Design for Safety
MCHE 201 – Spring 2019

Dr. Joshua Vaughan

Rougeou 225

joshua.vaughan@louisiana.edu

@Doc_Vaughan

Everything is Dangerous

Design for Safety Phases

1. Problem definition

2. Risk identification

3. Risk estimation

4. Risk evaluation

5. Design review

Iterative!

Guiding Principles

1. Design in Safety

2. Utilize Guards

3. Anticipate Operator Errors

4. Restrict Improper Use

5. Accommodate Unusual Operating Conditions

6. Utilize Redundancy

7. Design Safe Failure Modes

8. Facilitate Maintenance

9. Add Warning Labels and Systems

Design in Safety

This is *not* safety

Screenshot of Google Image Search Results Page

Design in Safety

- Do *not* rely on warning labels

- Do *not* rely on operator training or common sense

- Modify the design to make it safe
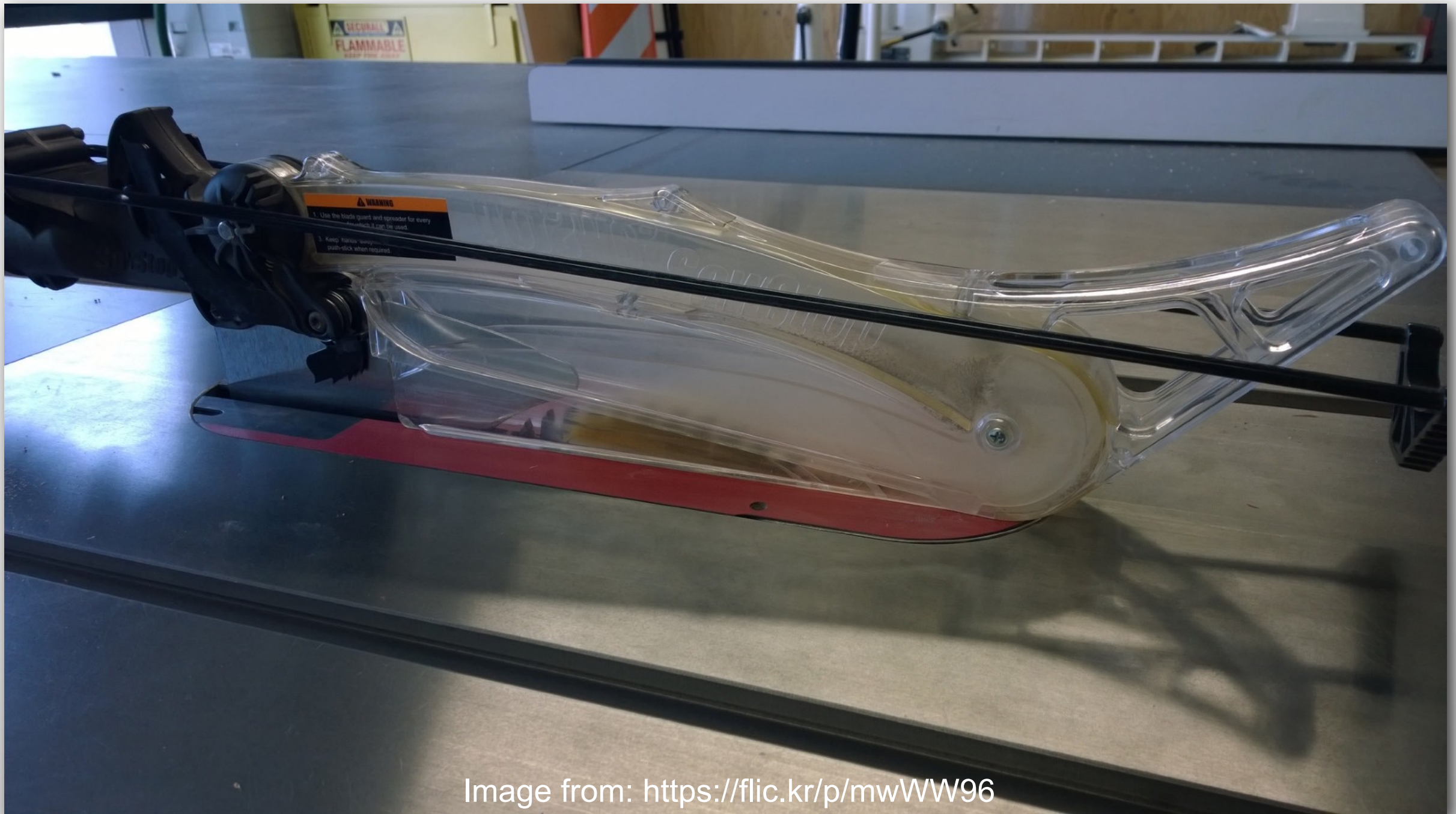
Table Saw

