PLEASE SIT TOWARD THE FRONT AND CENTER

Home

Safety & Liability
Risk Assessment & Management

ME 4182

Capstone Design

Dr. Ken Cunefare

(a work in progress)

Last revised 9/15/19

Home

Relevance to Capstone

- What are the risks and consequences?
- What are the failure modes for your design?
- What are your risk mitigation tactics?
- What Codes & Standards apply?
- Document your findings concerning, and the process for addressing, these issues

Home

Coverage/Contents

- Managing Risk and Liability
  - Hazards and Risk Assessment
  - Failure Modes and Effects Analysis FMEA
- Product Liability Concepts

- Backup materials
  - Citations and links (in progress…)
  - Liability
  - FMEA

20 Steps to Reduce Risk and Liability 1

1. Include safety as a primary specification in identifying needs during all phases of the product's existence
2. Design to a recognized standard (failure to do so may be "negligence *per se*")
   - UL, ANSI, ISO, ASTM (GT has ASTM stds)
   - Industry/Professional Society
     - ASHRAE, ASME (e.g., BPVC)
     - Product/industry/manufacturer specific (Espresso!)
   - Within these resources, look for
     - Required analysis methods
     - Required Factors of Safety
     - Required testing methods
     - Etc….

20 Steps to Reduce Risk and Liability

1. Include safety as a primary specification in identifying needs during all phases of the product's existence
2. Design to a recognized standard (failure to do so may be “negligence *per se*”)
3. Select materials and components that are known to have sufficient quality and a small enough standard deviation from the norm to consistently do the job expected
4. Apply accepted analysis techniques to determine if all electrical, mechanical, and thermal stress levels are well within published limits (what does factor of safety mean?)

Home

20 Steps to Reduce Risk and Liability

5. Test the device using accelerated aging tests, using a recognized test
6. Conduct a design review that includes persons knowledgeable about ALL aspects of a product.
7. Perform a failure and hazards analysis of the product for each stage of product life

Home

20 Steps to Reduce Risk and Liability 4

5. Test the device using accelerated aging tests, using a recognized test
6. Conduct a design review that includes persons knowledgeable about ALL aspects of a product.
7. Perform a failure and hazards analysis of the product for each stage of product life
8. Perform a worst-case analysis of the product
9. Submit product to independent testing laboratory (e.g. UL)
10. Make sufficient information (notes on drawings, component specifications, etc.) available to the factory to identify and mitigate/eliminate hazards

Home

20 Steps to Reduce Risk and Liability 5

11. Make a permanent record of the history of the product development.
12. Wherever there is a question regarding safety of a product, document the risk/utility considerations made during the design phase.
13. Use warning labels on the product when this is appropriate
14. Supply unambiguous instructions for properly installing or using the product
15. Determine any service or maintenance necessary to keep the product safe and operating

Home

20 Steps to Reduce Risk and Liability 6

16. Where feasible, have all products inspected after manufacture
17. Inform the quality control/manufacturing of manufacturing errors that may result in a dangerous product
18. Test the effects of mass manufacture on the product
19. Work with the advertising/marketing to guard against overstatements of product performance
20. Encourage sales and service personnel and dealers to report any complaints that have to do with injury or economic loss (but should ***act*** on the data!) (McDonald's coffee case burn)

Home

Relevance to Capstone

What are the risks and consequences?

What are the failure modes for your design?

What are your risk mitigation tactics?

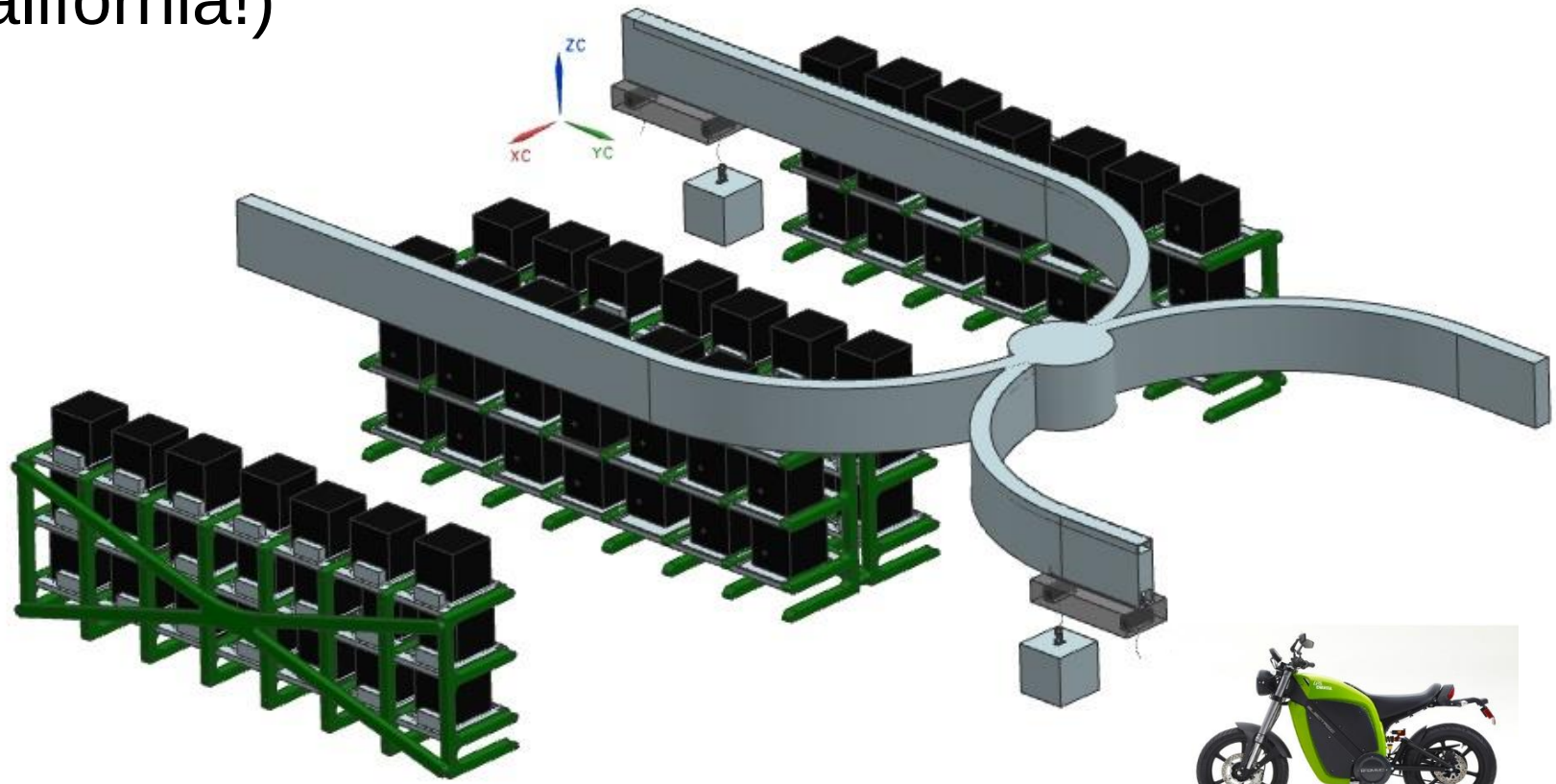
What Codes and Standards Apply?

Document your findings concerning, and the process for addressing, these issues

Home

Battery removal, storage, and recharge system

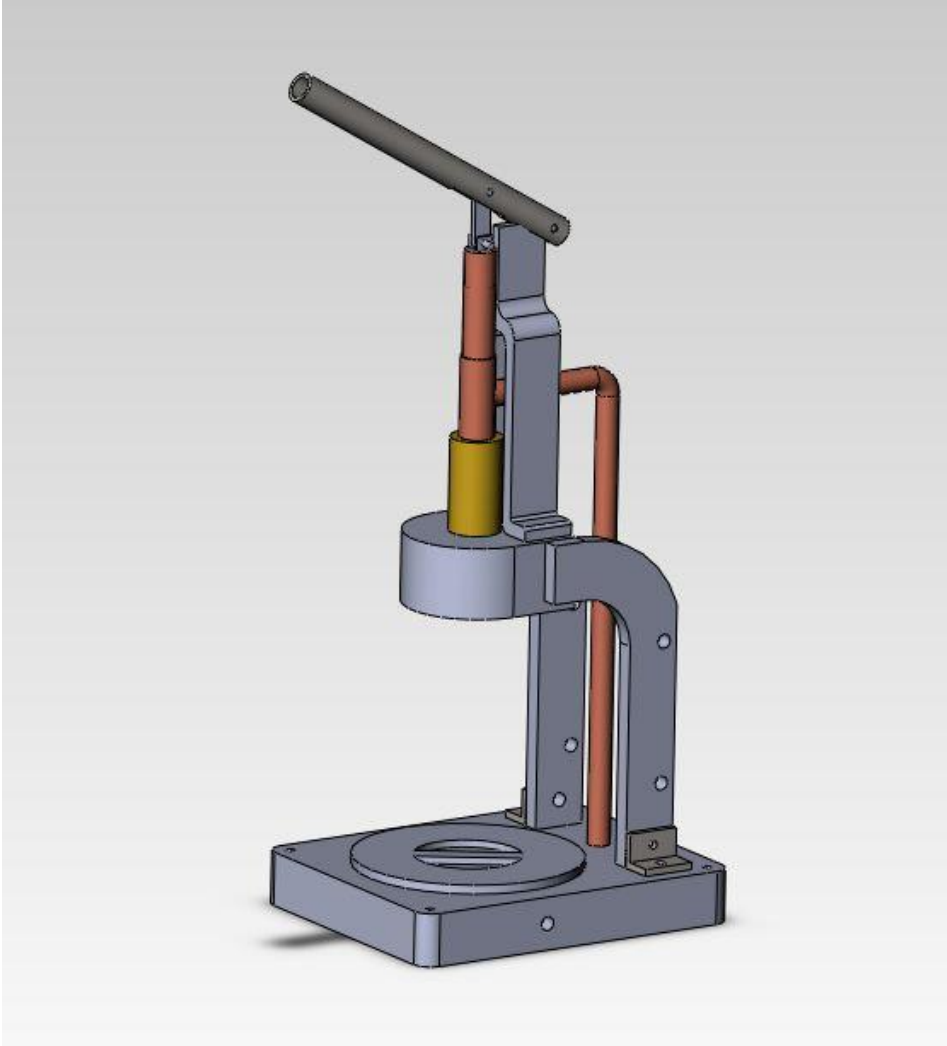
- What are the risks?
- What are the consequences?
- What are the applicable codes and standards? (California!)



Home

Stovetop Espresso Maker

- What are the risks?
- What are the consequences?
- What are the available codes and standards?
  - Certified Espresso



Home

Risk Assessment

When do we accept risk?

- When it's insignificantly low.
- When we are sure it is worth it.
- ***When we do not know it is there.***
- When it hasn't harmed or killed us yet
  - Normalization of deviation – when the abnormal becomes accepted as routine
    - Any cases spring to mind?
    - Space shuttles Challenger & Columbia

Home

Hazards and Risk Assessment

- A formalized, structured approach to identify, assess, and mitigate risk

Failure modes and effects analysis FMEA

- A formalized, structured approach to identify, assess, and mitigate failure modes (that lead to risk!)

Hazards and Risk Assessment

- A formalized, structured approach to identify, assess, and mitigate risk

DEPARTMENT OF DEFENSE
STANDARD PRACTICE FOR SYSTEM SAFETY

MIL-STD-882D Matrix

CATEGORY / FREQUENCY	(1) CATASTROPHIC	(2) CRITICAL	(3) MARGINAL	(4) NEGLIGIBLE
(A) FREQUENT ($X > 10^{-1}$)				
(B) PROBABLE ($10^{-1} > X > 10^{-3}$)				
(C) OCCASIONAL ($10^{-2} > X\ 10^{-3}$)				
(D) REMOTE ($10^{-3} > X > 10^{-6}$)				
(E) IMPROBABLE ($10^{-6} > X$)				

UNACCEPTABLE (must mitigate)

ACCEPTABLE WITH REVIEW (may mitigate)

UNDESIRABLE (should mitigate)

ACCEPTABLE WITHOUT REVIEW

Home

Need to know/define/determine…

- **Risk Level**
  - (1) High – Imperative to reduce risk level.
  - (2) Medium – Requires a mitigation plan.
  - (3) Low – No special risk mitigation activities are required.

- **Severity of Consequences**
  - (1) Catastrophic – Death or system loss.
  - (2) Critical - Severe injury or major system damage.
  - (3) Marginal - Injury requiring medical attention or system damage.
  - (4) Negligible - Possible minor injury or minor system damage.

