurrence = Probability it will happen – not well understood; rely on history of same and similar devices/systems and on expert opinion.

Avalanche Risk: Rutschblock Test

- Image Credits : https://vimeo.com/28912198 Bruce Jamieson

Avalanche Risk

- Probable Cause of Dying (US 2016)

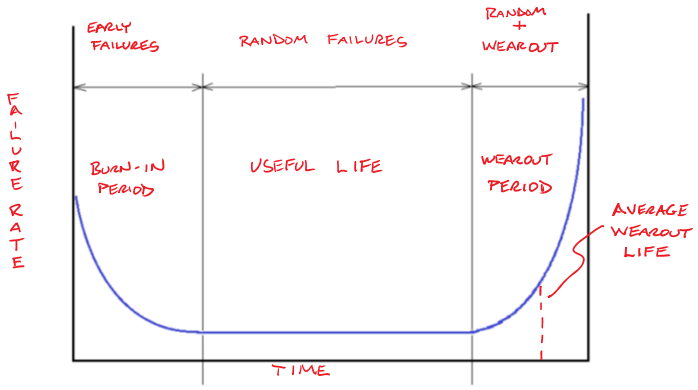


http://www.nsc.org/NSC%20Images_Corporate/odds-of-dying-graphic.jpg

Options for Handling Risk

- Share
  - out-source some design responsibility to other experts
- Mitigate
  - features that reduce severity, occurrence, detection ratings
- Avoid
  - lower risk substitute;
  - fail safes, inherently safe designs
- Retain
  - Accept (benefit outweighs risk)
- Transfer
  - Follow codes, standards
  - insurance (general liability, professional errors and omissions, limited project liability)

Failure and Reliability: Bathtub Curve

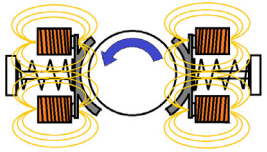


Failsafe Mechanisms

- Elevator hoisting mechanism
  - Relies on cable tension to disengage brake – if cable fails (tension is too low indicating a break or insufficient resistance), brake comes on and stops carriage

Failsafe on Machine Tool: Passive Electro-magnetic Brake

- Power Off – brake shoes applied by springs- spindle can't turn



- Power On – electromagnets on - brake shoes retracted against springs by - spindle is free to turn.

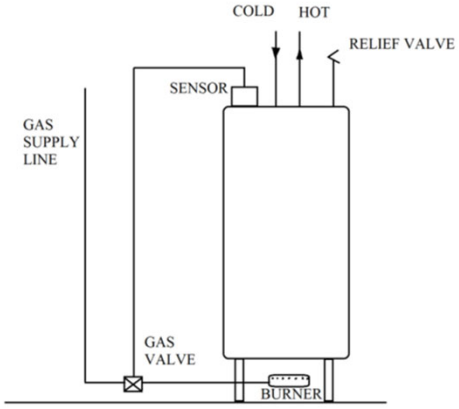
Machine can operate only if power to the brake is enabled. Opening the brake circuit causes the machine to stop.

Exploding Hot Water Tank

- https://www.youtube.com/watch?v=fUkjXGfCLIM&index=5&list=PL_OdYrUmrPWUuDd5vuxQ-Hj9TegVGv5AY

