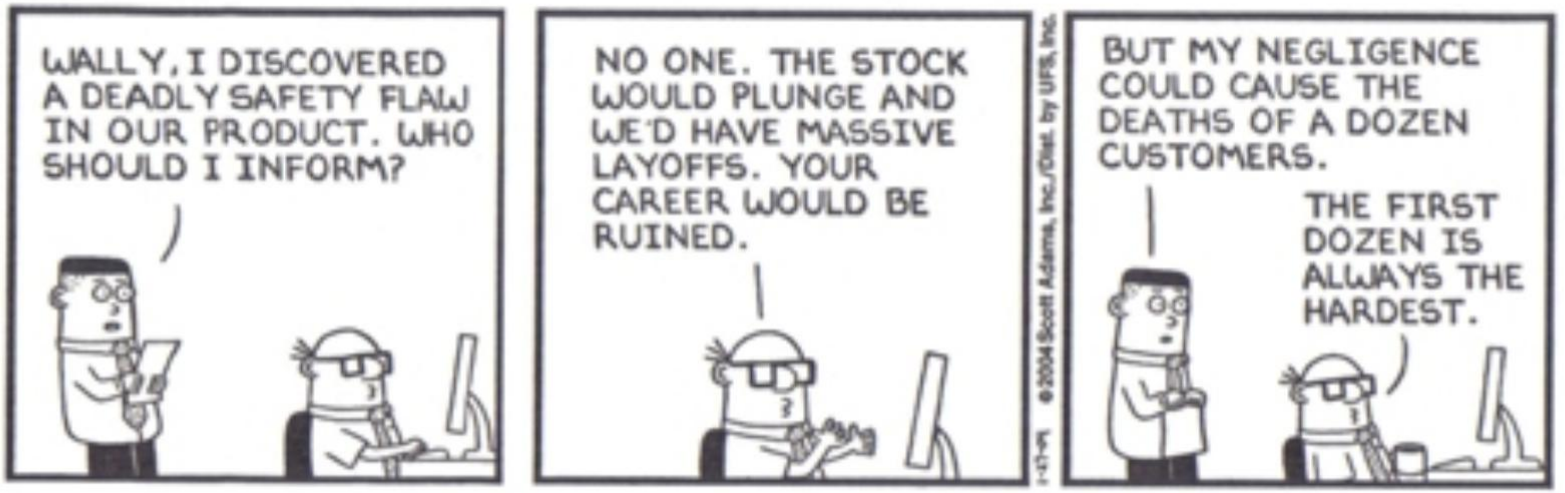
Ethics in Engineering and Research

Lecture #6 Safety and Risk

Prepared by
Asst. Prof. Chen Qingsha (version 1)

Modified by
Assoc. Prof. Aung Ko Ko Kyaw (version 2)

Department of Electrical and Electronic Engineering, SUSTech


WALLY, I DISCOVERED A DEADLY SAFETY FLAW IN OUR PRODUCT. WHO SHOULD I INFORM?
NO ONE. THE STOCK WOULD PLUNGE AND WE'D HAVE MASSIVE LAYOFFS. YOUR CAREER WOULD BE RUINED.
BUT MY NEGLIGENCE COULD CAUSE THE DEATHS OF A DOZEN CUSTOMERS.
THE FIRST DOZEN IS ALWAYS THE HARDEST.
©2004 Scott Adams, Inc./Dist. by UFS, Inc.

Engineer's Concern for Safety

- We demand safe products

  ...but we have to pay for safety

- What may be safe enough for you, may not be for others
  - ❑different perceptions
  - ❑different predispositions to harm
- Absolute safety is neither attainable nor affordable
- What exactly do we mean by "safety"?
- How do we assess it?

Safety Definition

"*A thing is safe if its risks are judged to be acceptable*" (not perfect)

"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!
- relative to people's value perspectives
- subjective to the extend that value perspectives differ

Risk

- Definition: A risk is the potential that something unwanted and harmful may occur
- "Experimental" risks associated with introducing new technology ("social experimentation")
- Example: Electrical car/blind 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

Risk of EV for blind and partially sighted people

- https://www.euroblind.org/campaigns-and-activities/finished-campaigns/silent-cars
- https://phys.org/news/2018-10-electric-cars-hazard-people.html
- https://www.carexpert.com.au/car-news/blind-people-want-louder-electric-cars#article_comments

Electronic Door Locks/Handle in EV cars

Electronic Door Locks Trap Driver in Burning Vehicle

The incident occurred when a Xiaomi SU7 Ultra collided with a median barrier at high speed, immediately bursting into flames. Bystanders desperately attempted to rescue the trapped driver, but the vehicle's electronic door handle system malfunctioned after impact, preventing anyone from opening the doors. The driver sadly perished in the inferno while would-be rescuers watched helplessly outside.

