Safety and Risk

Engineer's Concern for Safety

- We demand safe products

  ...but we have to pay for safety

  (important for the public to know this)
- What may be safe enough for you, may not be for others
- Absolute safety is neither attainable nor affordable
- Example: SanFrancisco earthquake...
- What exactly do we mean by "safety"?
- How do we assess it? Earlier capabilities approach of Amartya Sen

Safety…

- Safety, definitions:
  - "A thing is safe if, were its risks fully known, those risks would be judged acceptable by a reasonable person in light of their settled value principles" Safety is relative!
  - "A thing is safe (to a certain degree) with respect to a given person or group at a given time if, were they fully aware of its risks they would judge those risks to be acceptable (to a certain degree)." What is "degree"?
- Relative safety, examples:
  - Safety for an engineering prototype vs. a released product
  - Safety on a manufacturing line (traditions, laws, standards, etc.). *You may encounter this!*

Risk

- Definition: A risk is the potential that something unwanted and harmful may occur
- "Experimental" risks associated with introducing new technology ("social experimentation")
- Example: Toyota Prius/deaf people problem unforseen?, exposes environment-safety trade-off
- Risks with application of familiar technology
- Example: ABS rear-end collisions
- Remaining risk resulting from trying to make a system more safe

Acceptability of Risk

- Willingness to be subjected to risk:
  - People don't have as much of a problem with subjecting themselves to risks
  - Much less willing to involuntarily be subjected to risks
- Are risks on-the-job voluntary? What about in a manufacturing job?
  - Could quit! But is this always possible?
  - If piece-work-based, will workers behave less safely?
- Safety complaints from on-the-job should always be listened to.

Magnitude and Proximity of Risk

- What if personal connections with victims?
  - What if the person on the unsafe manufacturing line is your mother?
  - What if you definitely know that the "public" will immediately include your spouse and children?
  - A useful mental exercise to ensure that you are diligent!
- What creates such changed perceptions?
  - Personal/family relationships, sense of "solidarity" with workers
  - Proximity/magnitude - direct impact on you!
- What about work on a design project?
  - If risk appears small but there are hints that it may grow with time, BE CAREFUL!!
  - Example: Challenger disaster

Lessons for the Engineer

- Problems with the public's conception of safety:
  - Over-optimistic with regard to familiar products that have not hurt them before and that they have control over
  - Over-pessimism when accidents kill or maim large numbers or harm those we know (e.g., aircraft crashes)
  - Statistically speaking, the real risk may be quite small

Design Considerations, Risk

- Principles:
  - Absolute safety is not attainable
  - Improvements in safety often cost $$
  - Products that are not safe incur secondary costs:
    - Loss of customer goodwill and/or customers
    - Warranty expenses
    - Litigation
    - Business failure? Loss of your professional employees? Bad climate/hiring potential?