Home

Need to know/define/determine…

- **Frequency of Exposure**
  - (A) Frequent - Expected to occur frequently.
  - (B) Probable - Will occur several times in the life of an item.
  - (C) Occasional - Likely to occur sometime in the life of an item.
  - (D) Remote - Unlikely, but possible to occur in the life of an item.
  - (E) Improbable - So unlikely, it can be assumed occurrence may not be experienced.

Home

Example “Consequences”

Table 1: Example of Multiple Consequences for a Consequence Range
Source: MIL-STD-882D

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Home

Table 2: Example of Likelihood Ranges

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur more than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

Source: MIL-STD-882D

*Definitions of descriptive words may have to be modified based on quantity of items involved.

**The expected size of the fleet or inventory should be defined prior to accomplishing an assessment of the system.

Home

DEPARTMENT OF DEFENSE
STANDARD PRACTICE FOR SYSTEM SAFETY

MIL-STD-882D Matrix

CATEGORY / FREQUENCY	(1) CATASTROPHIC	(2) CRITICAL	(3) MARGINAL	(4) NEGLIGIBLE
(A) FREQUENT ($X > 10^{-1}$)				
(B) PROBABLE ($10^{-1} > X > 10^{-3}$)				
(C) OCCASIONAL ($10^{-2} > X\ 10^{-3}$)				
(D) REMOTE ($10^{-3} > X > 10^{-6}$)				
(E) IMPROBABLE ($10^{-6} > X$)				

UNACCEPTABLE (must mitigate)

ACCEPTABLE WITH REVIEW (may mitigate)

UNDESIRABLE (should mitigate)

ACCEPTABLE WITHOUT REVIEW

Home

- Okay, you've defined your risk tolerance
- Now what?
- FMEA (or other assessment tool)

What is FMEA?

- ***Failure Mode and Effects Analysis***
- Methodology of FMEA:
  - ***Identify*** *the potential failure of a system and its effects (Risk Assessment RA)*
  - ***Assess*** *the failures to determine actions that would eliminate the chance of occurrence*
  - ***Document*** *the potential failures*
- ***Mitigate*** *the potential failures (connect back to RA)*

Home

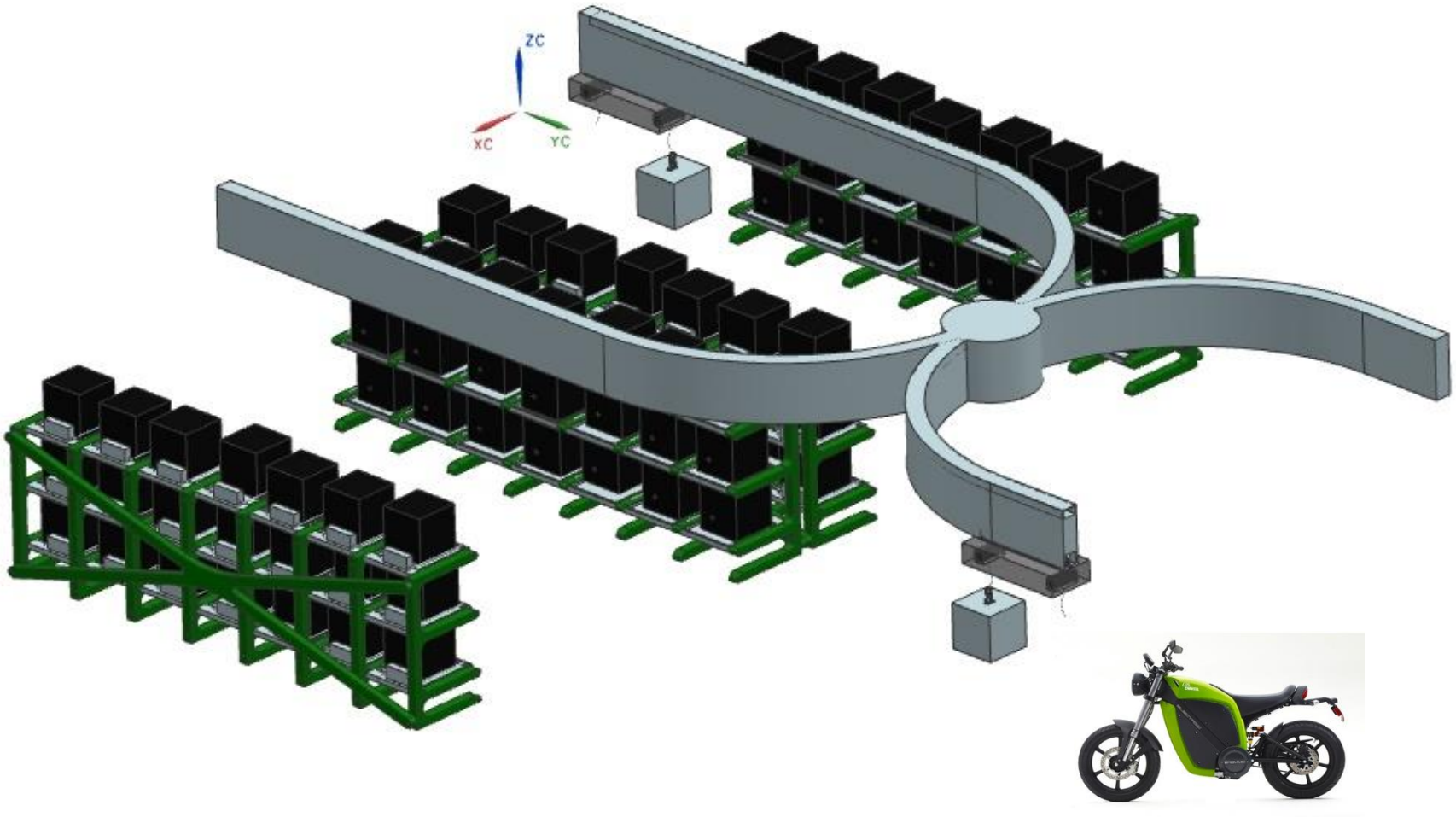
FMEA

- The aim of FMEA is to ***anticipate***:
  - what might *fail*
  - what *effect* this failure would have
  - what might *cause* the failure

… and take action to correct it!

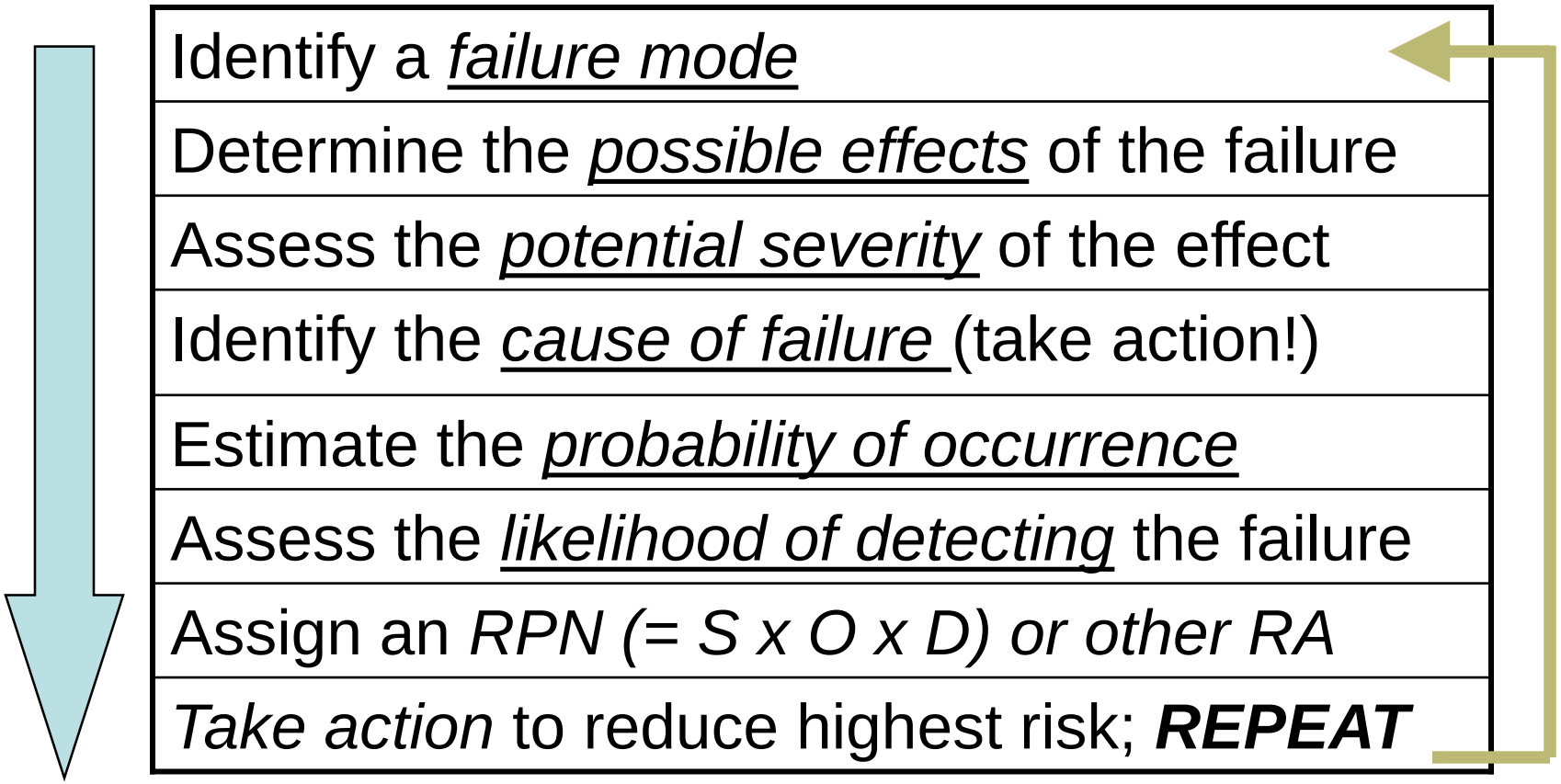
(see backup materials for process)

