Safety and Risk Assessment

Christopher Saldana, Ph.D.
Woodruff School of Mechanical Engineering
Georgia Institute of Technology
Atlanta, Georgia USA
Linkages to major quality management standards

In addition to ISO 9000, we will strive to be QS-9000 compliant.

That means falsifying the following documents: QSR, APQP, FMEA, MSA, SPC, PPAP and QSA.

Remember, you can't spell compliance without "liance."
Learning Objectives

Identify safety risks and assessment
  • Risk assessment matrix

Identify failure modes, their detectability, severity and probability of occurrence
  • Failure modes and effects analysis (FMEA)

Combining individual solutions to deal with these failure modes
Consumer product safety cases

**Toyota Accelerator**

Toyota Motor lied to regulators, Congress and the public for years about the sudden acceleration of its vehicles, a deception that caused the world’s largest automaker on Wednesday to be hit with a $1.2 billion Justice Department fine.

D. Douglas, “Toyota reaches $1.2 billion settlement to end probe of accelerator problems,” Washington Post, 03/19/2014

**McDonald’s Coffee**

In 1992, 79-year-old Stella Liebeck bought a cup of takeout coffee at a McDonald's drive-thru in Albuquerque and spilled it on her lap. She sued McDonald's and a jury awarded her nearly $3 million in punitive damages for the burns she suffered.

Consumer Attorneys of California, “The McDonald’s Hot Coffee Case,” 01/30/2017
Industrial safety cases: Aerial Lift

“2 workers fell from an aerial bucket lift and were killed at the Oxy Chemical Wichita plant,” KSN TV, June 30, 2016

“Notre Dame Student Dies at Practice,” Associated Press, October 27, 2010

Important questions:

• How should training/documentation and administrative/engineering controls be designed?
• How do we systematically assess risk?
Risk Assessment Matrix

Risk assessment matrix / form

- Tool for evaluating probable risks in terms of the likelihood or probability of the risk and the severity of the consequences
- Visualization of risk for decision making
- Development of actionable plans in a systematic manner

What Type of Risks Exist?
- Persons, Product, Environment

What are the SEVERITIES of the risk?

What is the PROBABILITY that the risk will occur?
Risk Assessment Matrix

Severity
Negligible – one minor injury
Marginal – one severe injury, multiple minor injuries
Critical – one death or multiple severe injuries
Catastrophic – multiple deaths

Probability – Certain, Likely, Possible, Unlikely, Rare
## Risk Assessment Matrix

### Risk Probability

<table>
<thead>
<tr>
<th></th>
<th>Negligible</th>
<th>Marginal</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>Likely</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Extreme</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
</tbody>
</table>

### Risk Severity

- **Low Risk**
- **Moderate Risk**
- **High Risk**
- **Extreme Risk**
Risk Assessment Matrix

**Extreme Risk:** The risks are most critical and that must be addressed on a high priority basis. The project team should gear up for immediate action, so as to eliminate the risk completely.

**High Risk:** Also call for immediate action or risk management strategies. Here in addition to thinking about eliminating the risk, substitution strategies may also work well. If these issues cannot be resolved immediately, strict timelines must be established to ensure that these issues get resolved before they create hurdles in the progress.

**Moderate Risk:** Take some reasonable steps and develop risk management strategies in time, even though there is no hurry to have such risks sorted out early. Such risks do not require extensive resources; rather they can be handled with smart thinking and logical planning.

**Low Risk:** These risks can be generally ignored as they usually do not pose any significant problem. However still, if some reasonable steps can help in fighting these risks, such steps should be taken to improve overall performance of the project.
Risk Assessment Matrix

Example: Unsafe use of a tablesaw

- What is the risk severity?
- What is the risk probability?
- How can design and/or use changes affect the risk assessment?
### Risk Assessment Matrix

**Example: Unsafe use of a tablesaw**

<table>
<thead>
<tr>
<th>Risk Probability</th>
<th>Negligible</th>
<th>Marginal</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>Likely</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Extreme</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
</tbody>
</table>