- *DANGEROUS!*

Image from: https://flic.kr/p/e6ZzRD

Table Saw

- *DANGEROUS!*

Image from: https://flic.kr/p/mwWW96

SawStop

Video from: https://youtu.be/eiYoBbEZwlk

Aerial Lift

Aerial Lift

Aerial Lift

Utilize Guards

- Don't allow access to dangerous parts of the design

Image from: https://flic.kr/p/7a4t95

Utilize Guards

- Don't allow access to dangerous parts of the design

Image from: https://flic.kr/p/jeLGc7

Table Saw

Image from: https://flic.kr/p/e6ZzRD

Table Saw

Image from: https://flic.kr/p/mwWW96
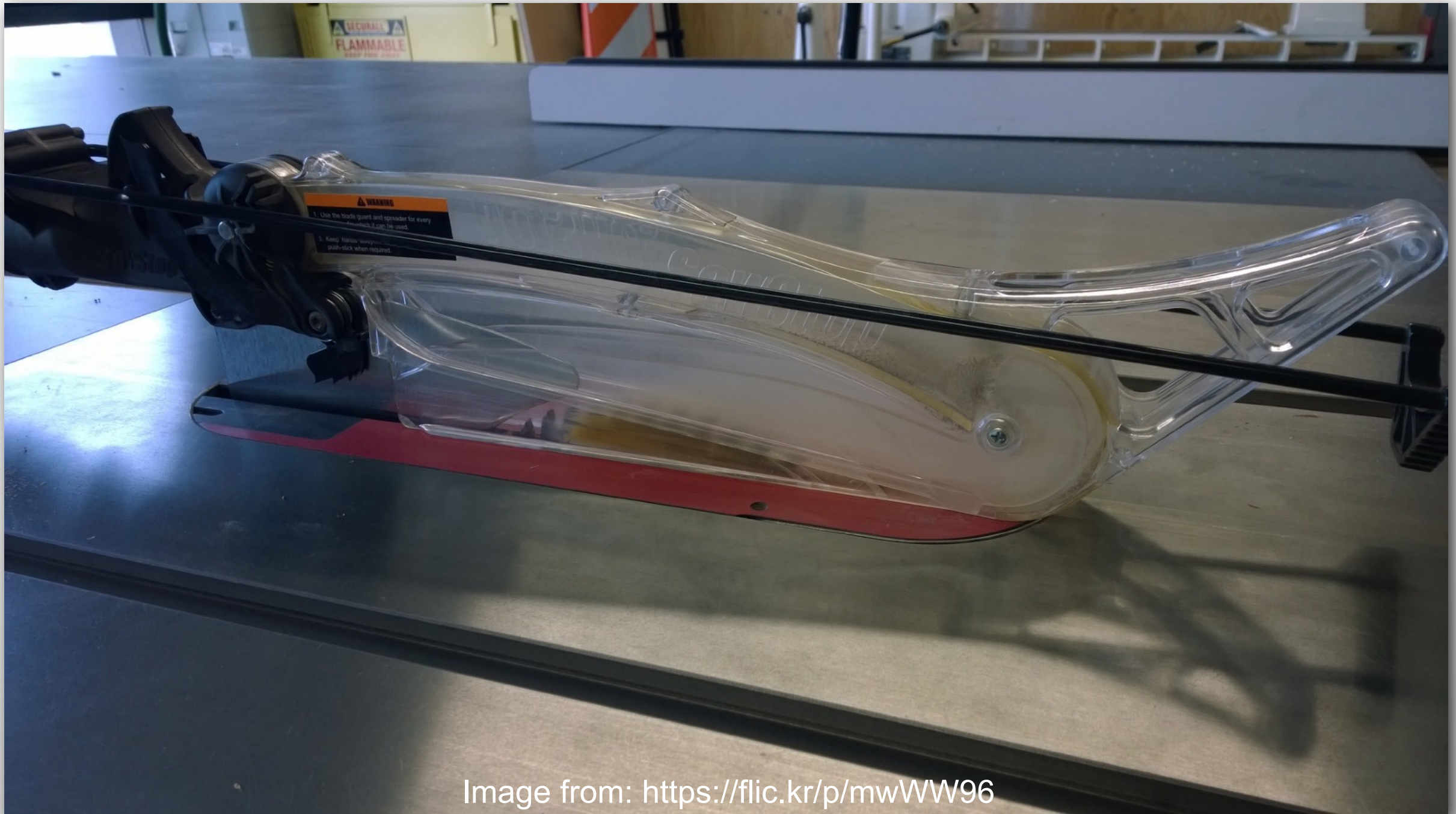
Anticipate Operator Errors