Battery removal, storage, and recharge system

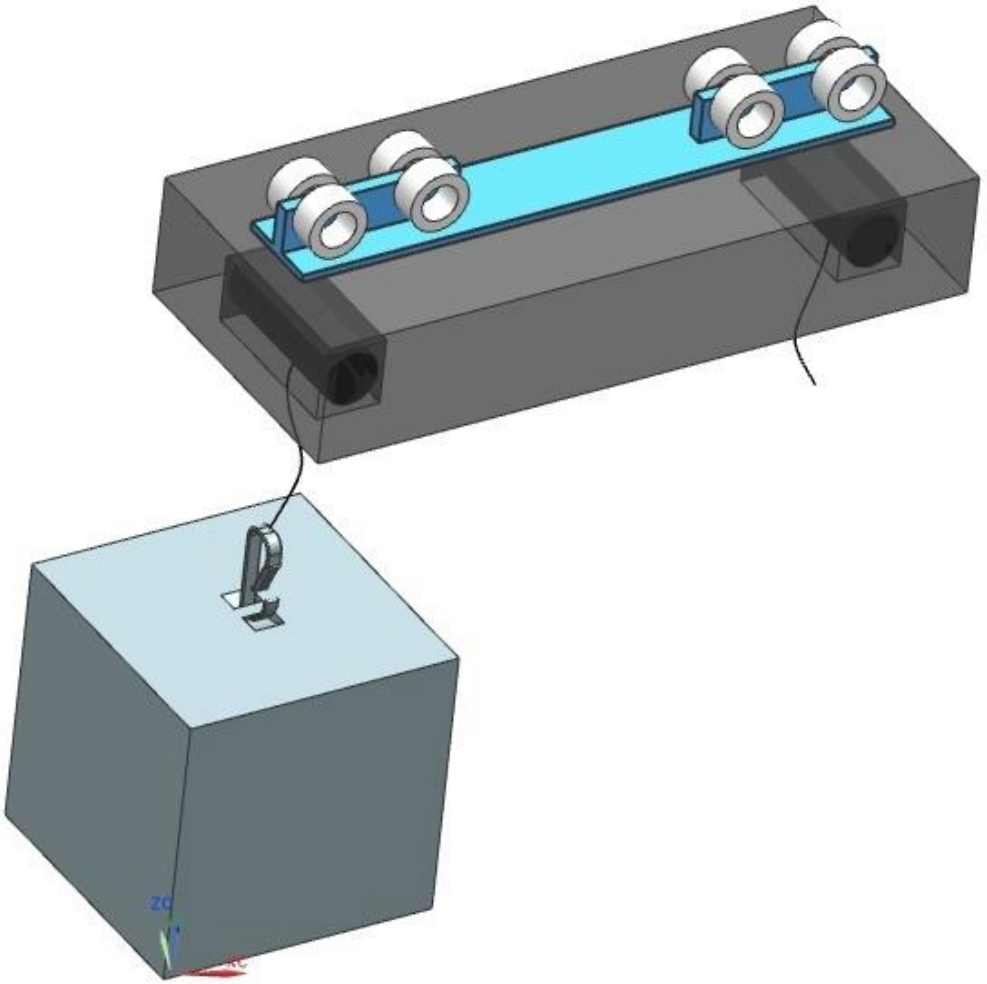


Home

Summary - FMEA Flowchart

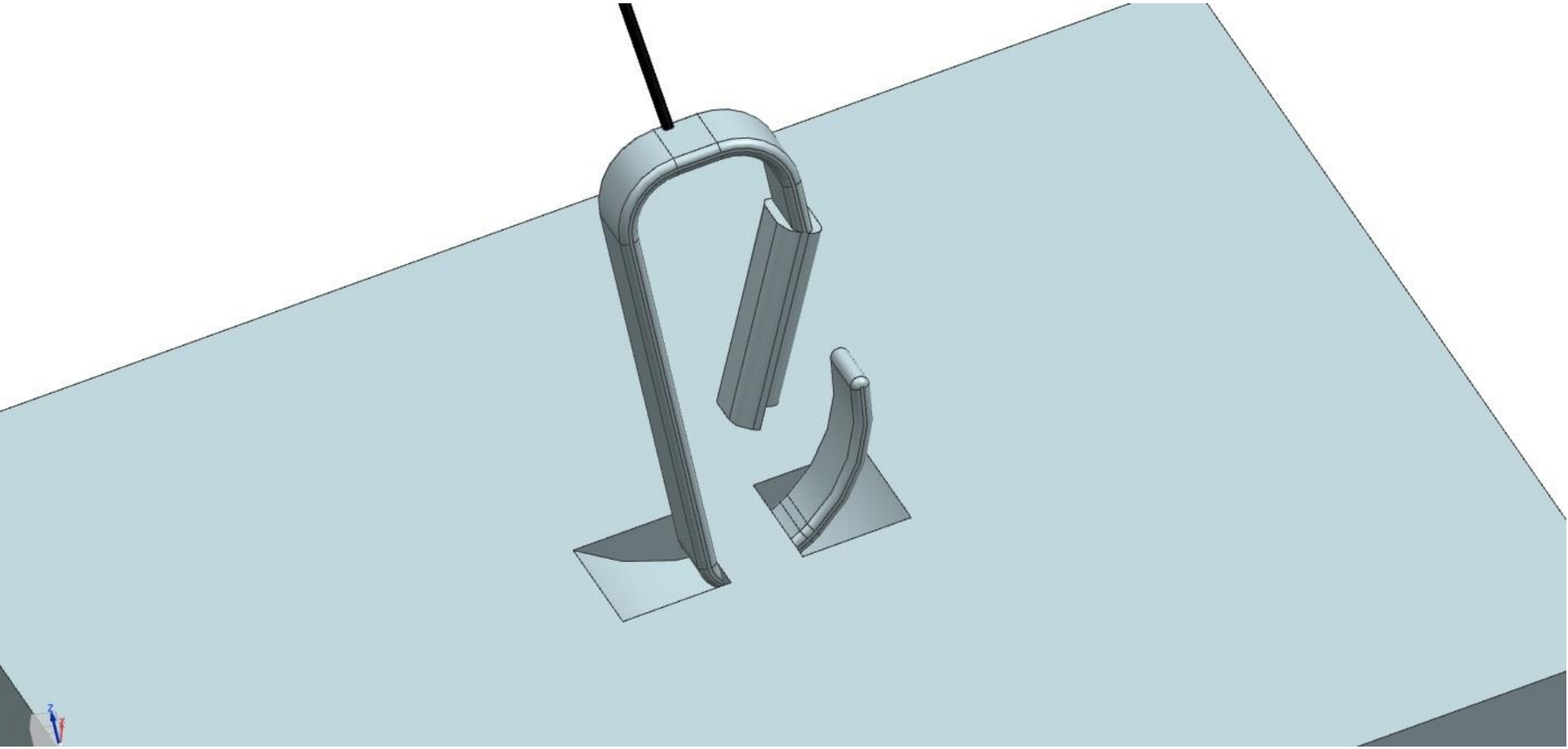


Battery Support/Trolley System



Home

Battery Attachment
Beware single-point failures!



Home

Example Risk Assessment Matrix

Frequency of Exposure	Severity			
	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	A1	A2	A3	A4
Probable (B)	B1	B2	B3	B4
Occasional (C)	C1	C2	C3	C4
Remote (D)	D1	D2	D3	D4

Risk Levels	High	Medium	Low

1	Catastrophic	major injury to driver, spectators
2	Critical	damage to property, and/or minor injury
3	Marginal	damage to vehicle only
4	Negligible	reparable damage to vehicle only, no injuries
A	Frequent	every time it is driven
B	Probable	with every race
C	Occasional	during/following repair
D	Remote	not expected during the life of the vehicle

Home

Example Mini-Baja HAR

Identify & Assess **Mitigate**

Hazard No.	Hazard	Frequency	Severity	Initial Risk Level	Mitigation	Final Risk Level
	Collisions					
1	Other Driver error	B	1	High	Restraint system, bumpers, side & rear-view mirrors, training	Medium
2	Steering Failure	D	2	Medium	Heavy-duty rack & pinion, bumper to cover steering	Low
3	Brake Failure	D	1	High	Emergency brake system, shut-off switches	Medium
4	Operator error	A	2	High	Restraint system, padded frame structure, bumpers, training	Medium
5	Rough terrain	B	3	Medium	Restraint system, padded frame structure, training	Low
	Fire					
6	Fuel spill	C	2	High	Firewall, fire extinguisher, looped fuel line system	Low
7	Engine damage	D	3	Low	Firewall, debri guard	Low
8	Welding error	C	2	High	Welding masks & gloves, fire extinguisher, isolated welding area	Low
	Projectiles					
9	Debris from terrain	B	3	Medium	Mud-guards, debri wall for whole cockpit	Low
10	Chain failure	B	3	Medium	Transmission cage	Low
11	Suspension failure	D	3	Low	Suspension limiters, bumper guards	Low
12	Engine explosion	D	1	High	Firewall, Engine cage, eye protection when working with engine	Medium

Frequency of Exposure	Severity			
	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	A1	A2	A3	A4
Probable (B)	B1	B2	B3	B4
Occasional (C)	C1	C2	C3	C4
Remote (D)	D1	D2	D3	D4

Risk Levels	High	Medium	Low
1	Catastrophic	major injury to driver, spectators	
2	Critical	damage to property, and/or minor injury	
3	Marginal	damage to vehicle only	
4	Negligible	reparable damage to vehicle only, no injuries	
A	Frequent	every time it is driven	
B	Probable	with every race	
C	Occasional	during/following repair	
D	Remote	not expected during the life of the vehicle	

Home

FMEA Template

Description of FMEA Worksheet

Protection:The spreadsheets are not protected or locked.

System _____
Subsystem _____
Component _____
Design Lead _____
Core Team _____

Potential Failure Mode and Effects Analysis (Design FMEA)

Key Date _____

FMEA Number _____
Prepared By _____
FMEA Date _____
Revision Date _____
Page _____ of _____

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
Coolant containment. Hose connection. Coolant fill. M	Crack/break. Burst. Side wall flex. Bad seal. Poor hose rete	Leak	8	Over pressure	8	Burst, validation pressure cycle.	1	64	Test included in prototype and production validation testing.	J.P. Aguire 11/1/95 E. Eglin 8/1/96					

Write down each failure mode and potential consequence(s) of that

Severity - On a scale of 1-10, rate the Severity of each failure (10= most severe). See Severity

Likelihood - Write down the potential cause(s), and on a scale of 1-10, rate the Likelihood of each failure (10= most likely). See

Detectability - Examine the current design, then, on a scale of 1-10, rate the Detectability of each failure (10 = least detectable). See Detectability sheet.

Risk Priority Number - The combined weighting of Severity, Likelihood, and Detectability. RPN = Sev X Occ X Det

Response Plans and Tracking

Relevance to Capstone

What are the risks and ***consequences***?

What are the failure modes for your design?

What are your mitigation tactics?

Document your findings concerning, and the process for addressing, these issues

Home

Product Liability Concepts

- Definition:
  - *Corporate liability for injuries or damages suffered by the user from products*
- Applies to manufacturers, sellers and distributors of goods
- *Liability:* An obligation to rectify or recompense for any injury or damage for which the liable person has been held responsible or for failure of a product to meet a warranty.

Home

Legal Theories

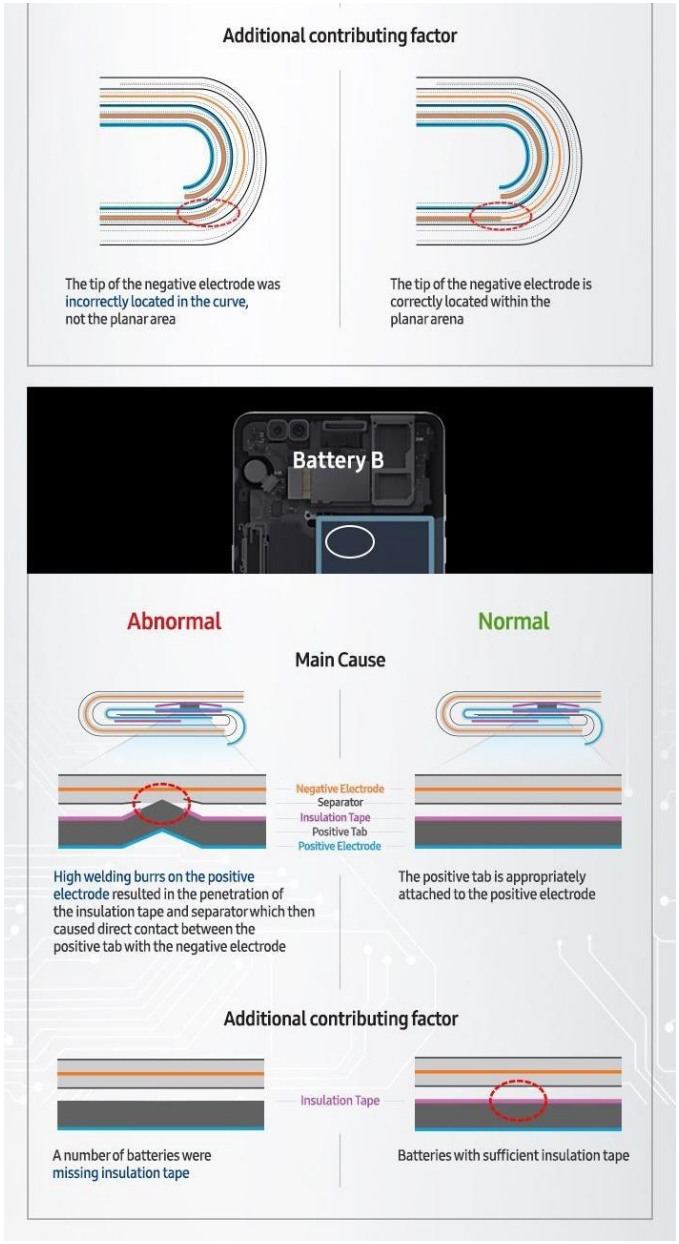
- Three theories in Product Liability cases:
  - *Strict Liability*
  - *Breach of Warranty*
  - *Negligence*

Home

Definitions & Concepts 1

- *Strict liability in tort:* The legal theory that a manufacturer of a product is liable for injuries due to product defects, without the necessity of showing negligence of the manufacturer.
  - Defect in design
  - Defect in manufacture