Tesla Under Scrutiny For Door Handles Too

Tesla is now redesigning its door handles after federal regulators launched investigations into reports that electronic handles failed, leaving children trapped inside vehicles. The NHTSA investigation found at least nine complaints, with four cases where parents smashed windows to free their kids. Tesla's design chief announced plans to combine electric and manual door releases into a single, more intuitive mechanism, an admission that over-engineering basic safety features creates unacceptable risks.

This tragedy highlights a disturbing trend in modern door handle design: manufacturers prioritizing sleek aesthetics over reliable emergency access. The Xiaomi SU7 Ultra features flush, electronically-controlled door handles that require electrical power to function. This means the door opening mechanism fails during crashes when power is lost. What was once a simple mechanical latch has become a complex electronic system with deadly consequences when it fails.

Acceptability of Risk

- A Risk is acceptable when those affected are generally no longer (or not) apprehensive about it.
- Apprehensiveness depends on
  - ✓Whether the risk is accepted voluntarily
  - ✓Knowledge on the probability of harm (or benefit)
  - ✓Job-related or not
  - ✓Risk is immediately noticeable or not
  - ✓whether the potential victims are identifiable beforehand
- Are the risks on-the-job voluntarily?
- 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 familiar products that have not hurt them before and that they have control over (e.g. less careful with ABS)

– Over-pessimistic when accidents kill large numbers or harm those we know but might occur infrequently (e.g., aircraft crashes)

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?

