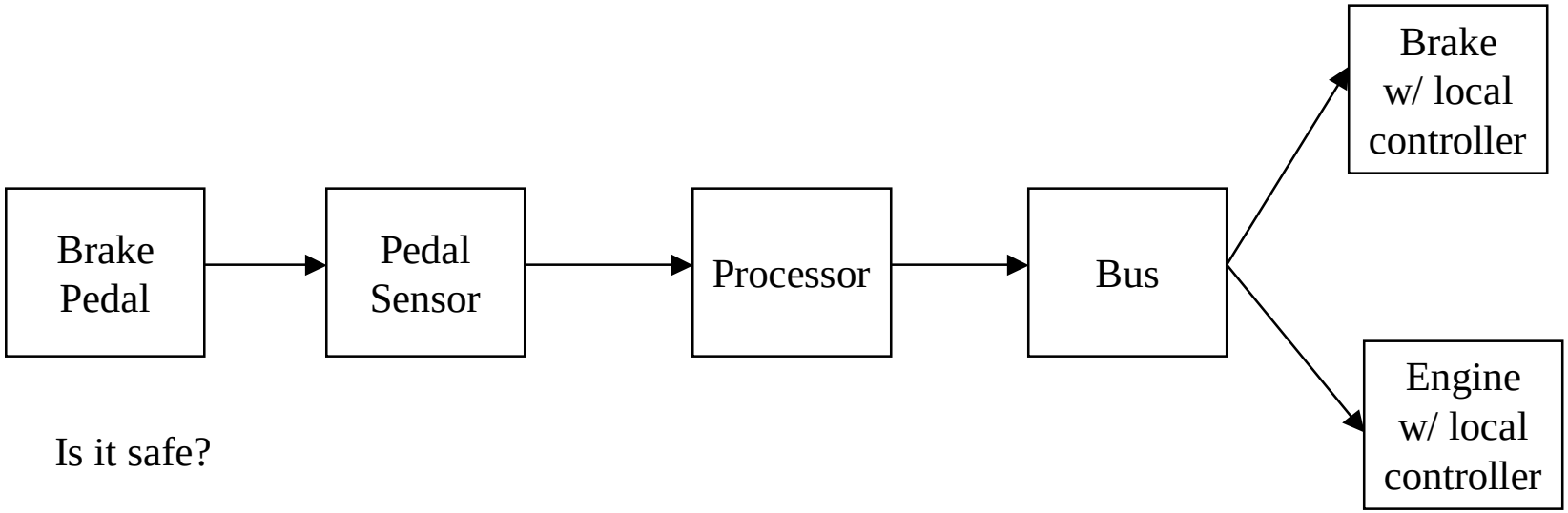
Safety

- Terms and Concepts
- Safety Architectures
- Safe Design Process
- Software Specific Stuff
- Sources

  Hard Time by Bruce Powell Douglass, which references *Safeware* by Nancy Leveson

What is a Safe System?



Is it safe?

Add
electronic watch dog
between brake and bus

What does “safe” mean?