Definitions & Concepts 2

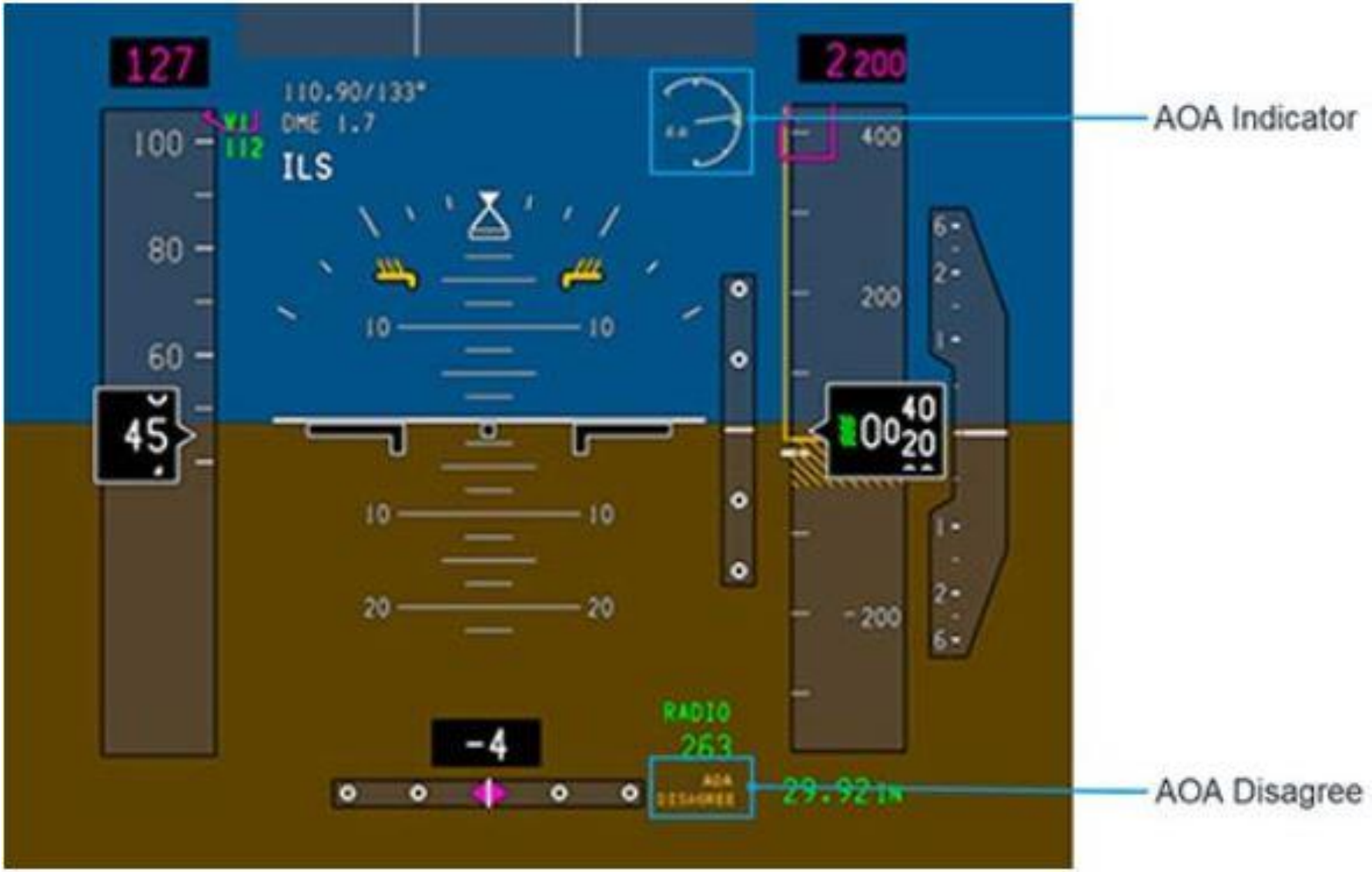


Home

Boeing 737 Max
Maneuvering Characteristics Augmentation System

Home

Home

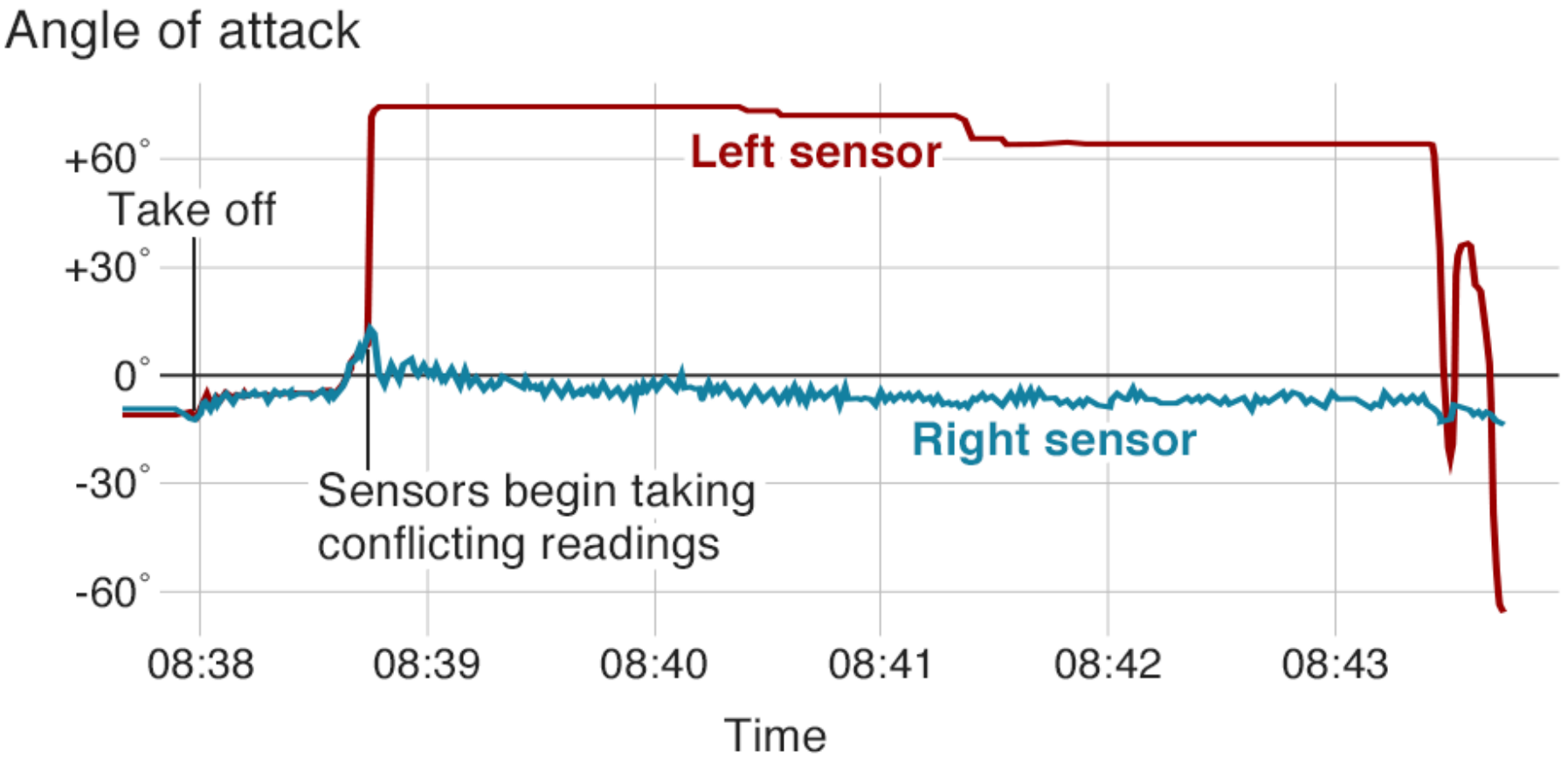


- *Optional* AoA disagreement indicator

- After recognition of problem by pilot
- Disable electric elevator trim
- Use manual trim wheel for pitch forces
  - Excessive load at high air speed
- Re-engaging electric trim re-enables MACS
- Cycle begins again…

Home

The plane's sensors took different readings



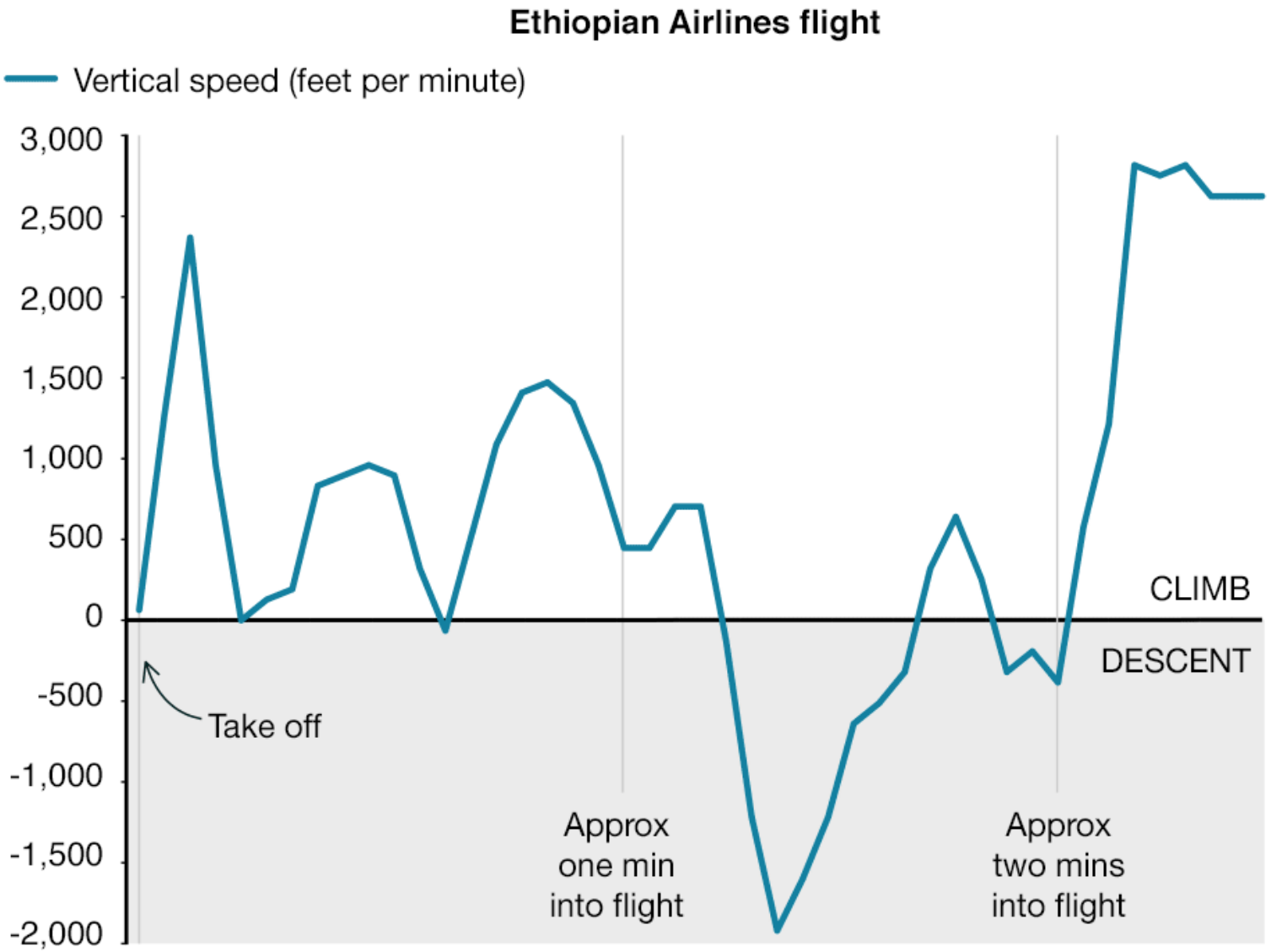
Source: Ethiopian Aircraft Accident Investigation Bureau