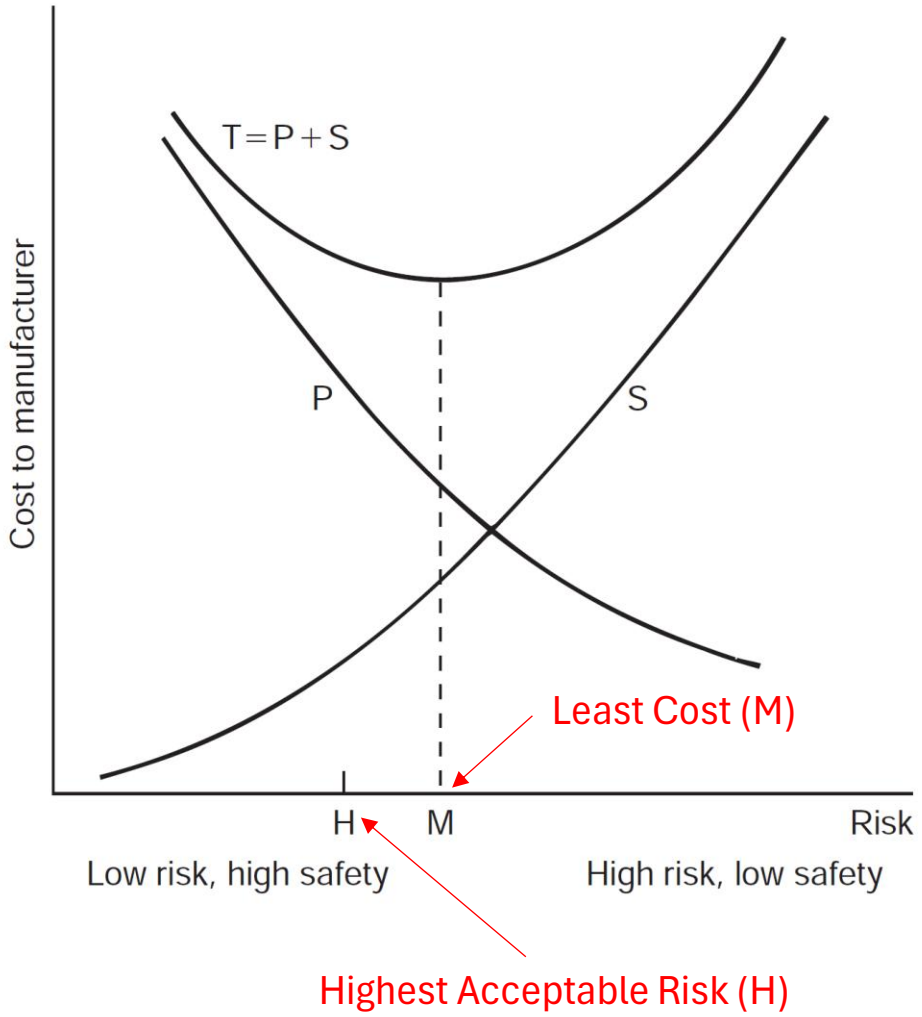
Design principle, risk/trade-offs

How safe should we make a product?