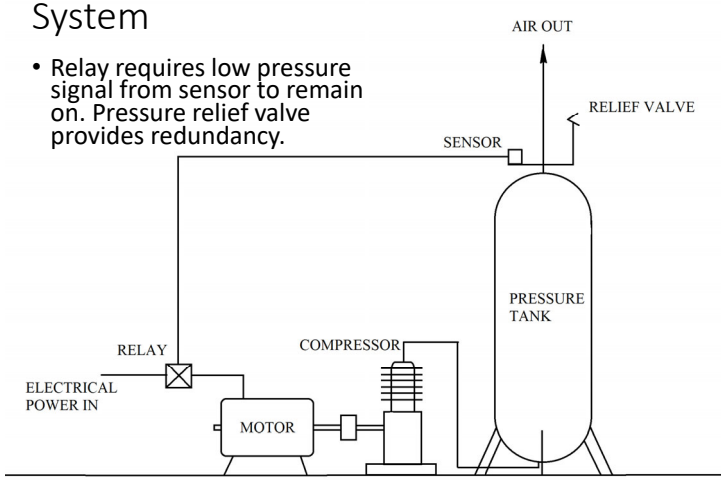
Hot Water Tank Failsafe

- Burner gas controlled by valve. Sensor indicating low pressure = valve open.
- Pressure relief valve provides redundancy.



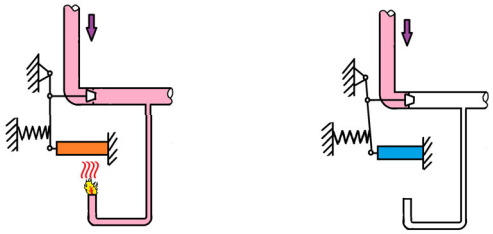
Failsafe in a Compressed Air Supply System

- Relay requires low pressure signal from sensor to remain on. Pressure relief valve provides redundancy.



Gas- Fired Device Mechanical Pilot Light Valve

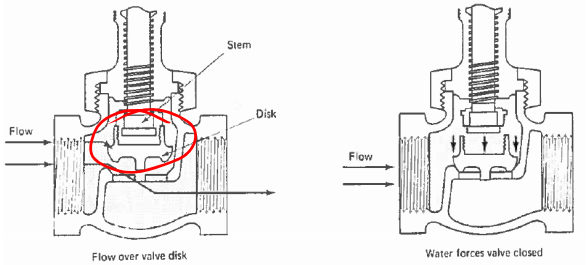
- Pilot light is used to ignite the main burner of a furnace, stove, etc.
- Heat from the flame keeps the valve open; if the flame goes out, the valve automatically closes



Gas Explosion

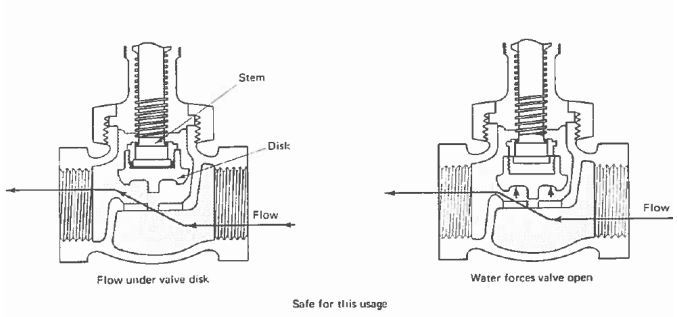
http://www.thetimes.co.uk/tto/news/uk/article3996271.ece

Failsafe may occur if device is implemented correctly: Boiler Throttling Valve



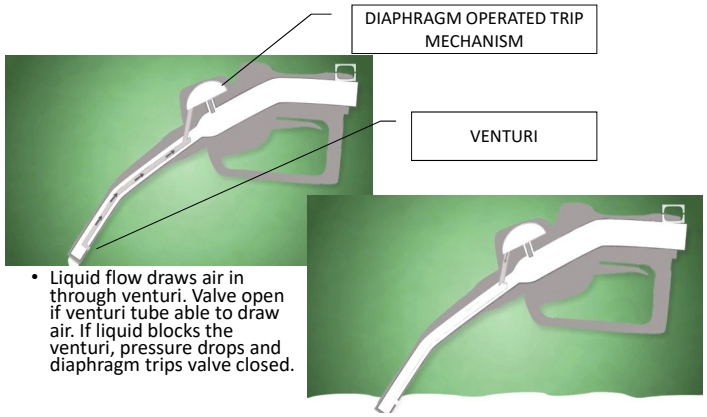
- Incorrect: Unsafe Flow Direction

Opposite Flow Direction Is Safer :



Self- Regulating Devices

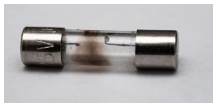
- Gas filler nozzle automatic shut-off



- Liquid flow draws air in through venturi. Valve open if venturi tube able to draw air. If liquid blocks the venturi, pressure drops and diaphragm trips valve closed.