BBC

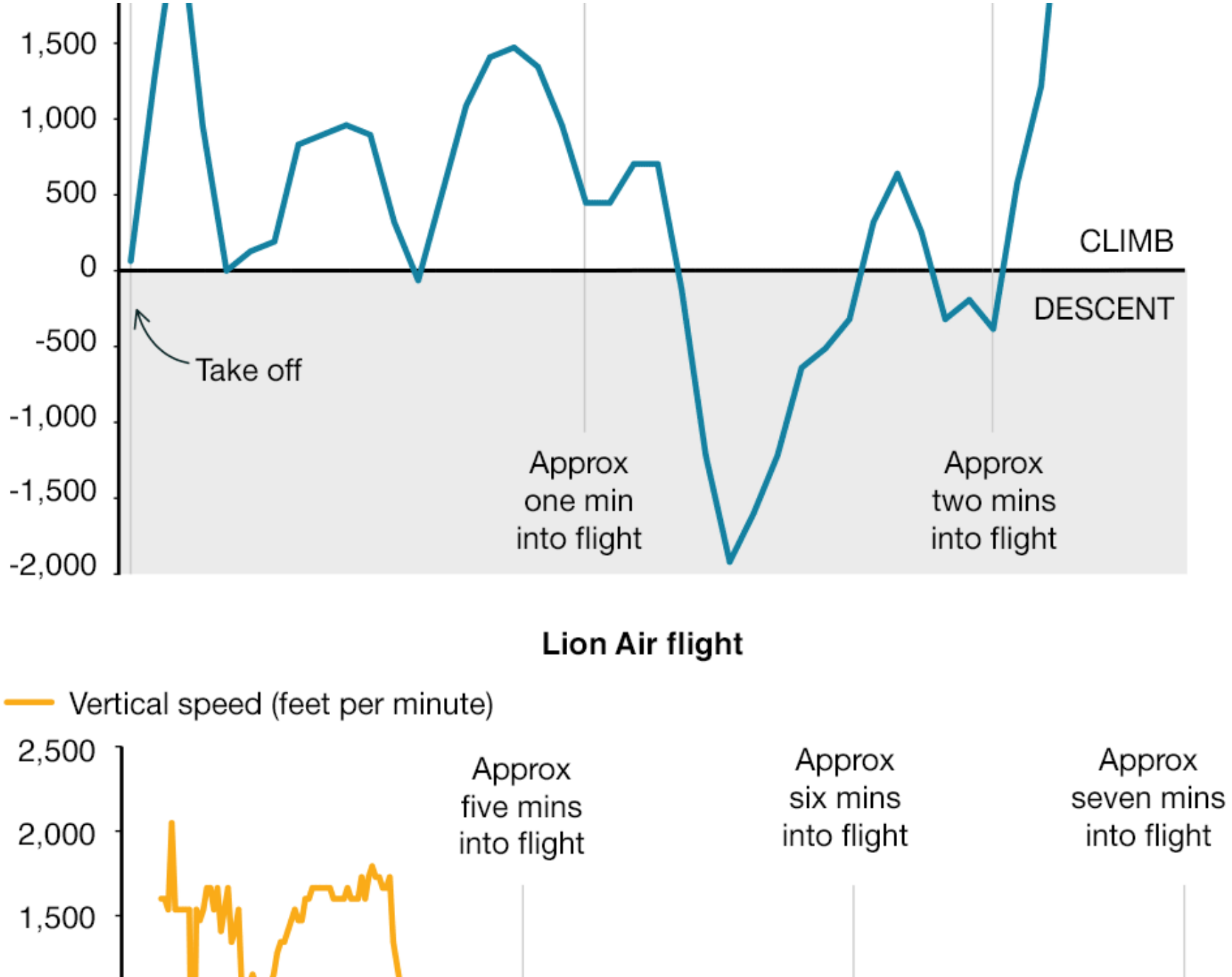
Home

Investigators say there are similarities between two 737 Max 8 crashes

Vertical speeds of Lion Air flight 610 and Ethiopian Airlines flight 302



Home


1,500
1,000
500
0
-500
-1,000
-1,500
-2,000
CLIMB
DESCENT
Take off
Approx
one min
into flight
Approx
two mins
into flight
Lion Air flight
Vertical speed (feet per minute)
2,500
2,000
1,500
Approx
five mins
into flight
Approx
six mins
into flight
Approx
seven mins
into flight

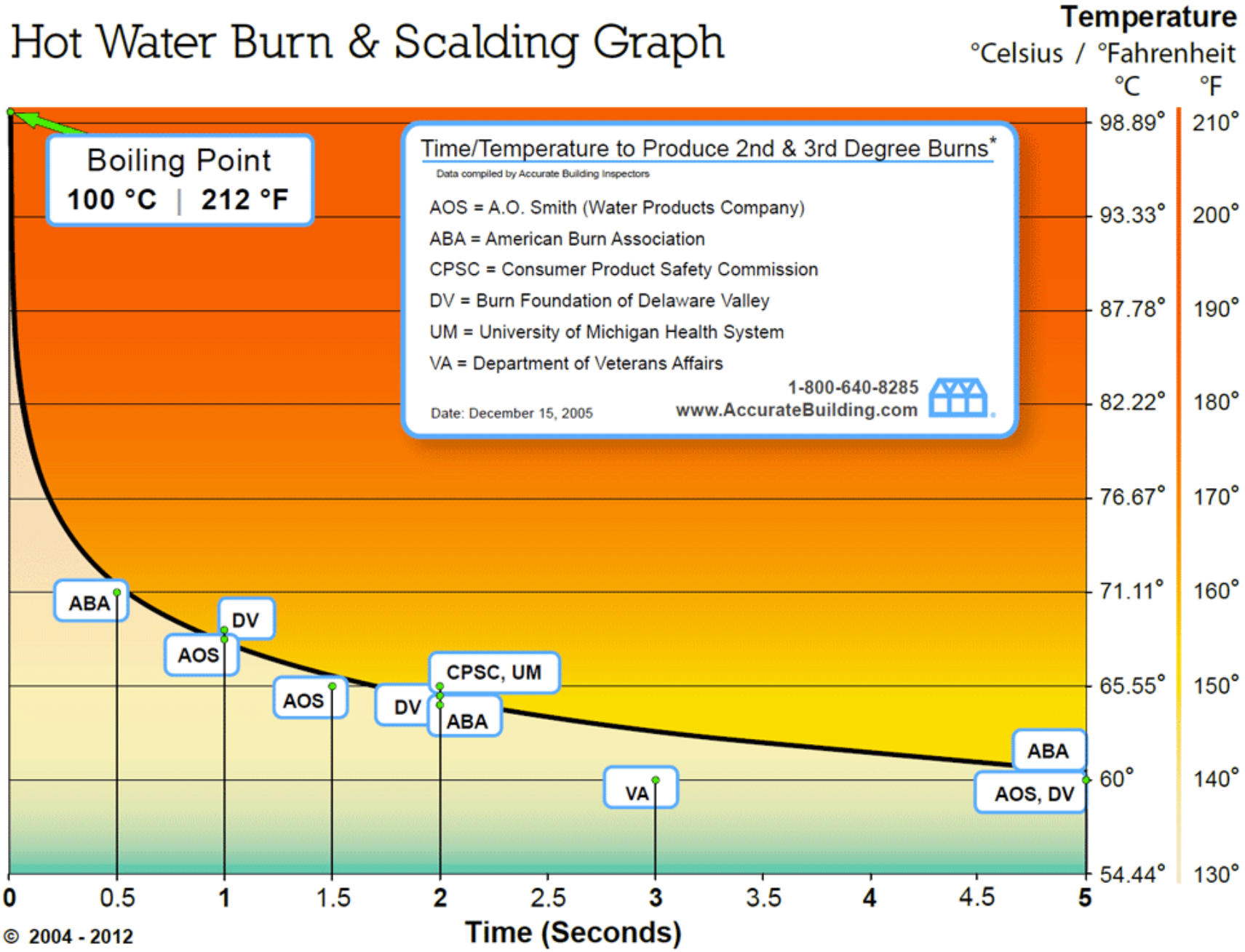
Definitions & Concepts 3

- *Breach of warranty:* Failure of the product to meet its warranty, be it either express or implied

- *Express warranty: A* statement by a manufacturer or seller, either in writing or orally, that his product is suitable for a specific use and will perform in a specific way.

- *Implied warranty:* An automatic warranty, implied by law, that a manufacturer's or dealer's product is suitable for either ordinary or specific purposes and is reasonably safe for use (“merchantability and fitness”; McDonald’s coffee-burn case)

Home


Hot Water Burn & Scalding Graph
Temperature
°Celsius / °Fahrenheit
°C
°F
Boiling Point
100 °C | 212 °F
Time/Temperature to Produce 2nd & 3rd Degree Burns*
Data compiled by Accurate Building Inspectors
AOS = A.O. Smith (Water Products Company)
ABA = American Burn Association
CPSC = Consumer Product Safety Commission
DV = Burn Foundation of Delaware Valley
UM = University of Michigan Health System
VA = Department of Veterans Affairs
1-800-640-8285
www.AccurateBuilding.com
Date: December 15, 2005
98.89°
93.33°
87.78°
82.22°
76.67°
71.11°
65.55°
60°
54.44°
210°
200°
190°
180°
170°
160°
150°
140°
130°
ABA
DV
AOS
AOS
CPSC, UM
DV
ABA
VA
ABA
AOS, DV
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
Time (Seconds)
© 2004 - 2012

Definitions & Concepts 4

- *Negligence:* Failure to exercise a reasonable amount of care or to carry out a legal duty which results in injury or property damage to another

- *Contributory negligence:* Negligence of the plaintiff that contributes to his injury and at common law ordinarily bars him from recovery from the defendant although the defendant may have been more negligent than the plaintiff

- *Negligence per se:* Breach of a regulation or a standard which was designed to prevent the type of harm suffered by the plaintiff

Home

Definitions & Concepts 5

- *Duty of care:* The legal duty of every person to exercise due care for the safety of others and to avoid injury to others whenever possible.

- *Great care:* The high degree of care that a very prudent and cautious person would undertake for the safety of others.

- *Reasonable care:* The degree of care exercised by a prudent person in observance of his legal duties toward others.

Home

Definitions & Concepts 6

- *Foreseeability:* The legal theory that a person may be held liable for actions that result in injury or damage only where he was able to foresee dangers and risks that could reasonably be anticipated.

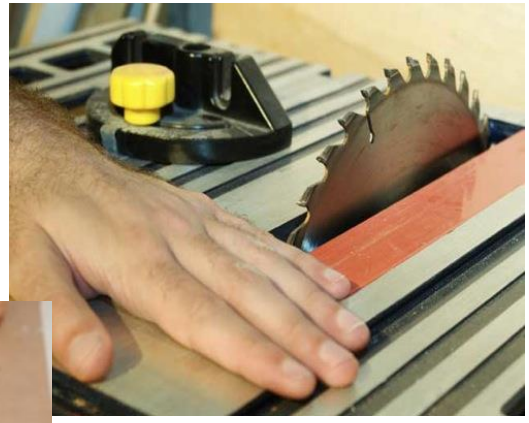
http://carpelibrisreviews.com/bialetti-moka-express-stovetop-coffee-maker-giveaway/

Home

Definitions & Concepts 7

- *Obvious peril:* The legal theory that a manufacturer is not required to warn prospective users of products whose use involves an obvious peril, especially those that are well known to the general public and that generally cannot be designed out of the product.

http://www.norriscantulaw.com/defective-products/



http://www.michaels-smolak.com/lawyer-attorney-1501239.html

http://www.conybearelaw.com/practice-areas/product-liability/

http://www.arizonapilawyer.com/personal-injury/defective_product.html

Home

Definitions & Concepts 8

- *Assumption of risk:* The legal theory that a person who is aware of a danger and its extent and knowingly exposes himself to it assumes all risks and cannot recover damages, even though he is injured through no fault of his own.

Assumed Risk

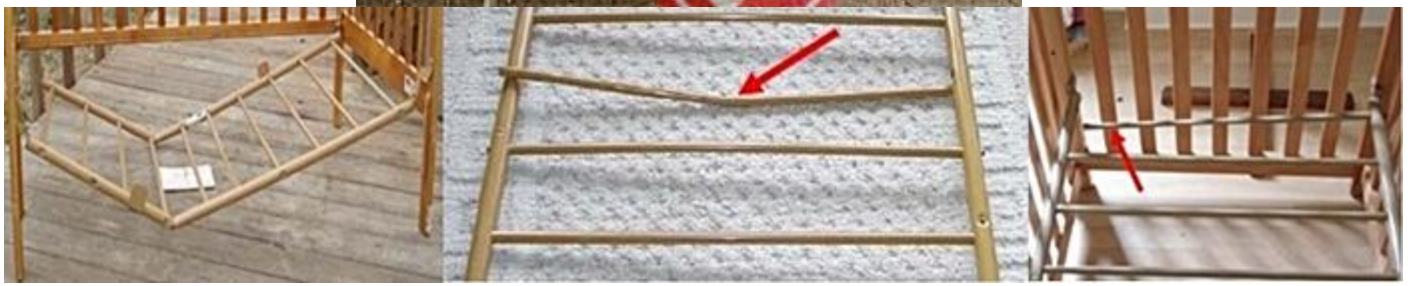
•A person who is aware of a danger and its extent and knowingly exposes himself to it assumes all risks and cannot recover damages, even though he is injured through no fault of his own.
•But may recover under other theory, e.g., negligence or breach of warranty

www.historicbanningmills.com

Home

Liability suits to come?