There are trade-offs…

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

S = secondary costs



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

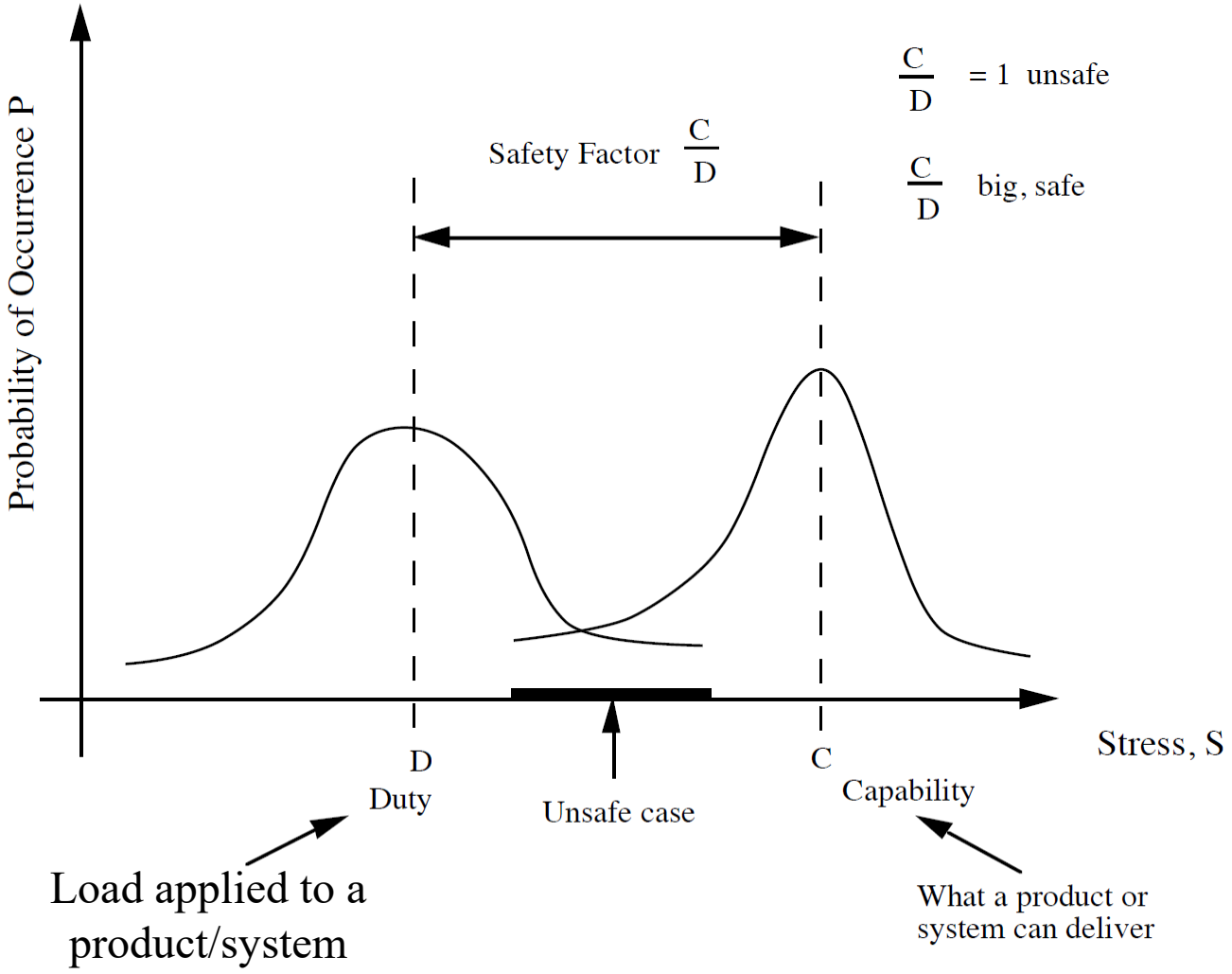
Tacoma Narrows Bridge Collapse

Resistor Color Table

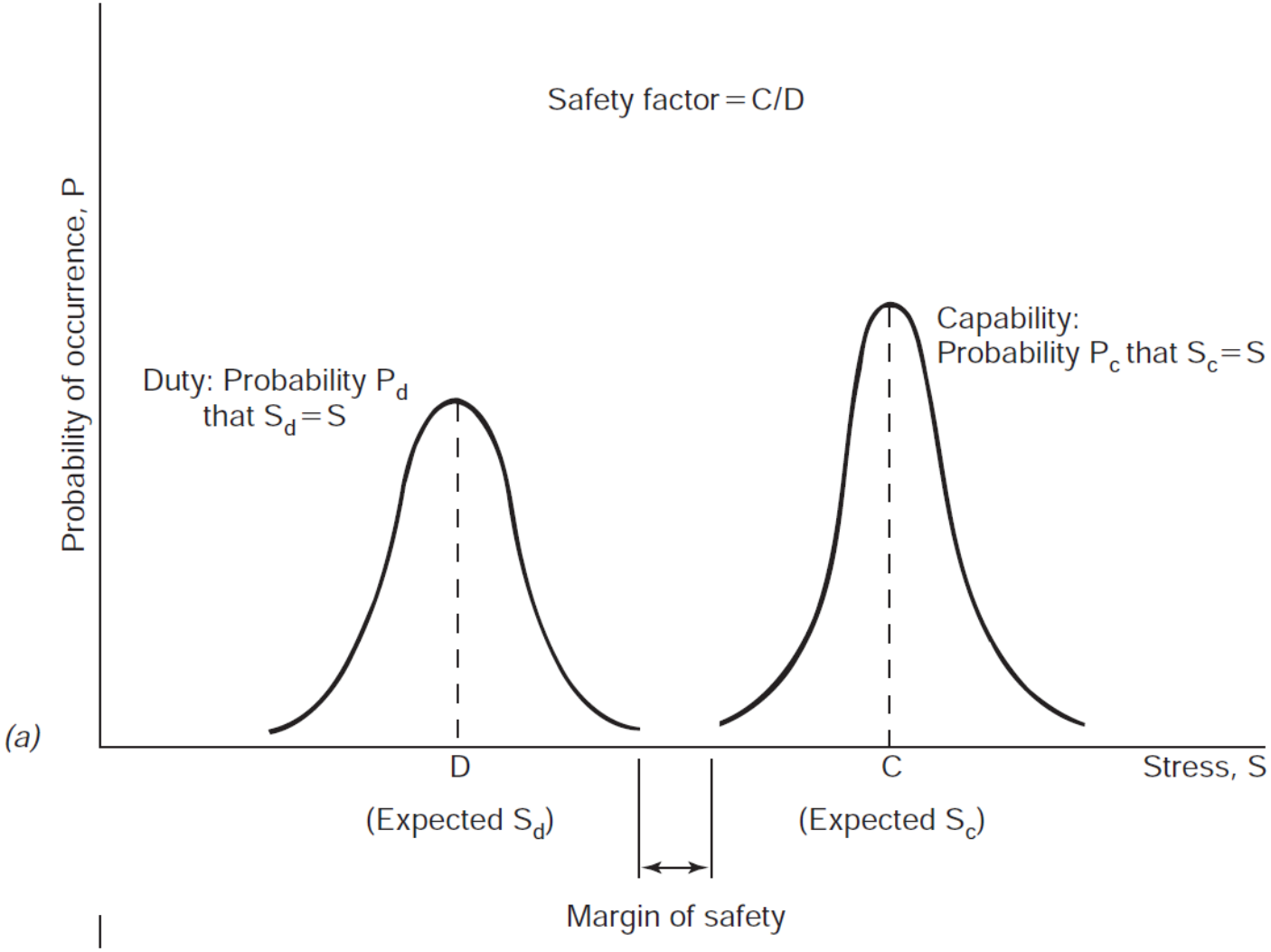
62 Ω ±5%

1st Digit	2nd Digit	Multiplier	Tolerance
0	0	x 1 Ω	
1	1	x 10 Ω	± 1%
2	2	x 100 Ω	± 2%
3	3	x 1 KΩ	
4	4	x 10 KΩ	
5	5	x 100 KΩ	
6	6	x 1 MΩ	
7	7		
8	8	x 0.1 Ω	± 5%
9	9	x 0.01 Ω	± 10%