Protection Devices: Electrical Fuses and Breakers

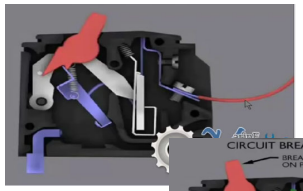
Fuses



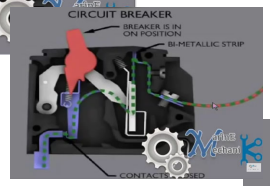
Wire element melts due to excess current

- Must be replaced with new fuse
- fast acting: momentary current (milliseconds)
- slow-blow: permits start-up inrush current spikes but triggers on longer duration high current flows

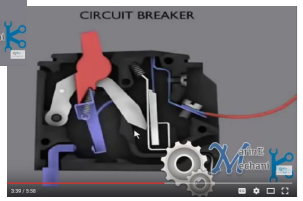
Circuit Breaker



Off – no current flow



On – current flow through contacts



Trip: change in dimension of metallic element latches in the open position

GFCI (Ground Fault Circuit Interrupt) Breaker

- additional sensing circuit monitors fault to ground

AFCI (Arc Fault Circuit Interrupt) Breaker

- additional sensing circuit monitors arcing contacts

http://diy.stackexchange.com/questions/33231/should-i-use-a-gfci-or-afci-circuit-breaker-with-knob-and-tube-wiring

Thermal Protection

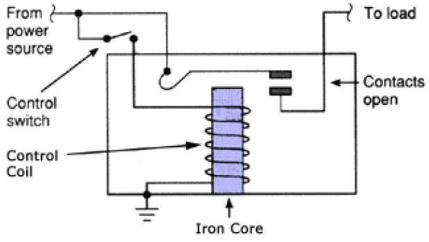
- Thermal Cut-outs
  - Fuse style
    - single use; must be replaced

http://electronics.stackexchange.com/questions/45422/do-thermal-cutoff-switches-exist-for-temperatures-below-50-c

  - Switch style
    - re-setting; trip circuit needed

https://en.wikipedia.org/wiki/Thermal_cutoff

Relays



http://relays.weebly.com/how-relays-work.html

- Multi contact relay
  - Permits sensing circuit to monitor state of relay – can detect failed relay (contacts welded together is common failure mode)
- Magnetic latching relay
  - Current must be maintained to keep relay on – once off, a deliberate action is required to re-enable the circuit

Fire Sprinklers

- Temperature sensitive component in tension or compression is holding back water pressure. If the component melts/collapses, the valve opens.
- Bismuth metal alloys are commonly used (mixture of bismuth, lead, indium and tin) as they can have melt temperatures as low as 47° C

https://commons.wikimedia.org/wiki/File:Fire_sprinkler_roof_mount_side_view.jpg

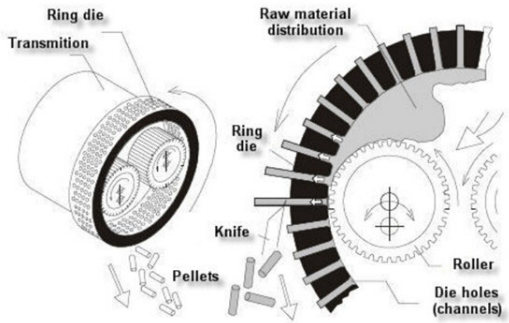
Some Design Approaches to Deal With Failure

For Systems Relying on Signals

- *Keep running until you get a stop signal*
  - E.g. sense the bad situation, then activate a stop - generally not the best approach for critical applications
- Absence of a signal – good
- Absence of the correct signal – better
- Absence of the correct signal at the expected time – even better

