Engr2110

Week 6 Product Safety/Liability
Why women live longer than men?
Product Safety

Not just human loss or injury

- Effect on other devices
- Impact on environment in case of failure
Safety Considerations

• All products have some degree of safety risk

• If your product poses significant risks, then you should perform a thorough safety analysis (more than putting safety in HOQ)

• “Design for Safety’
Safety Analysis

• What can go wrong with the product?

• What are the consequences of product failure?

• What is the probability of failure?

• How can risk be reduced?
Safety Considerations

• When is the most useful time to perform a safety analysis? Why?

• Design phase
  • potential hazards can be eliminated and risks reduced
Safety Considerations

• Design phase is the most difficult time to analyze safety. Why?
  • Limited amounts of quantitative data on failure rates and failure consequences

• What can be done to compensate for this?
  • Theoretical predictions (assumptions)
  • Computer simulations
  • Design experience
  • Experimental testing
Design for Safety Phases

• Problem Identification
• Risk Identification
• Risk estimation
• Risk evaluation
• Design Review
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

* Should be augmented by safety concerns that arise from your specific design project
Product Safety

• Design safety directly into product

• Add protective devices to product eg.

• Warnings of the dangers inherent in the use of the product
Design for Safety

• Should we use qualitative or quantitative measures?
  • May include either or both

• How do you decide what specific methods to apply in each phase?
  • Depends on the product being developed
Design in Safety

• Cannot rely on warning labels or operator training to make your product safe

• If known safety hazard then modify design to eliminate or reduce risk and consequences associated with the product
Design in Safety

Significant Risk of tip over when cherry picker is raised to its working height
Design in Safety

Device has stabilizing arms that extend outward, contact the ground and make a wider more stable base, WHAT can we do to ensure these are used when they should be used?
Utilizing Guards

• Many products must contain dangerous components to provide the desired function
  – Eg. lawnmower

• What guards in the lawnmower design keep the operator and people in the vicinity safe?
Operator Error

- Can’t assume operators will be highly trained and they will use the machine in a consistent manner.

- What are some new design solutions for operator error for automobiles?
Restrict Improper Use

• Every product you design will occasionally be used improperly eg. lawnmowers
• What are ways you have used products improperly?
• Your job is to make it impossible for the user to accidentally use your device in an unsafe manner
Unusual conditions

• Cherry picker may operate in rain, strong winds, ground may not be firm

• What can be done to eliminate the need for the operator to place wood underneath the stabilizing arms?
Redundancy

• 18 wheel tractor trailer-blowout, the remaining tires can carry the load

• Other examples?
Safe Failure Modes

• Design such that when the product does wear out or malfunction, it fails in a safe manner. Segway??

• Facilitating maintenance
  – Low cost, easy increases chances it will be performed

• Warning labels or systems
  – Weakest safety measure, exhaust all others before implementing
Hazard/Risk Assessment Matrix

• Why?
  – Safety in design
  – Well documented acceptable tool for risk assessment (Litigation protection)

• Standards Organizations
  – OSHA, FAA, NTSB, ISO, EPA, JCSS (look up acronyms)
## Hazard Assessment Matrix

### MIL-STD-882D

### Hazard Severity Categories

<table>
<thead>
<tr>
<th>Description</th>
<th>Category</th>
<th>Environmental, Safety, and Health Result Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>I</td>
<td>Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.</td>
</tr>
<tr>
<td>Critical</td>
<td>II</td>
<td>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.</td>
</tr>
<tr>
<td>Marginal</td>
<td>III</td>
<td>Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigable environmental damage without violation of law or regulation where restoration activities can be accomplished.</td>
</tr>
<tr>
<td>Negligible</td>
<td>IV</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Hazard Assessment Matrix

**MIL-STD-882D**

#### Hazard Probability Levels

<table>
<thead>
<tr>
<th>Description</th>
<th>Level</th>
<th>Specific Individual Item</th>
<th>Fleet or Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>A</td>
<td>Likely to occur often in the life of an item, with a probability of occurrence greater than $10^{-1}$ in that life.</td>
<td>Continuously experienced.</td>
</tr>
<tr>
<td>Probable</td>
<td>B</td>
<td>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.</td>
<td>Will occur frequently.</td>
</tr>
<tr>
<td>Occasional</td>
<td>C</td>
<td>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.</td>
<td>Will occur several times.</td>
</tr>
<tr>
<td>Remote</td>
<td>D</td>
<td>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.</td>
<td>Unlikely, but can reasonably be expected to occur.</td>
</tr>
<tr>
<td>Improbable</td>
<td>E</td>
<td>So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than $10^{-6}$ in that life.</td>
<td>Unlikely to occur, but possible.</td>
</tr>
</tbody>
</table>
# Hazard Assessment Matrix

## Table I Risk matrix

<table>
<thead>
<tr>
<th>Probability</th>
<th>Severity</th>
<th>I. Catastrophic</th>
<th>II. Critical</th>
<th>III. Marginal</th>
<th>IV. Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Frequent</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>B. Probable</td>
<td>2</td>
<td>5</td>
<td>9</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>C. Occasional</td>
<td>4</td>
<td>6</td>
<td>11</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>D. Remote</td>
<td>8</td>
<td>10</td>
<td>14</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>E. Improbable</td>
<td>12</td>
<td>15</td>
<td>17</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

*Source: Excerpted from MIL-STD-882D*

## Mishap Risk Assessment Value

<table>
<thead>
<tr>
<th>Mishap Risk Assessment Value</th>
<th>Mishap Risk Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 5</td>
<td>High</td>
</tr>
<tr>
<td>6 – 9</td>
<td>Serious</td>
</tr>
<tr>
<td>10 – 17</td>
<td>Medium</td>
</tr>
<tr>
<td>18 – 20</td>
<td>Low</td>
</tr>
</tbody>
</table>