- People will:
    - make mistakes
    - be distracted
    - be tired
    - not read the operator's manual
    - not pay attention during and/or not remember training
    - not maintain the equipment properly
    - be drunk

- Designing for these things will typically make your design easier to use as well

The User is Drunk

Boeing Crane Story

•

Image from: https://flic.kr/p/eUNsDZ

More Crane Accidents

Restrict Improper Use

- People will… So, don't let them mess up

Image from: https://flic.kr/p/jeLGc7

Dead-man's Switch Example

- Gamepad

Throttle
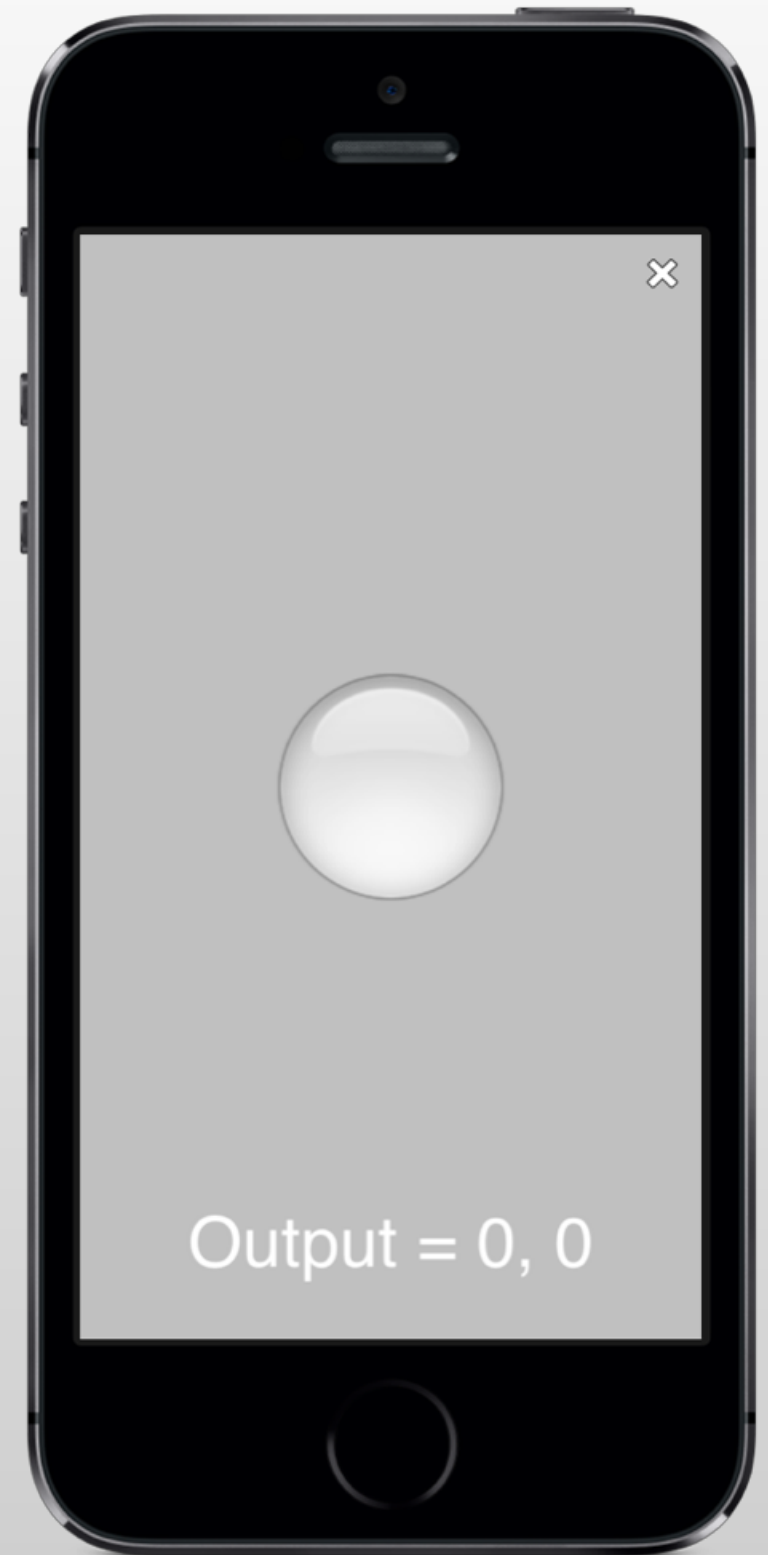