- http://www.recalls.gov/recent.html
- http://www.cpsc.gov/



Home

HYATT REGENCY WALKWAY COLLAPSE

http://www.materials.drexel.edu/programs/Sensors/Links/

INTRODUCTION

- On July 17, 1981, two suspended walkways collapsed in the Hyatt Regency Hotel in Kansas City, Missouri during a dance festival
- 114 dead and in excess of 200 injured.
- Millions of dollars in costs related to lawsuits, etc., resulted from the collapse, and hundreds of lives were adversely affected.

HYATT REGENCY WALKWAY COLLAPSE

Home

HYATT REGENCY WALKWAY COLLAPSE

- Original
- Walkways suspended long rods.
- Rod through the top walkway down to bottom walkway.
- On each rod, under each walkway, nut used to carry the load of walkway.
- Issue
- Running nuts 30 feet up the rods, the entire length of the rods had to be threaded.
- Threading 30 feet of rod difficult and costly.
- The fabricator decided to modify the original design to make it easier and less costly to construct.

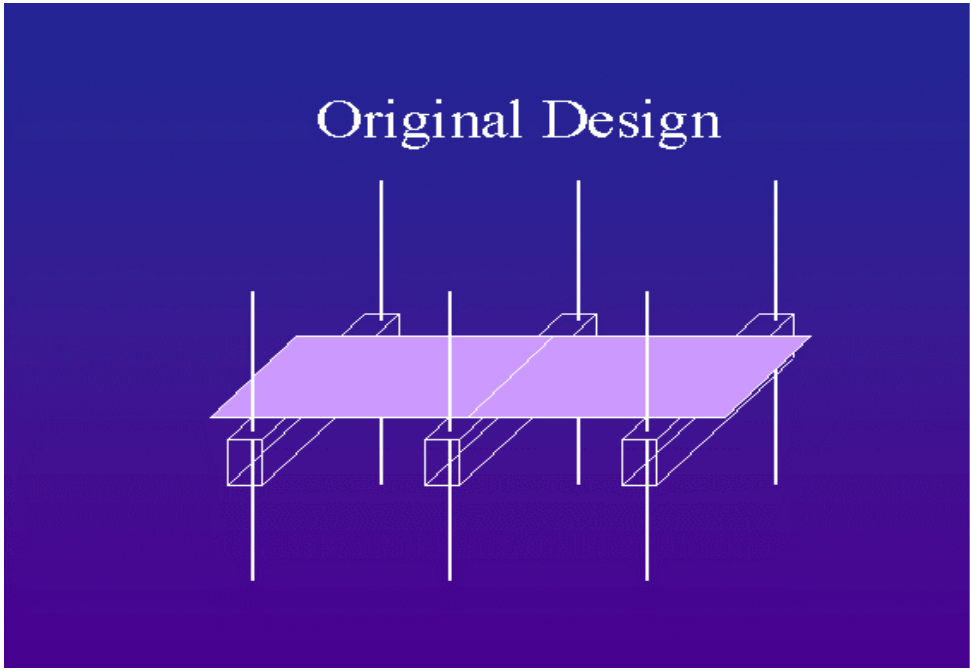
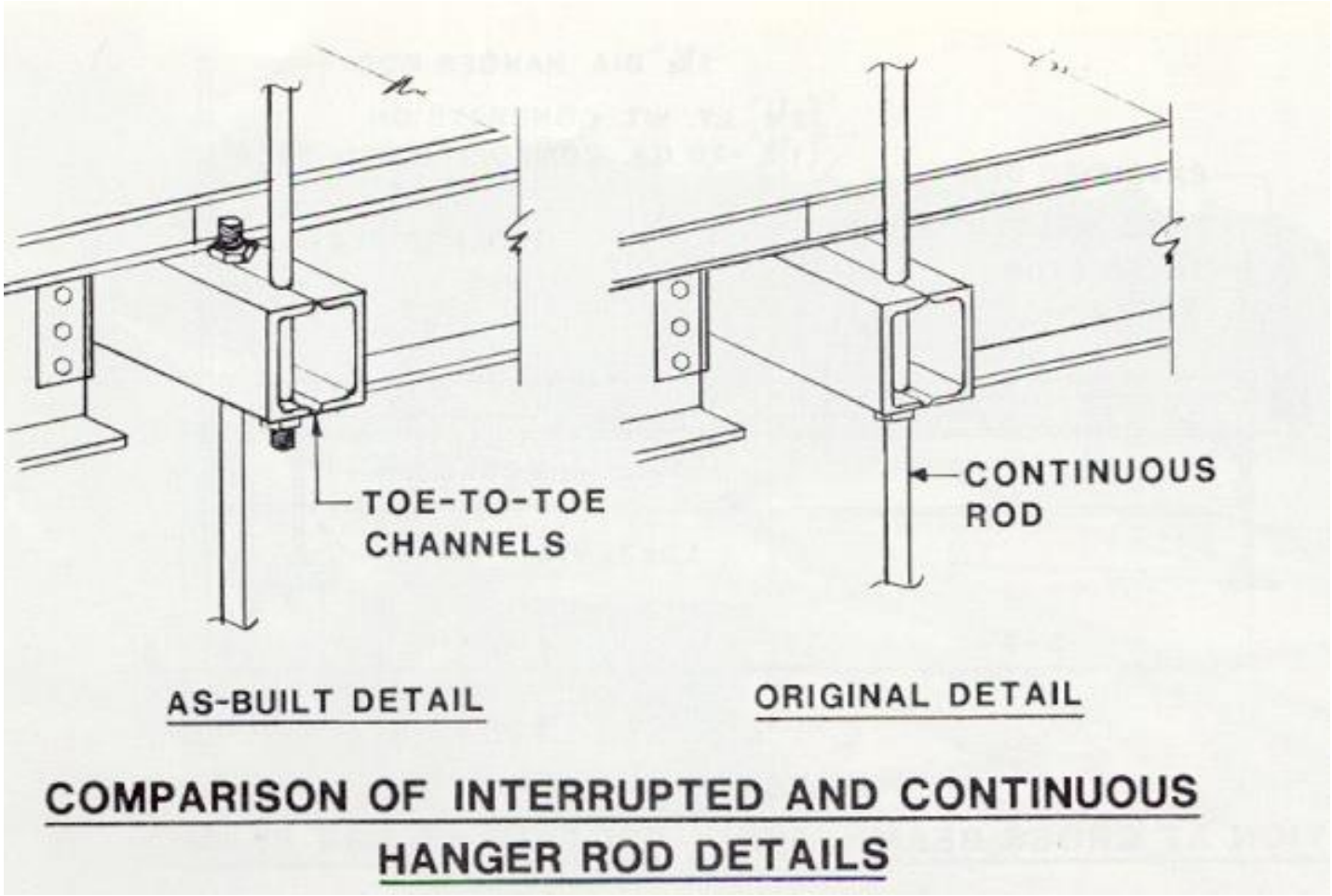