#### Risk Types
- Low Risk
- Moderate Risk
- High Risk
- Extreme Risk

#### Design and/or training changes:
- Design changes, engineering controls, administrative controls
- How do we systematically assess risk?
Risk Matrix – Methods for Improvement

National Institute of Occupational Safety and Health (NIOSH)

Elimination/Substitution
• Most effective
• Difficult to implement for existing processes

Engineering controls
• Methods built into design to minimize hazards
• Good idea as operator-independent
• Can be expensive to implement

Administrative controls
• Rules and work practices to minimize hazards
• Good idea as these are cheap to implement
• Operator-dependent need good safety culture

Personal protective equipment
• Bare minimum to reduce exposure to hazard
• Should not be the only method used
## Risk Assessment Matrix

### Example: Unsafe use of a tablesaw

<table>
<thead>
<tr>
<th>Risk Probability</th>
<th>Negligible</th>
<th>Marginal</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>Likely</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Extreme</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
</tbody>
</table>

### Risk Types
- Low Risk
- Moderate Risk
- High Risk
- Extreme Risk
## Risk Assessment Matrix

**Example: Unsafe use of a tablesaw**

<table>
<thead>
<tr>
<th>Probability</th>
<th>Negligible</th>
<th>Marginal</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
<td>Extreme</td>
</tr>
<tr>
<td>Likely</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Extreme</td>
</tr>
<tr>
<td>Rare</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
</tbody>
</table>

### Risk Types
- Low Risk
- Moderate Risk
- High Risk
- Extreme Risk
Failure modes and effects analysis (FMEA)

- FMEA - structured approach to:
  - Identifying the ways in which a product or process can fail
  - Estimating risk associated with specific causes
  - Prioritizing the actions that should be taken to reduce risk
  - Evaluating design validation plan (design FMEA) or current control plan (process FMEA)

- FMEA types – design and process

- Role in industrial processes
Failure modes and effects analysis (FMEA)

- Important terms
  - Failure mode – manner by which failure occurs for a function (related accident scenarios)
  - Cause – failure mechanism for a specific failure mode
  - Effect – consequences of failure on operation, function or status

- Important metrics for failures
  - Severity (S) – 1 (not severe) to 10 (very severe)
  - Occurrence (O) – 1 (not likely) to 10 (very likely)
  - Detection (D) – 1 (easy to detect) to 10 (not easy to detect)

- Important overall measures
  - Risk priority number (RPN), $RPN = S \times O \times D$
  - Criticality (CRIT), $CRIT = S \times O$
Failure modes and effects analysis (FMEA)

1. For each process input or product function, determine the ways in which the input or function can go wrong (failure modes)
2. For each failure mode, determine the potential effects and select a severity level for the effects.
3. Identify potential causes of each failure mode and select an occurrence level for the causes.
4. List current controls for each cause, select detection level for each cause.
5. Calculate the Risk Priority Number (RPN)
6. Develop actions and assign responsible persons (prioritize high RPNs)
7. Determine effects of possible changes in controls or design to RPNs
What can go wrong here?

Peel P50 (1964)

p50cars.com
Automobile with one headlight (no instrument cluster)

What are the failure modes, effects, causes and controls?

Possible Failure Modes:
• Light doesn’t turn on
• Light doesn’t turn off

Possible Failure Effects:
• Light doesn’t turn on
  • Driver can’t see obstacles
  • Car inoperable at night (S = 8)
• Light doesn’t turn off
  • Battery dies
  • Car won’t start (S = 10)

Possible Root Causes:
• Light doesn’t turn on
  • Battery dead (O = 8)
  • Broken wire (O = 3)
  • Headlight out (O = 10)
  • Switch corroded (O = 2)
  • Switch broken (O = 3)
• Light doesn’t turn off
  • Short circuit in switch (O = 2)
  • Operator error (left on) (O = 8)

Example adapted from: Cyders, Ohio University, 2013.
Example: FMEA redesign

Automobile with one headlight (no instrument cluster)

What are the failure modes, effects, causes and controls?