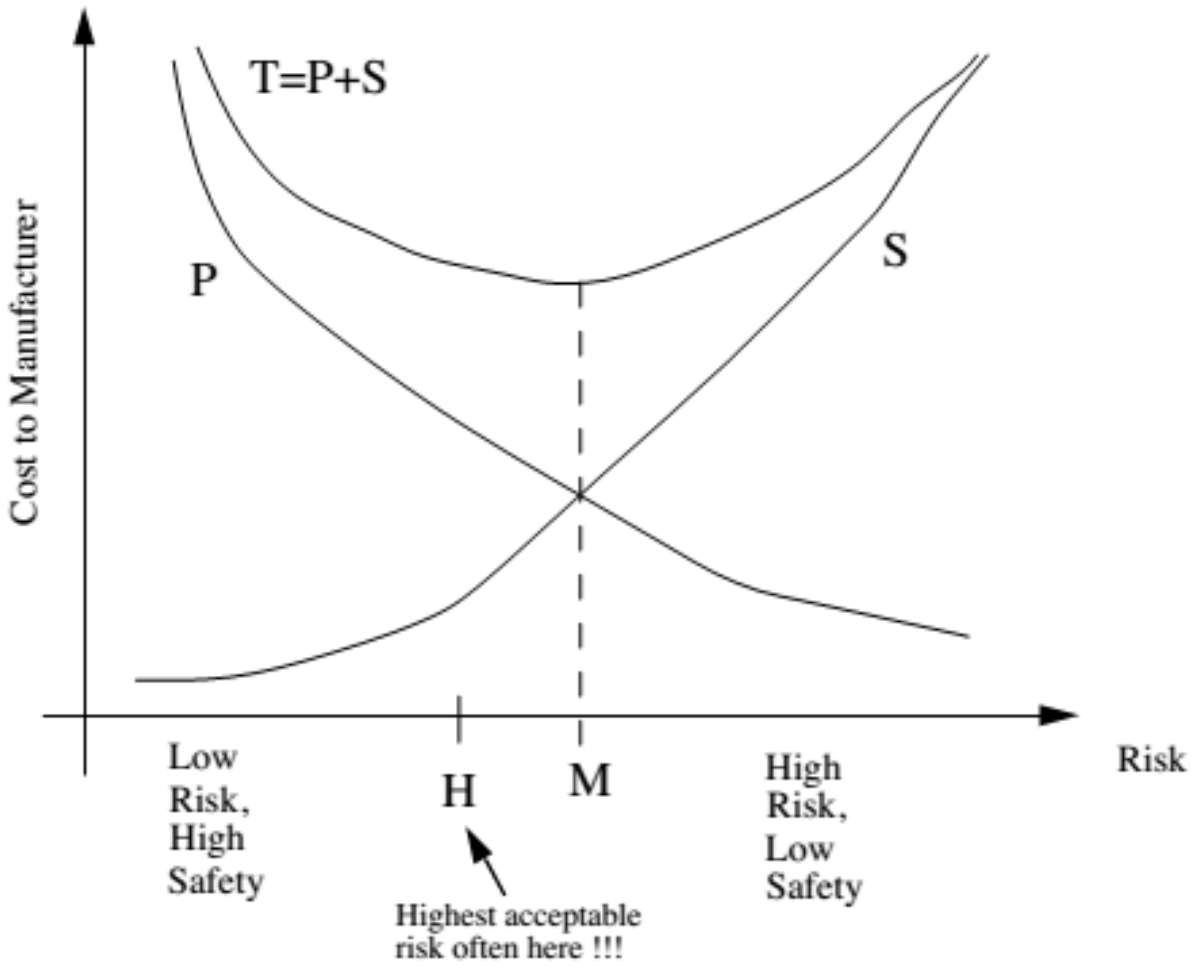
Design principle, risk/trade-offs

How safe should we make a product?

There are trade-offs...

P = primary cost of a product (including safety measures)

S = secondary costs



Ethical issues!