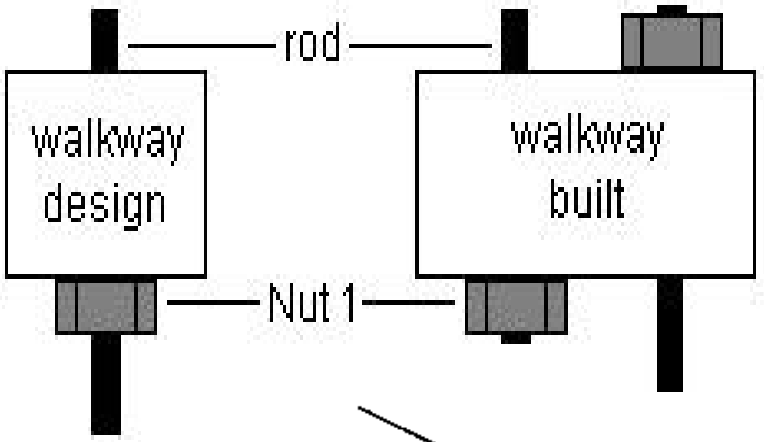
Figure 1

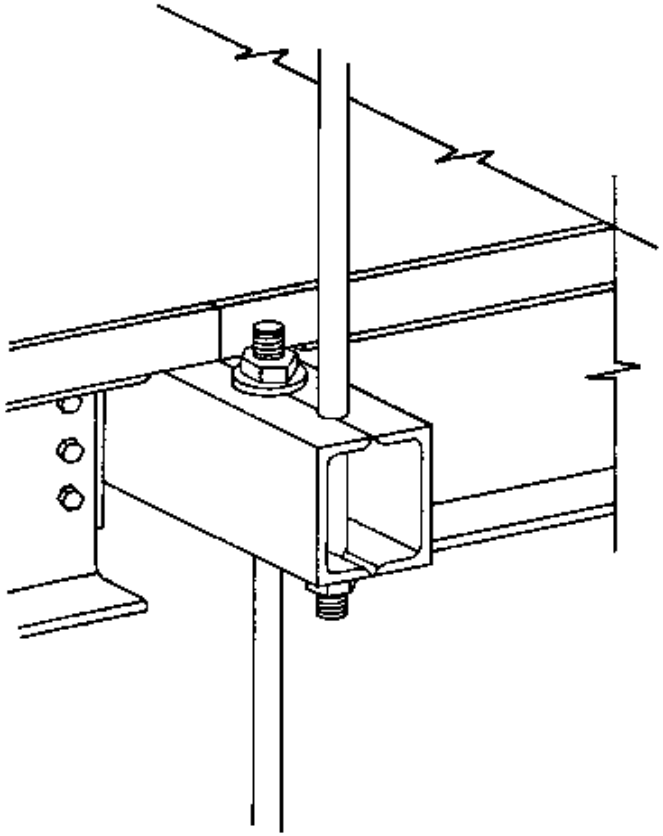


COMPARISON OF INTERRUPTED AND CONTINUOUS HANGER ROD DETAILS

Home

THE TWO SUPPORT MODELS

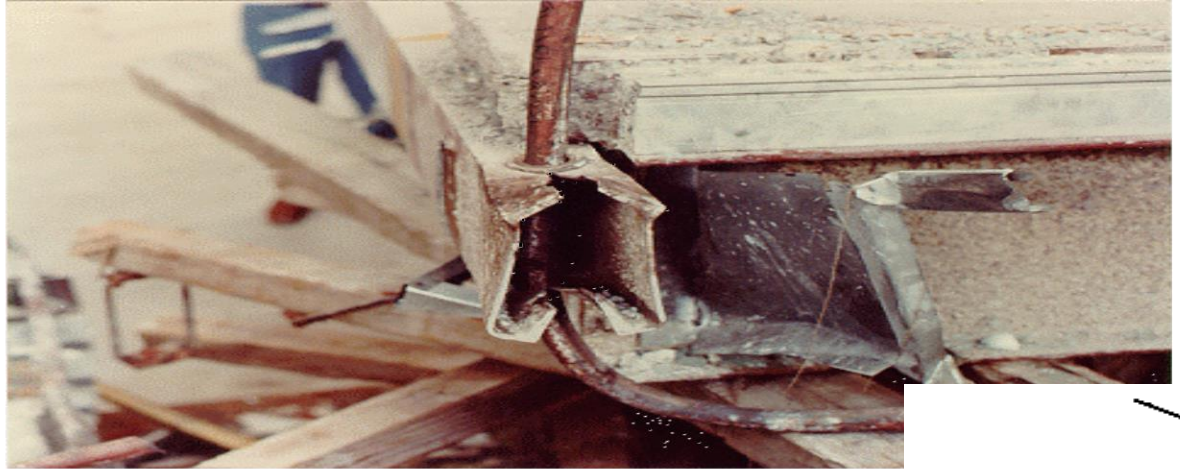


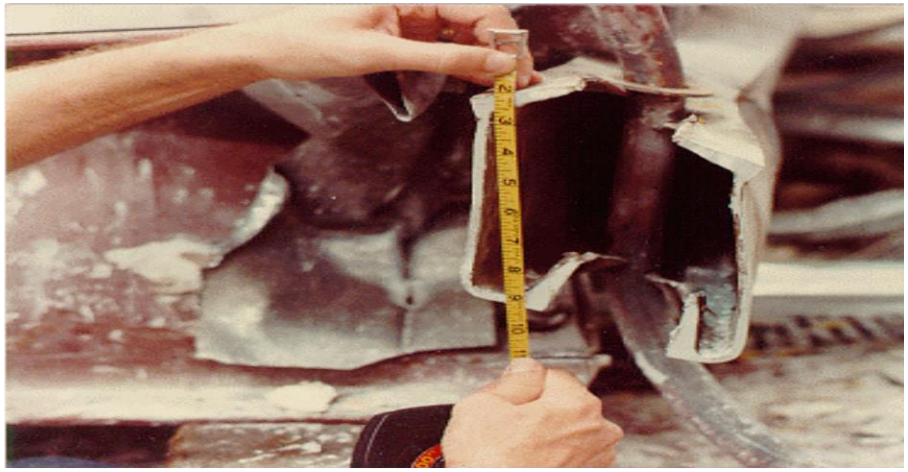


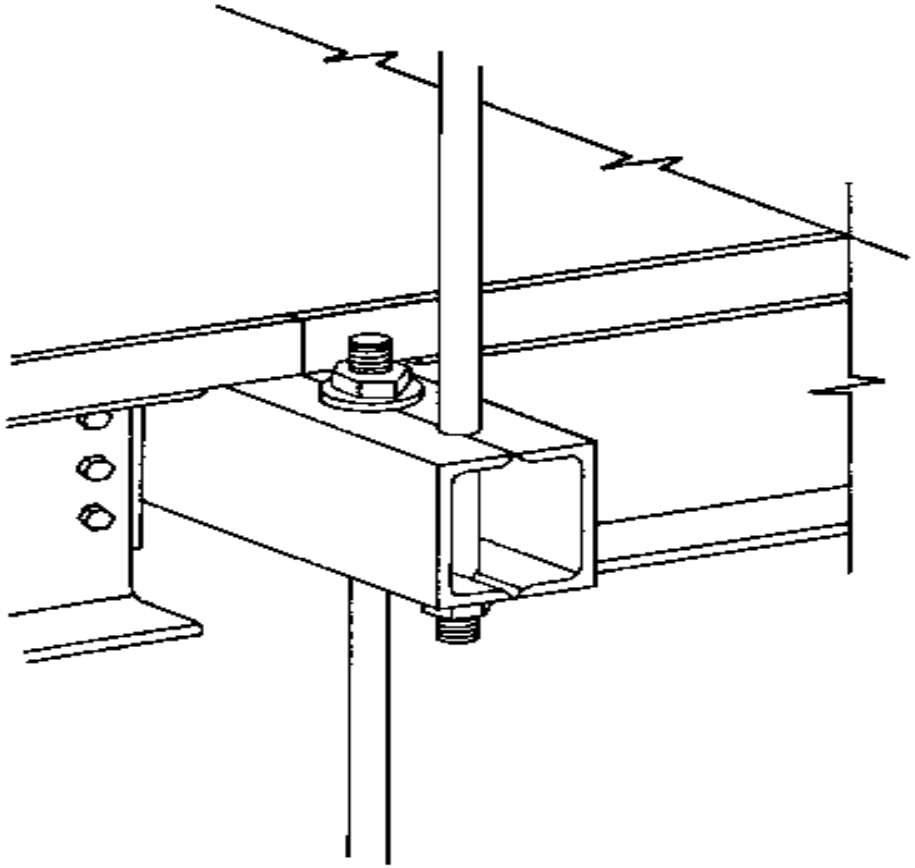
- Walkway-design: Nut 1 supports only the walkway above it. The weight of the second walkway is supported through the rod.

- Walkway-built: Nut 1 not only holds the weight of the walkway above it, but also the hanging weight of the second walkway and the rods used to support it.

Home







Deformed 4th Floor Beam

Home

HYATT REGENCY WALKWAY COLLAPSE
Negligence Per se

- Failure of either design to meet Kansas City Building Codes
- KCBC dictated minimum value for mean ultimate load capacity for beams should be 151 kN.
- The mean ultimate capacity of the single-rod connection approximately 91 kN, depending on the weld area
- Capacity actually available using the original connection 60% of that expected of a connection designed in accordance with AISC Specifications
- Modified and as-built design held 30% of the minimum weight by KCBC

- By mere calculations, the first design was obviously the more effective one even though it was faulty to begin with
- How many legal theories of liability apply?

Relevance to Capstone

What are the failure modes for your design?

What are the risks and consequences?

What are your risk mitigation tactics?

What Codes & Standards apply?

Document your findings concerning, and the process for addressing, these issues

Home

Home

Coverage/Contents

- Product Liability
- Hazards and Risk Assessment
- Failure Modes and Effects Analysis FMEA

- Backup materials
  - Citations and links (in progress…)
  - Liability
  - FMEA

Home

Citations and links

- References
  - *What every engineer should know about product liability,* Thorpe and Middendorf, Marcel Dekker, Inc., New York, NY, 1979.
  - *Fundamentals of product liability law for engineers*, Enghagen, Industrial Pres, Inc., New York, NY, 1992.
  - *Products Liability, Smith's Review,* Finz, Emanual Law Outlines, Inc., Larchmont NY,1993.
  - *Products liability: Design and Manufacturing Defects*, Bass, Shepard's/McGraw Hill, Colorado Springs, CO, 1986. (this one is quite a weighty tome)
  - *Designing an effective Risk Matrix,* An ioMosaic Corporation Whitepaper, Salem, NH, 2009.

- Source materials
  - Materials on ethics and liability, including the KC Hilton
  - Ethics & FMEA

Home

Legal Theories
Definitions and Concepts (support)

- "Causes of action"
- *Legal theory under which plaintiff believes damages should be awarded*
- Basis of court's jurisdiction (civil law; state & Fed)
- Required conditions for an action:
  - *Tort: A* wrongful act or failure to exercise due care, from which a civil legal action may result.
  - *Proximate cause:* The act that is the natural and reasonably foreseeable cause of the harm or event that occurs and injures the plaintiff.

Home

Additional materials on legal aspects

Home

Recoverable Damages

- Personal injuries
  - *Past, present and future*
- Fair and adequate compensation
- Medical expenses
- Lost earnings
- Pain and suffering
- Impaired future earnings capacity
- Property damage
- Punitive damages
  - *(most states)*

Home

Punitive Damages

- Awarded to Plaintiff over and above full compensation for injuries
- Intended to “punish” defendant and “deter” others from following the defendants example
- Example:
  - *Coffee spill cases*
  - *Airline crashes*

Home

Strict Liability

- Liability without fault
- Proximate Causation

Home

Negligence

- Failure to exercise reasonable care under circumstances
- Contributory Negligence
- Duty, breach, damages

“Negligence Per Se”

- Violation of a regulation which was designed to prevent the type of harm suffered by the plaintiff
- E.g., design not conforming to standards, not conforming to regulation

Breach of Warranty

- Manufacture liable if product was not *"reasonably safe"* and did not conform to an express or implied warranty
- Strict liability if warranty breached
- Express vs. Implied Warranties
  - Express = *"basis of the bargain"*
  - Implied = given by someone *"in the business of selling"*

Home

Negligence

- The law of negligence imposes a duty to think before you act.
- The ordinary care standard imposes a social standard which is judged by members of the community who may or may not agree with your evaluation of your own conduct.
- Therefore, it is important to look at your acts and omissions from the stand point of others in the community who will be judging your conduct.
- If you have negligence concerns, ask:
- 1. What would members of the community require me to do under these circumstances;
- 2. What would members of the community forbid me to do under these circumstances;
- 3. What would members of my profession/vocation/calling require of me under these circumstances;
- 4. What would members of my profession/vocation/calling counsel me to avoid under these circumstances;
- 5. What are the risks of my conduct, considering the probability of harm and the degree of injury or damage that would result if an accident occurred; and
- 6. Would ordinary people in the community believe that I am taking reasonable risks?

Proving Negligence

- Negligence is 'conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm' [4].
- In order to establish liability for damage, the courts analyze the following four elements:
  - duty
  - breach
  - proximate cause
  - damages.

Proving Negligence

Negligence: the injured party (plaintiff) must prove:

- a) that the party alleged to be negligent had a duty to the injured party-specifically to the one injured or to the general public,
- b) that the defendant's action (or failure to act) was negligent-not what a reasonably prudent person would have done because it did not fulfill the “standard of care” typical of how any similar engineer would judge and act in similar situations
- c) that the damages were caused ("proximately caused") by the negligence.
- d) That the damages were "reasonably foreseeable" at the time of the alleged negligence.

Standard of Care

- In legal cases, a judge or jury, has to determine what the standard of care is and whether an engineer has failed to achieve that level of performance.
- They do so by hearing expert testimony.
- People who are qualified as experts express opinions as to the standard of care and as to the defendant engineer's performance relative to that standard.
- The testimony from all sides is weighted and then a decision is made what the standard of care was and whether the defendant met it

Standard of Care

- Jury instructions have been standardized. A Bench Approved Jury Instruction (BAJI, 1986) reads:
- "In performing professional services for a client, a (structural engineer) has the duty to have that degree of learning and skill ordinarily possessed by reputable (structural engineers), practicing in the same or similar locality and under similar circumstances.
- It is (the structural engineer's) further duty to use the care and skill ordinarily used in like cases by reputable members of the (structural engineering) profession practicing in the same or similar locality under similar circumstances, and to use reasonable diligence and (the structural engineer's) best judgment in the exercise of professional skill and in the application of learning, in an effort to accomplish the purpose for which (the structural engineer) was employed.
- A failure to fulfill any such duty is negligence"

Standard of Care

Three key items in this instruction bear repeating:

1. ...have learning and skill ordinarily possessed by reputable engineers practicing in the same or similar locality and under similar circumstances.
2. ...use care and skill ordinarily possessed by reputable engineers practicing in the same or similar locality and under similar circumstances.
3. ...use reasonable diligence and best judgment to accomplish the purpose for which the engineer was employed.

- If any one of these conditions is not met, the engineer has failed to meet the standard of care, and is professionally negligent.

Comparative Negligence

- Negligence involving joint tortfeasors
  Joint Tortfeasors (wrongdoers): two or more persons whose negligence in a single accident or event causes damages to another person.
- In many cases the joint tortfeasors are jointly and severally liable for the damages, meaning that any of them can be responsible to pay the entire amount, no matter how unequal the negligence of each party was.
- Example: Harry Hotrod is doing 90 miles an hour along a two-lane road in the early evening,
- Adele Aimster has stopped her car to study a map with her car sticking out into the lane by six inches.
- Hotrod swings out a couple of feet to miss Aimster's vehicle, never touches the brake, and hits Victor Victim, driving from the other direction, killing him.
- While Hotrod is grossly negligent for the high speed and failure to slow down, Aimster is also negligent for her car's slight intrusion into the lane. As a joint tortfeasor she may have to pay all the damages, particularly if Hotrod has no money or insurance.
- However, comparative negligence rules by statute or case law in most jurisdictions will apportion the liability by percentages of negligence among the tortfeasors and the injured parties.

Res Ipsa Loquitur
(The Thing Speaks for Itself)

- (rayz ip-sah loh-quit-her) n. Latin for "the thing speaks for itself,"
- A doctrine of law that one is presumed to be negligent if he/she had exclusive control of whatever caused the injury even though there is no specific evidence of an act of negligence, and without negligence the accident would not have happened.
- Examples: a) a load of bricks on the roof of a building being constructed by High-rise Construction Co. falls and injures Paul Pedestrian below
- High-rise is liable for Pedestrian's injury even though no one saw the load fall.
- b) While under anesthetic, Isabel Patient's nerve in her arm is damaged although it was not part of the surgical procedure, and she is unaware of which of a dozen medical people in the room caused the damage.
- Under res ipsa loquitur all those connected with the operation are liable for negligence.
- Lawyers often shorten the doctrine to "res ips," and find it a handy shorthand for a complex doctrine.

Negligence Per Se

- Negligence due to the violation of a public duty, such as high speed driving.
- In Black's Law Dictionary negligence 'per se' is defined as: "Conduct, whether of action or omission, which may be declared and treated as negligence without any argument or proof as to the particular surrounding circumstances, either because it is in violation of a statute or valid municipal ordinance, or because it is so palpably opposed to the dictates of common prudence that it can be said without hesitation or doubt that no careful person would have been guilty of it. As a general rule, the violation of a public duty, enjoined by law for the protection of person or property, so constitutes."

Details on FMEA

Home

What is FMEA?

- FMEA is an acronym that stands for
  Failure Mode and Effects Analysis
- Methodology of FMEA:
  - ***Identify*** *the potential failure of a system and its effects*
  - ***Assess*** *the failures to determine actions that would eliminate the chance of occurrence*
  - ***Document*** *the potential failures*

FMEA

- The aim of FMEA is to ***anticipate***:
  - what might *fail*
  - what *effect* this failure would have
  - what might *cause* the failure

… and take action to correct it!