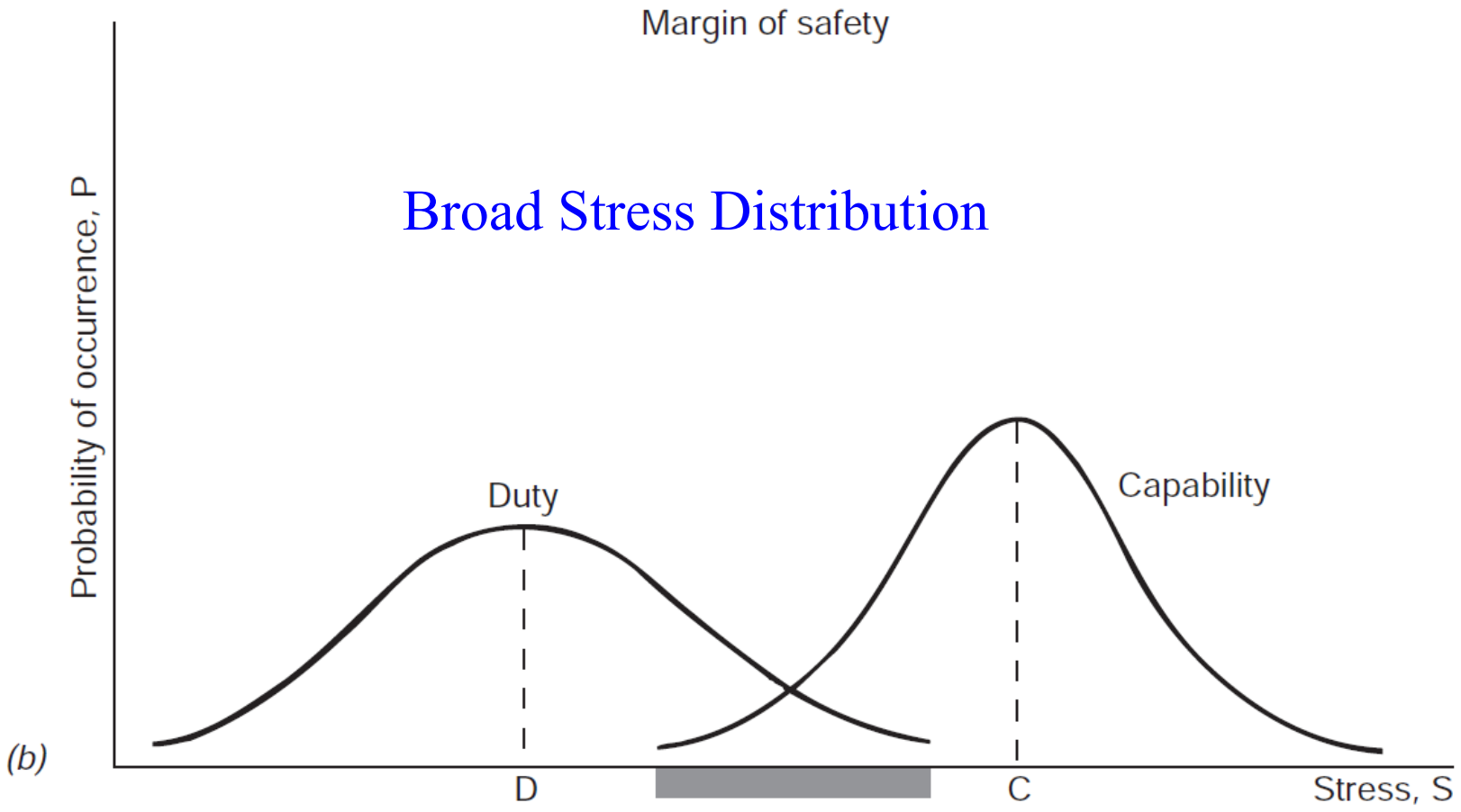
Design Principle:
Safe if Capability Exceeds Duty