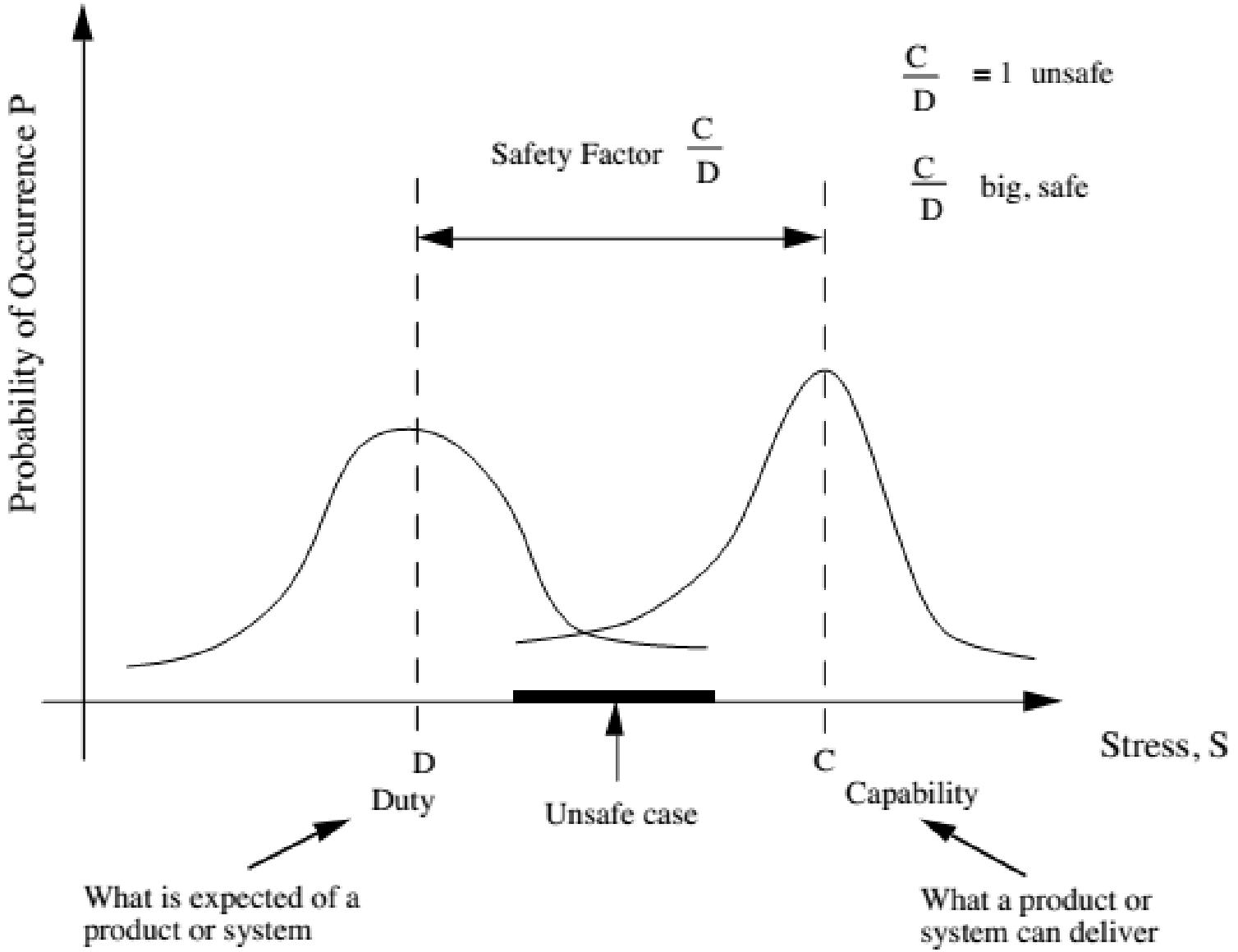
Knowledge of Risk

- Safety issues, even for standard products, are often not well understood
  - Information is often not shared between industries, or even engineers in an organization
  - Always new application of old technology so we do not know what our products will encounter.
- Uncertainties in design cause risk
- Engineers use "safety factors" in design

Uncertainties in design...

- Examples:
  - Uncertainties in materials (e.g., what does the silver or gold band on a resistor mean?). Supplier's data based on statistical averages? What is the underlying probability density function?
  - Designs that do well under static loads often do not do well under dynamic loads

Design Principle: Safe if Capability Exceeds Duty



Do we know capability and duty?

- No, not precisely, we must determine (estimate) it!
- Testing for safety
  - Design tests with the above comments in mind
  - Be careful to do accurate tests, be honest in trying to find the problem
  - Sometimes it may be good to get an outsider's perspective
  - Be careful with the results of other's tests - don't just blindly trust them when it comes to safety
- Testing cannot always be performed
  - Failures would be catastrophic
  - Tests are too expensive
- What do to in these cases?
  - Scenario analysis
  - Fault tree analysis