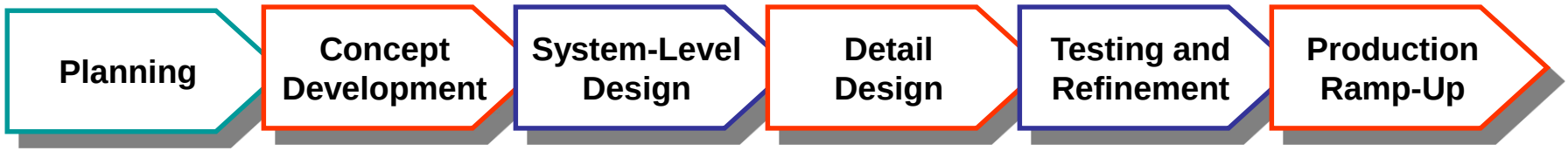
Home

FMEA

- The ***significance*** of the failure is assessed against:
  - The ***probability of failure***
  - An ***assessment of the severity*** of the effect of that failure
  - The ***probability of*** existing quality systems ***spotting the failure before it occurs (detection)***

Home

Where Does FMEA Occur?



Concept FMEA

(CFMEA)

Design FMEA

(DFMEA)

Process FMEA

(PFMEA)

Design Project FMEA

- Design FMEA's should cover:
  - all new components
  - carried over components in a new environment
  - any modified components
- Mandatory on all control and load carrying parts

Home

FMEA Process

For *each component*

1. Identify a *failure mode*
2. Determine the *possible effects* or *consequences* of the failure
3. Assess the *potential severity* of the effect
4. Identify the *cause of failure* (take action!)
5. Estimate the *probability of occurrence*
6. Assess the *likelihood of detecting* the failure

1. Failure Mode

- ***Failure mode*** - the manner in which a component or system failure occurs *(doesn't meet design intent)*
- Potential ***failure modes***
  - Complete failure
  - Partial failure
  - Intermittent failure
  - Failure over time
  - Over-performance failure

Failure Mode - Identification

- List ***potential failure modes*** for the particular part or function
  - assume the failure *could* occur, however unlikely
- For example, sketch free-body diagrams (if applicable), showing applied/reaction loads. Indicate ***location of failure*** under this condition.
- List conceivable ***potential causes of failure*** for each failure mode

2. Failure Mode – Effects

- For each failure mode, identify the potential downstream consequences of each failure mode (the ***Effects***)

- Team brainstorms to identify failure modes and effects

FM-1	Effect 1-1
	Effect 1-2
	Effect 1-3
FM-2	Effect 2-1
	Effect 2-2

3. Failure – Severity

To analyze *risk*, first ***quantify the severity*** of the Effects

- Assume that all Effects will result if the Failure Mode occurs
- Most serious Effect takes precedence when evaluating risk potential
- Design and process changes can reduce severity ratings

DFMEA Severity Table

Severity of Failure	Rank
Hazardous – No warning: Unsafe operation, without warning	10
Very high: Product inoperable; loss of primary function	8, 9
High: Product operable, but at a reduced level	6, 7
Low: Product operable; comfort or convenience items at reduced level	4, 5
Minor: Fit/finish, squeak/rattle don't conform; average customer notices	2, 3
No effect	1

4. Failure Mode – Causes

- After Effects and Severity addressed, identify the ***Causes*** of the Failure Modes
- Causes of failure that result in a Failure Mode are ***design deficiencies***
- Causes are rated in terms of ***Probability of Occurrence***
  - Likelihood that a given Cause will occur AND result in the Failure Mode

5. Failure Mode - Occurrence

- Estimate the ***probability of occurrence*** on a scale of 1 -10
  - consider any fail-safe controls intended to prevent cause of failure
- Consider the following two probabilities:
  1. *probability the potential cause of failure will occur*
  2. *probability that once the cause of failure occurs, it will result in the indicated failure mode*

Failure Occurrence - Ranking

Occurrence Criteria	Rank
Very High – almost certain failure, in a major way	10
High – similar designs have failed in the past	7, 8, 9
Moderate – similar designs have occasional moderate failure rates	4, 5, 6
Low – similar designs have low failure rates	2,3
Remote - unreasonable to expect failure	1

Example DFMEA Occurrence Table

Probability of Failure	Failure Rates	Rank
Very High: Failure almost inevitable	≥ 1 in 2	10
	1 in 3	9
High: Repeated failures	1 in 8	8
	1 in 20	7
Moderate: Occasional failures	1 in 80	6
	1 in 400	5
	1 in 2000	4
Low: Relatively few failures	1 in 15,000	3
	1 in 150,000	2
Remote: Failure unlikely	≤ 1 in 1,500,000	1

Current Controls

- Design controls grouped according to purpose
  - **Type 1 Controls:** *prevent* Cause or Failure Mode from occurring, or reduce rate of occurrence
    - Ex: Shear pin designed to fail to keep system from failing
  - **Type 2 Controls:** *detect* Cause of Failure Mode and lead to corrective action
    - Ex: LED lights when batteries are low
  - **Type 3 Controls:** *detect* Failure Mode before product reaches “customer”
    - Ex: 100% inspection

6. Detection

- *Detection values* are associated with type of Controls
- ***Detection*** is a measure of Type 2 Controls to detect Causes of Failure, or ability of Type 3 Controls to detect subsequent Failure Modes
- High values indicate a *Lack of Detection*
- Value of 1 does not imply 100% detection

DFMEA Detection Table

Detection	Criteria: Likelihood of Detection	Rank
Absolute Uncertainty	Design Control does not detect, or there is no Design Control	10
Very Remote	Very remote chance Control will detect	9
Remote	Remote chance Control will detect	8
Very Low	Very low chance Control will detect	7
Low	Low chance Control will detect	6
Moderate	Moderate chance Control will detect	5
Moderately High	Mod. High chance Control will detect	4
High	High chance Control will detect	3
Very High	Very high chance Control will detect	2
Almost Certain	Control almost certain to detect	1

Home

Design Project FMEA - RESULTS

- **Risk Priority Number (RPN)**

$$RPN = S \times O \times D$$

S = Severity, O = (Probability of) Occurrence, D = Detection

  - Note: S, O, and D are not equally weighted in terms of risk, and individual scales are not linear

Interpreting the RPN

- No physical meaning to RPN
- Used to “bucket problems”
- Rank order according to RPN
- Don’t spend a lot of time worrying about what a measure of “42” means
- Note that two failure modes may have the same RPN for far different reasons:
  - S=10, O=1, D=2: RPN = 20
  - S=1, O=5, D=4: RPN = 20

Criticality (Another Measure)

Criticality = S x O

- High *Severity* values, coupled with high *Occurrence* values merit special attention

  (*Detection* has been omitted from the RPN)
- Although neither RPN nor Criticality are perfect measures, they are widely used for risk assessment

Reducing Risk

The *fundamental purpose* of the FMEA is to *recommend and take actions* that reduce risk

- Design revision may result in lower Severity and Occurrence ratings
- Revised ratings should be documented with originals in Design History File

Actions

Actions taken are the important part of FMEA

1. Change design to reduce:
   - *Severity* (consider redundancy?)
   - *Occurrence* (change in design, or processes)
   - *Detection* (improve ability to identify the problem before it becomes critical)
2. Assign responsibility for action
3. Follow up and assess result with new RPN

FMEA DOCUMENT

	Failures			Cause		Detection		
Item	Potential Failure Mode	Effect	Severity	Casue	Occurance	Design control	Detection	RPN

Home

FMEA DOCUMENTATION

FMEA																
	Failure			Cause		Detection		Action			Action Results					
Item/ Function	Potential Failure Modes	Potential Effect of Failure	Severity	Potential Cause	Occurrence	Current Design Control	Detection	Risk Priority Number	Recommended Action	Responsibility	Action Taken	S	O	D	RPN
Deposit Ink	Too little Ink	No printing	7	Clogged Heads	4	None - instructions to user to regularly clean heads	3	**84**	design change to reduce chance of clogged heads	Ink head design team	More Robust Design	7	2	2	28
			7	Low Ink Levels	4	Ink Level light	1	**28**	None						
	Too much Ink	Can't read letters	8	Failure in Print head	2	Internal controls	3	**48**	Failure analysis	Ink head design team	Improved Control Algorithm	8	1	1	8

Home

FMEA

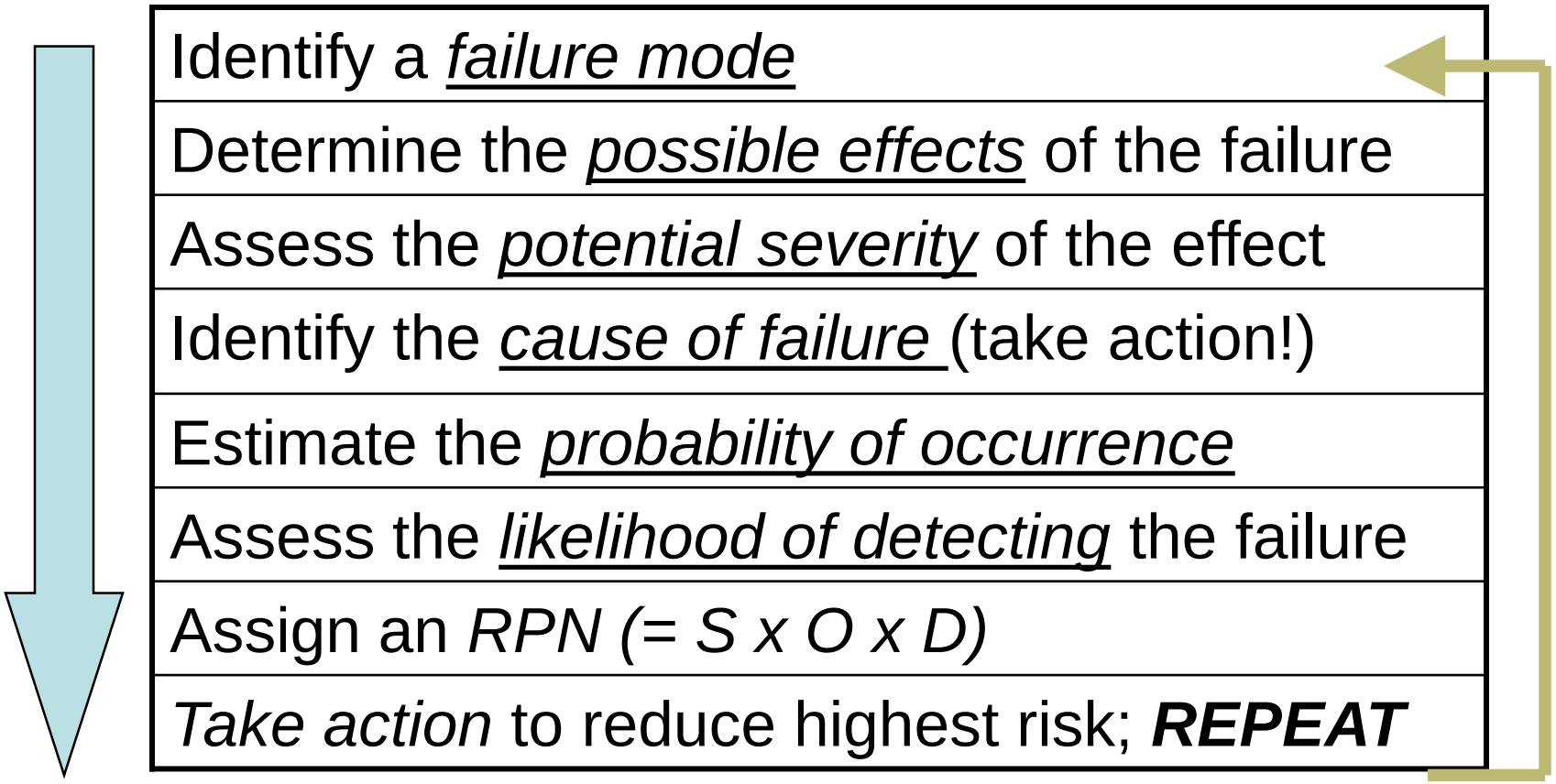
Benefits

- Systematic way to manage risk
- Comprehensive
- Prioritizes risk management actions

Problems

- Based on qualitative assessment
- Can be unwieldy
- Hard to trace through levels
- Not always followed up

Summary - FMEA Flowchart



Home

OTHER BACKUPS

Home

MISTAKES

Could It Be that the Purpose of Your Capstone Project Is Only To Serve As A Warning To Others?

www.despair.com

Home