Helm

Port
Bucket

Starboard
Bucket
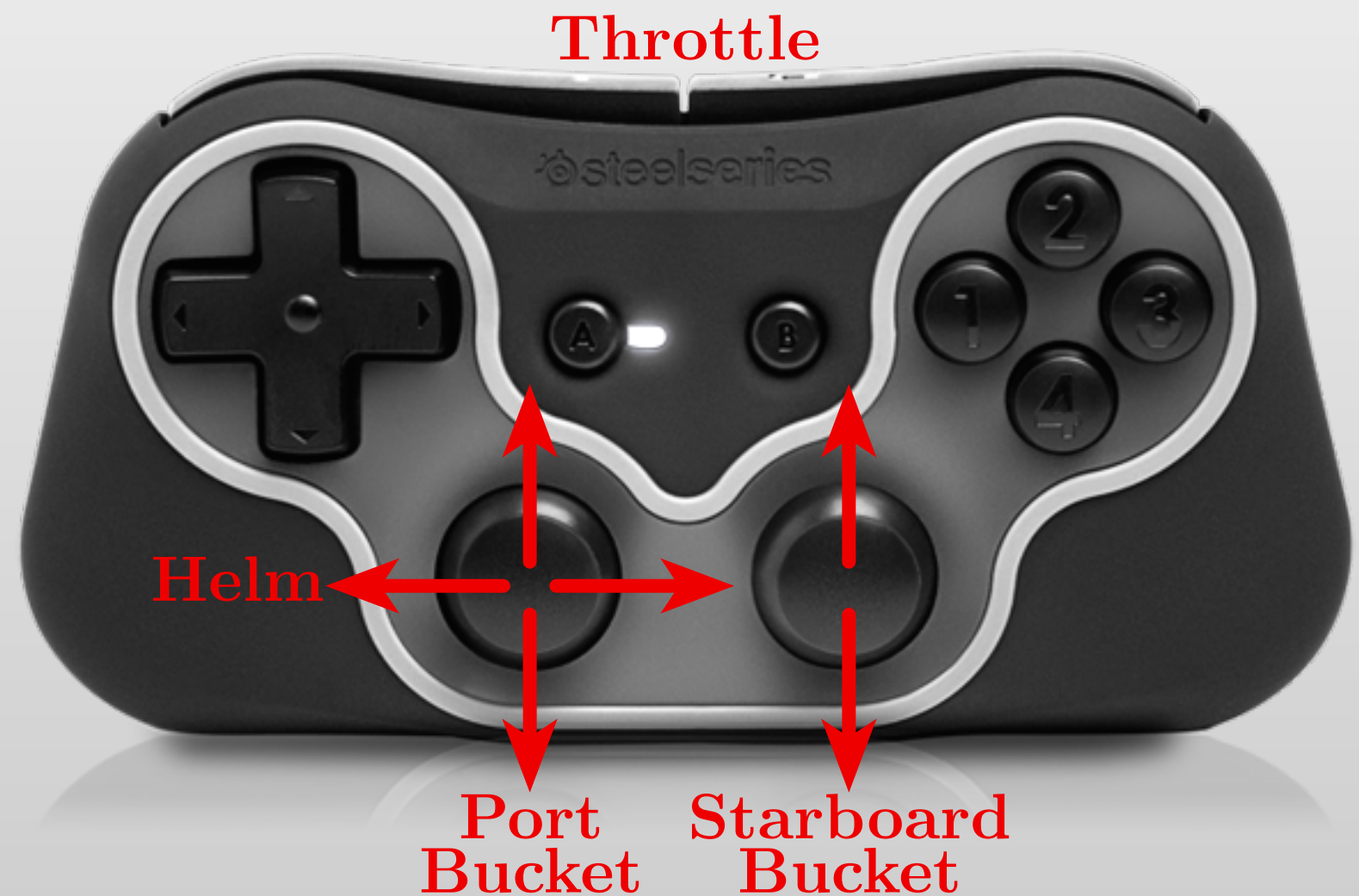
Dead-man's Switch Example

- Gamepad

- iOS-based remote
  - Joystick
  - Tilt-based

Output = 0, 0

At the Feb. 18 Demo

UL Partners with SwiftShips
Autonomous Vessel

"... it is your job to make it impossible for the user to accidentally operate your device in an unsafe manner. Users should have to make an intentional and concerted effort in order to injure themselves or others."

Accommodate Unusual Operating Conditions

- People will use your design how they want, not how you intended.

- Anticipate improper use and unusual conditions

Utilize Redundancy

- Avoid singe-point-of-failure designs

Design Safe Failure Modes

Image from: https://flic.kr/p/cPebu

Facilitate Maintenance

- If maintenance is needed, make it easy.

Image from: https://flic.kr/p/eHVVe2

Facilitate Maintenance

- If maintenance is needed, make it easy.

Image from: http://www.chevrolet.com/corvette-z06-supercar/exterior-pictures.html

Facilitate Maintenance

- If maintenance is needed, make it easy.

Image from: http://www.hansotten.com/index.php?page=apple-ii

Facilitate Maintenance

- If maintenance is needed, make it easy.