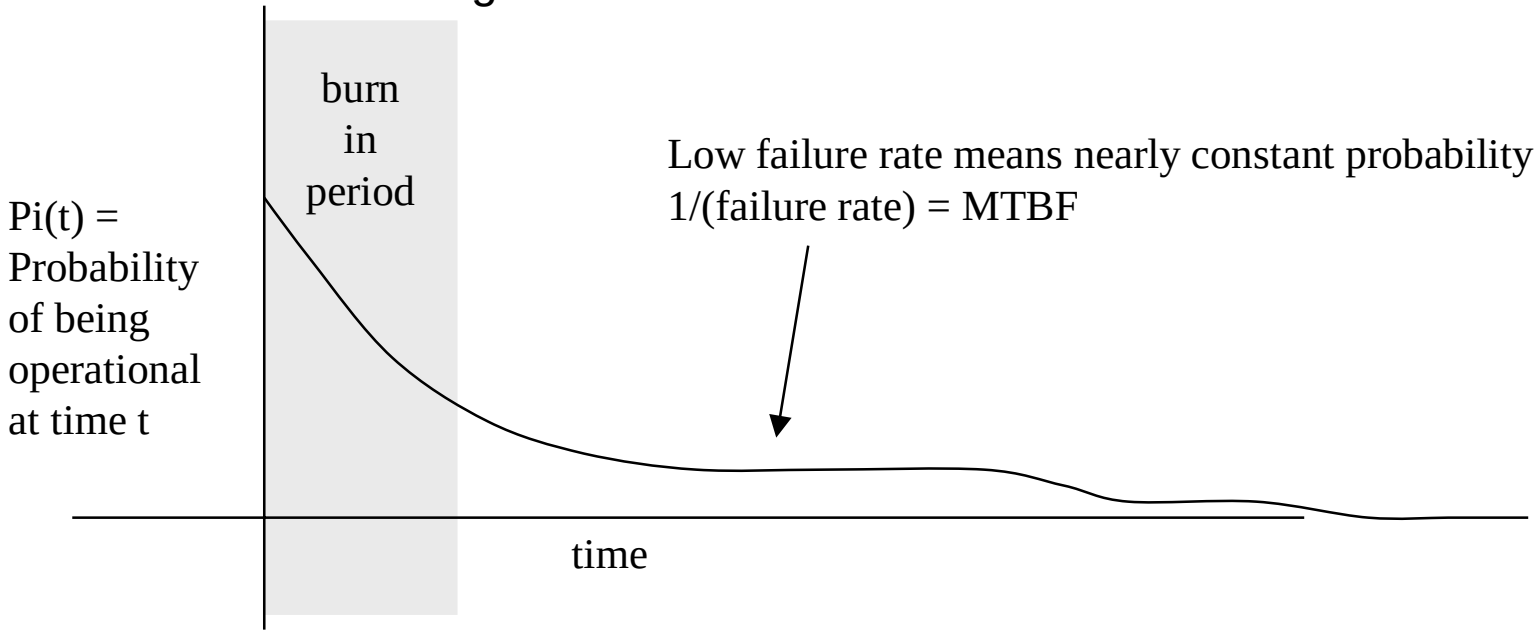
Add mechanical linkage
from separate brake pedal
directly to brake

Add a third mechanical linkage….

How can we make it safe?

Terms and Concepts

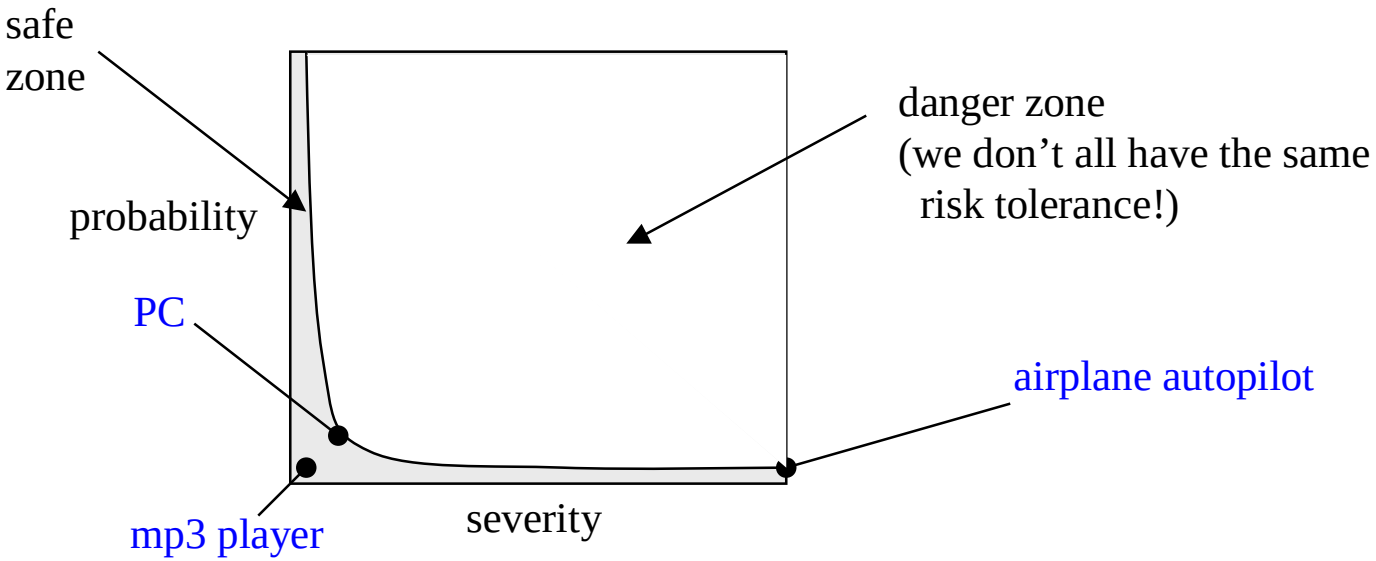
- **Reliability** of component i can be expressed as the probability that component i is still functioning at some time t.