Relatively Safe Case ☺



Not Safe! ☹


Margin of safety
Broad Stress Distribution
Probability of occurrence, P
Duty
Capability
(b)
D
C
Stress, S

Risk-Benefit Analysis

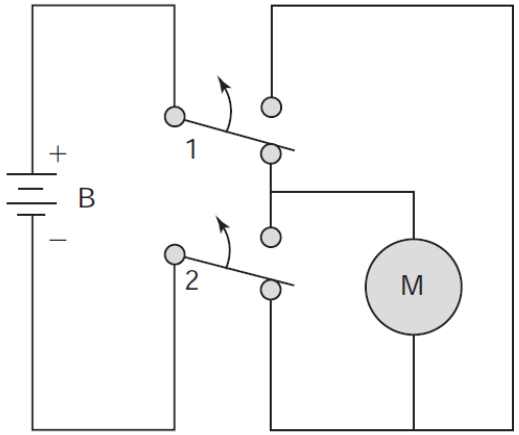
- Risk-Benefit Analysis
  - Is a product worth the risks connected with its use?
  - What are the benefits? To whom?
  - Do they outweigh the risks? To whom? Environmental impact?

"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?"

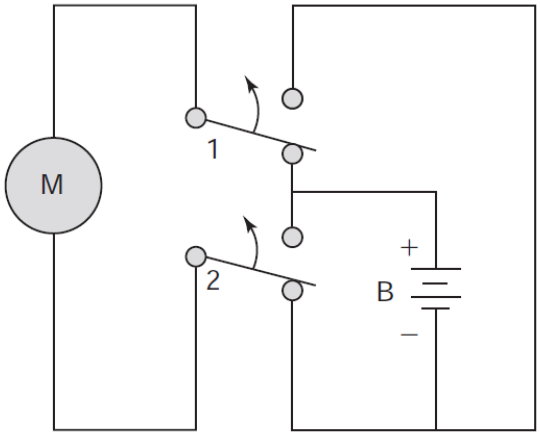
- How do you place value in $$ on a human life?? Recall cost-benefit analysis. Human rights / dignity/ respect?
- Other difficulties in assessment
  - How to address expected values as both risk and benefits occur in the future (probably at different time periods)
  - Benefit goes to one party and risk is incurred by another party

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)



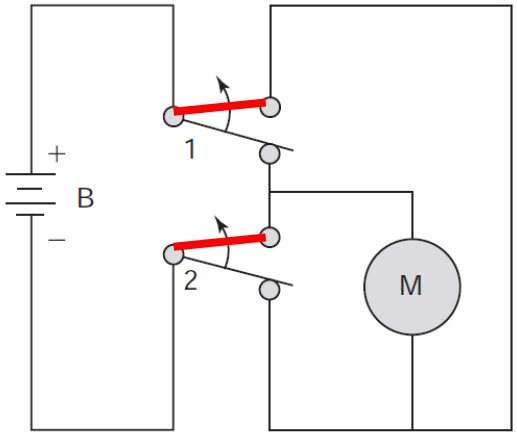
(a)



(b)

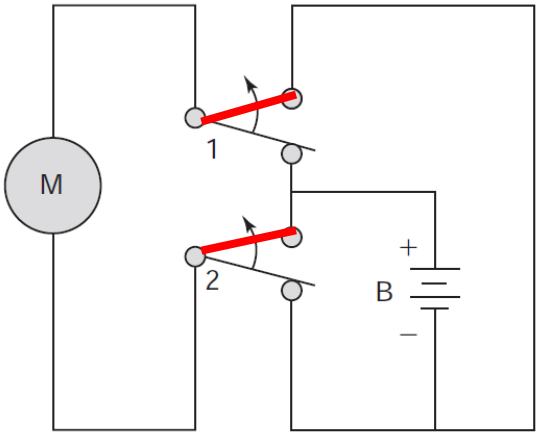
Under the proper way of operation

Original design



(a)

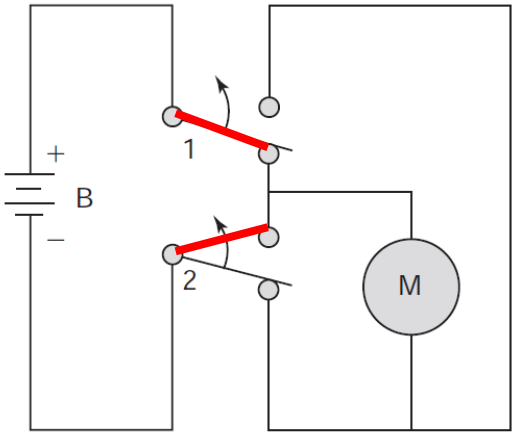
New design



(b)