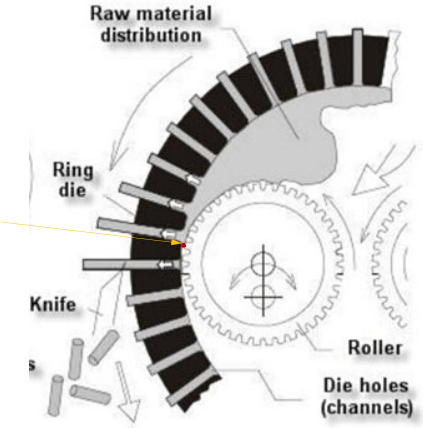
Avoiding Failure in Machine Design: Nominal versus Worst Case Loading

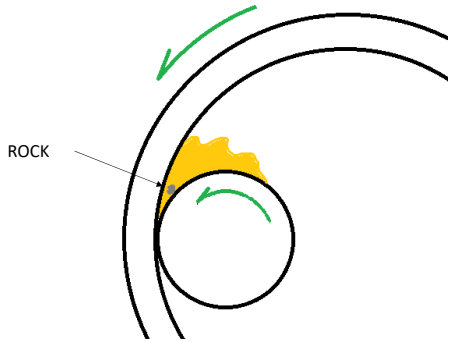
- Biomass pelleting machine



Designs and operating principles of pellet mills-Ring die pellet mill

Nominal versus Worst Case Loading





Monitoring for Failure: Signs of Failure Mechanisms

- **Corrosion** produces signs of deterioration and metal oxides or rust.
- **Erosion** typically produces some form of debris resulting from thinning. In the case of an internally lubricated device, the deteriorated material will be apparent during oil analysis.
- While the cracks that result from **fatigue** are not apparent until a significant number of cycles are complete, the presence of fatigue causing stresses might be made apparent from vibration or displacement (bending) of components.
- **Overload** also frequently has some physical signs of its presence. Sagging or bending for supporting elements, overheating of load-bearing elements or accelerated deterioration of loaded components are signs that a component is overloaded.

Good Practices (source: Daniel Daley, P.E., CMRP , Continuing Education and Development, Inc. , NY

- 1. Keep metals isolated from others that are more or less chemically active. Avoid creating corrosion cells.
- 2. Provide protection where forms of erosion are possible.
- 3. Where movement of vibration can be present, be careful to avoid situations that might allow rubbing. Use non-metallic grommets to shield electrical conductors passing through holes in bulkheads.
- 4. Where movement of vibration can be present, provide supports or bracing that will limit movement and prevent fatigue.
- 5. In situations where the protection afforded by enclosures depends on seals that deteriorate with age or wear, be sure that those seals are properly maintained.
- 6. Provide capacity or capabilities in systems for loading at worst-case conditions. When providing a safety factor in the design, the safety factor should not be provided only to handle unusual but expected loadings. All expected loadings should be handled within normal design tolerances and the safety factor should go beyond those limits.
- 7. When producing a “fleet” or a number of items using the same design, construct one or more “rabbit” units using the same manufacturing processes that are intended to be used on all the units to follow. Closely review the completed “rabbit” units to identify any shortcomings that exist within the assembly process. Test the “rabbit” units using extreme conditions that the units may experience during actual use. If leaks, vibrations, rubbing or any number of undesired effects are noticed, correct the problem on the “rabbit” and alter the manufacturing process to address the problems.
- 8. Maintain the systems of prevention rather than deterioration to the asset. When a form of needed prevention is no longer effective and deterioration to the asset must be maintained, the likelihood of failure and costs of maintenance will increase dramatically.

For your projects:

- Identify places in your design if and where fail-safes or redundancy should be used.
- Identify worst-case scenarios for each sub system
- Identify potential solutions
- For each solution, indicate impacts on performance and compliance with requirements