Risk-Benefit Analysis

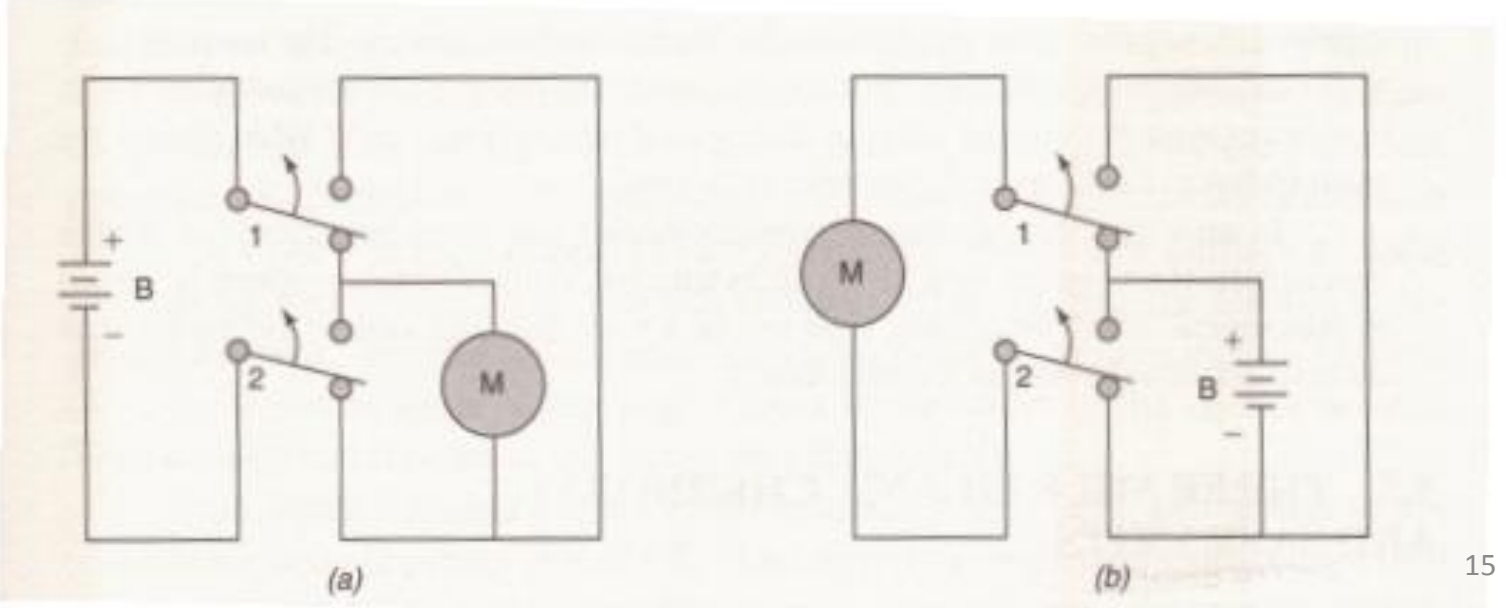
- Risk-Benefit Analysis
  - Is a product worth the risks connected with its use?
  - What are the benefits? To whom?
  - Do they outweigh the risks? To whom? Environmental impact?

"Under what conditions, if any, is someone in society entitled to impose a risk on someone else on behalf of a supposed benefit to yet others?"

- How do you place value in $$ on a human life?? Recall cost-benefit analysis. Human rights/dignity/respect?
- Engineers often supply facts on risk. Caution!
- Example: Operator error and negligence are most often not the principle causes of accidents - often unsafe conditions that are incorrectly assessed

Making a product safe does not automatically increase costs

- Safety should be built into the original design
  - Warnings are often not adequate, cannot fall back on insurance!
  - Must "embed" safety; requires competence, broad perspective!
- Examples: Improved safety
  - Magnetic door catch on a refrigerator (safety for less money!)
  - Ground-fault interrupter (but costs some?)
  - Motor reverse circuit (no cost)



Fail-Safe and Safe-Exit

- Examples of "fail-safe" systems:
  - Concealed headlights on a car
  - Elevators?
- "Safe-exits" are important (fail safe, abandon/escape safe):
  - Three Mile Island, Chernobyl