When one arm does not move

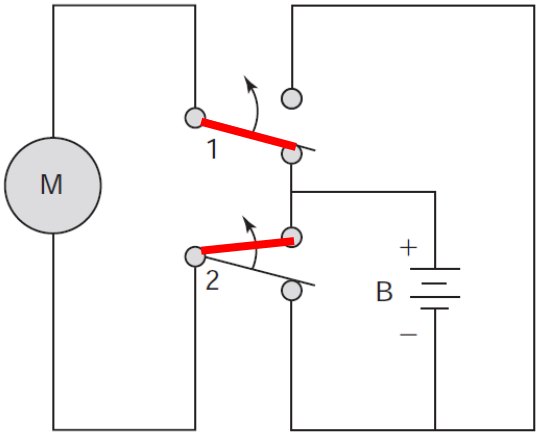
Original design



(a)

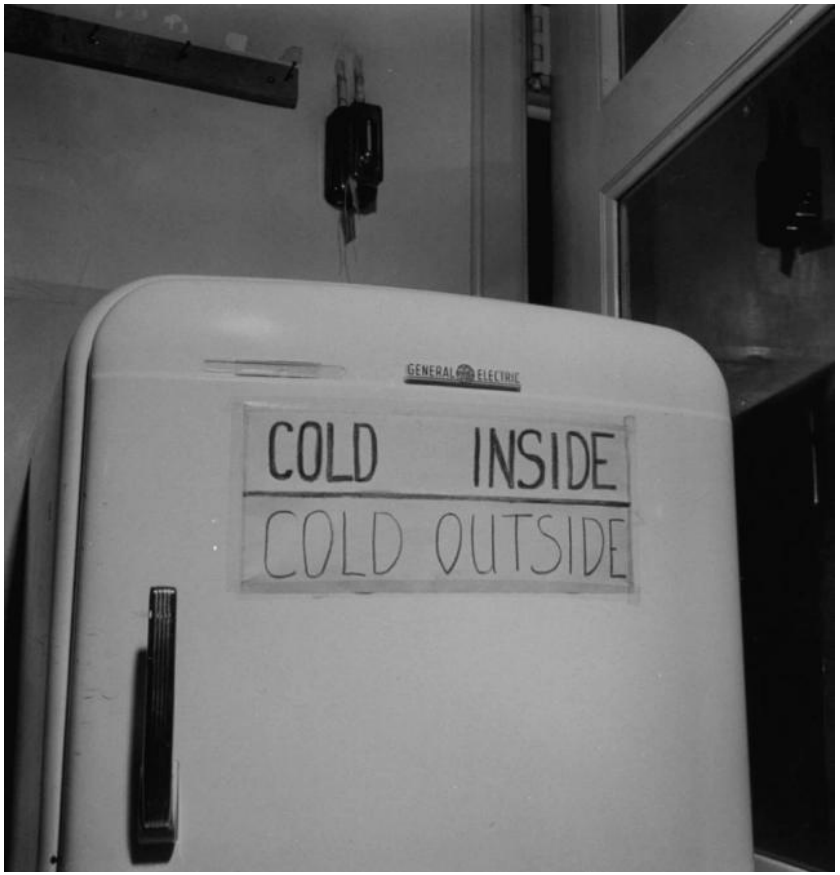
Short circuit
across the battery.

New design



(b)

The battery is not
short-circuited.



The old-style handle fridges have a dark secret (Picture: Charles E. Steinheimer/The LIFE Picture Collection/Getty Images)

Testing to see if this little girl could open the new fridges from the inside (Picture: pediatrics.aappublications.org)

Safe Exists

- It is almost impossible to build a completely safe product or one that will never fail.
- So when a product fails, be ensure
  1. it will fail safely (fail-safe system)
  2. it can be abandoned safely
  3. the user can safely escape the product.

Safe Exist!

- Fail-safe example: elevator, traffic light
- an integral part of the social experimental procedure (sound engineering)
- Examples:
  - Ship with enough lifeboats
  - Building with fire escape, evacuation route