- Is system reliability $P_s(t) = \Pi P_i(t)$?
- Assuming that all components have the same component reliability, Is a system w/ fewer components always more reliable ?
- Does component failure system failure ?

A Safety System

- A system is **safe** if it's deployment involves assuming an *acceptable* amount of risk…acceptable to whom?
- Risk factors
  - Probability of something bad happing
  - Consequences of something bad happening (Severity)
- Example
  - Airplane Travel – high severity, low probability
  - Electric shock from battery powered devices – hi probability, low severity



More Precise Terminology

- **Accident or Mishap**: (unintended) Damage to property or harm to persons. Economic impact of failure to meet warranted performance is outside of the scope of safety.
- **Hazard**: A state of the the system that will inevitably lead to an accident or mishap
  - Release of Energy
  - Release of Toxins
  - Interference with life support functions
  - Supplying misleading information to safety personnel or control systems. This is the desktop PC nightmare scenario. Bad information
  - Failure to alarm when hazardous conditions exist

Faults

- **A fault** is an “unsatisfactory system condition or state”. A fault is not necessarily a hazard. In fact, assessments of safety are based on the notion of *fault tolerance*.
- **Systemic** faults

  Design Errors (includes process errors such as failure to test or failure to apply a safety design process)

  Faults due to software bugs are systemic

  Security breech
- **Random** Faults

  Random events that can cause permanent or temporary damage to the system. Includes EMI and radiation, component failure, power supply problems, wear and tear.

Component v. System

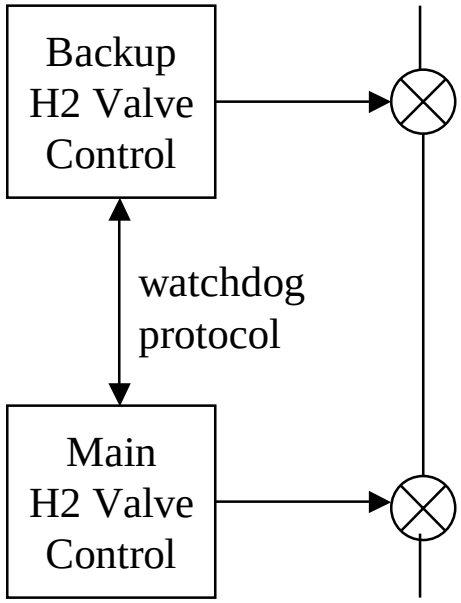
- Reliability is a component issue
- **Safety** and **Availability** are system issues
- A system can be safe even if it is unreliable!
- If a system has lots of redundancy the likelihood of a component failure (a fault) increases, but so may increase the safety and availability of that system.
- Safety and Availability are different and sometimes at odds. Safety may require the shutdown of a system that may still be able to perform its function.

  A backup system that can fully operate a nuclear power plant might always shut it down in the event of failure of the primary system.

  The plant could remain available, but it is unsafe to continue operation

Single Fault Tolerance (for safety)

- The existence of any single fault does not result in a hazard
- Single fault tolerant systems are generally considered to be safe, but more stringent requirements may apply to high risk cases…airplanes, power plants, etc.



If the handshake fails, then either one or both can shut off the gas supply. Is this a single fault tolerant system?