Image from: http://www.theverge.com/2015/3/9/8180315/apples-shrinking-skills-in-new-macbook   24
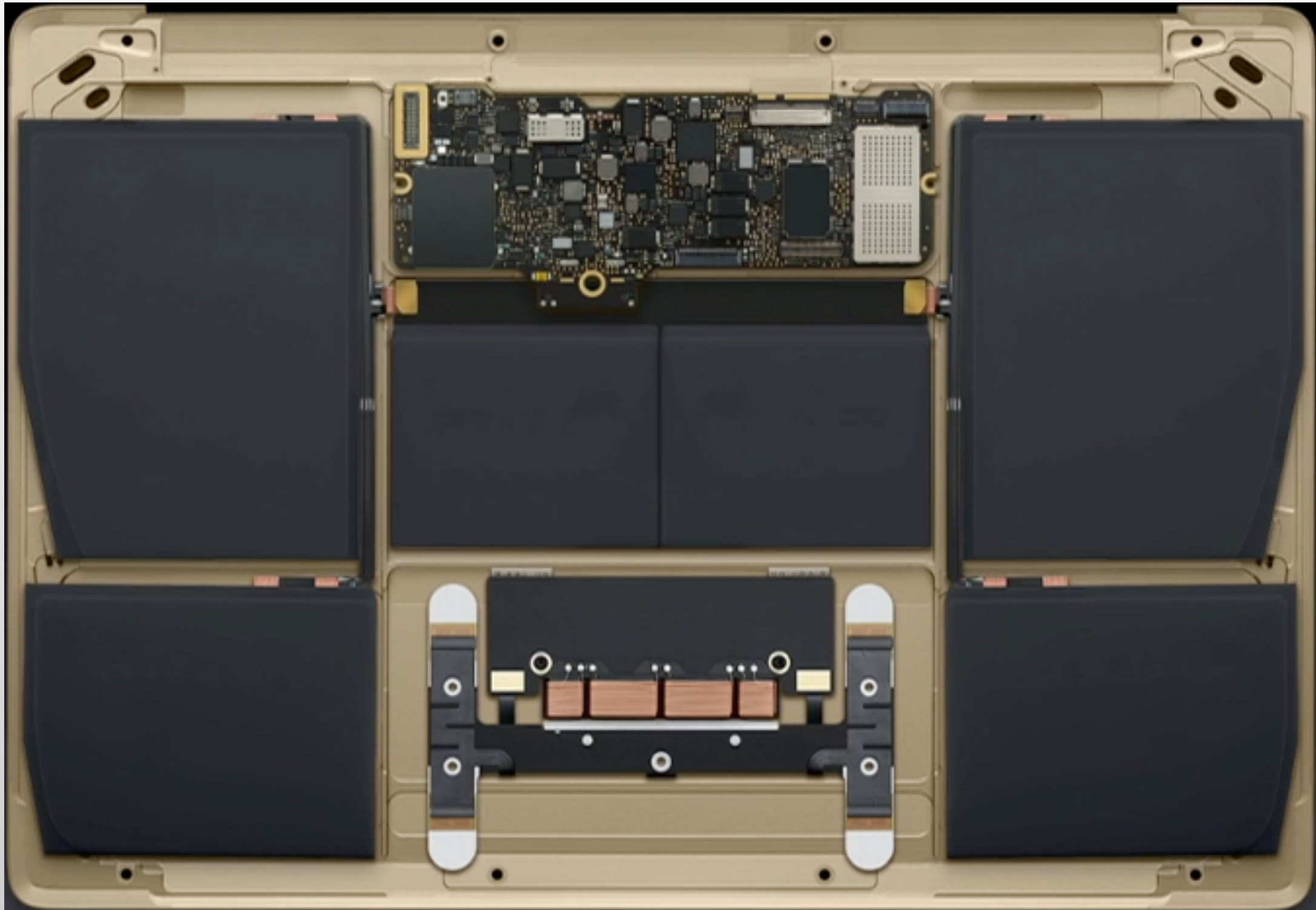
Add Warning Labels and Systems

Image from: https://flic.kr/p/o7q6tD

Add Warning Labels and Systems

- Do all of that and…