Controls/indicators:
- Light doesn’t turn on
  - User notices lights off in dark
- Light doesn’t turn off
  - User notices lights on in dark

Detectability (D):
- Light doesn’t turn on \((D = 6)\)
  - User notices lights off in dark
  - User doesn’t notice lights off during day
- Light doesn’t turn off \((D = 6)\)
  - User notices lights on in dark
  - User doesn’t notice lights not on during day
Example: FMEA redesign

Original: Single headlight automobile.

Failure Mode: *Light doesn’t turn on*

<table>
<thead>
<tr>
<th>Possible Effect</th>
<th>Root Cause</th>
<th>S</th>
<th>O</th>
<th>D</th>
<th>RPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Car inoperable at night</td>
<td>Battery dead</td>
<td>10</td>
<td>8</td>
<td>6</td>
<td>480</td>
</tr>
<tr>
<td></td>
<td>Broken wire</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>144</td>
</tr>
<tr>
<td></td>
<td>Headlight out</td>
<td>8</td>
<td>10</td>
<td>6</td>
<td>480</td>
</tr>
<tr>
<td></td>
<td>Switch corroded</td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>Switch broken</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>144</td>
</tr>
</tbody>
</table>

Redesign: (1) Use two headlights instead of one  
(2) Add visual lights-on console display

<table>
<thead>
<tr>
<th>Possible Effect</th>
<th>Root Cause</th>
<th>S</th>
<th>O</th>
<th>D</th>
<th>RPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Car inoperable at night</td>
<td>Battery dead</td>
<td>10</td>
<td>8</td>
<td>2</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td>Broken wire</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>144</td>
</tr>
<tr>
<td></td>
<td>Headlight out</td>
<td>3</td>
<td>10</td>
<td>6</td>
<td>180</td>
</tr>
<tr>
<td></td>
<td>Switch corroded</td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>Switch broken</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>144</td>
</tr>
</tbody>
</table>

Result: improves usability at night (lower severity score)  
enables detection (lower detectability score)

Example adapted from: Cyders, Ohio University, 2013.
## Example: FMEA redesign

### FMEA worksheet (original)

<table>
<thead>
<tr>
<th>Process Step or System Function</th>
<th>Potential Failure Mode</th>
<th>Potential Failure Effect</th>
<th>Potential Causes</th>
<th>Current Controls</th>
<th>Severity (S)</th>
<th>Occurrence (O)</th>
<th>Detectibility (D)</th>
<th>Risk Priority Number (RPN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headlight operation / Provide driver visibility at night</td>
<td>Light doesn't turn on</td>
<td>Car inoperable at night</td>
<td>Battery expended</td>
<td></td>
<td>10</td>
<td>8</td>
<td>6</td>
<td>480</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Wire broken</td>
<td></td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>144</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bulb failure</td>
<td></td>
<td>8</td>
<td>10</td>
<td>6</td>
<td>480</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Switch corroded</td>
<td></td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Switch broken</td>
<td></td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>144</td>
</tr>
</tbody>
</table>

### FMEA worksheet (redesign)

<table>
<thead>
<tr>
<th>Process Step or System Function</th>
<th>Potential Failure Mode</th>
<th>Potential Failure Effect</th>
<th>Potential Causes</th>
<th>New Controls</th>
<th>Severity (S)</th>
<th>Occurrence (O)</th>
<th>Detectibility (D)</th>
<th>Risk Priority Number (RPN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headlight operation</td>
<td>Light doesn't turn on</td>
<td>Car inoperable at night</td>
<td>Battery expended</td>
<td>Use two headlights instead of one. Add “lights on” console indicator. User observation.</td>
<td>10</td>
<td>8</td>
<td>2</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Wire broken</td>
<td></td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>144</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bulb failure</td>
<td></td>
<td><strong>3</strong></td>
<td>10</td>
<td>6</td>
<td><strong>180</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Switch corroded</td>
<td></td>
<td>8</td>
<td>2</td>
<td>6</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Switch broken</td>
<td></td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>144</td>
</tr>
</tbody>
</table>
Summary / Learning Objectives

Identify safety risks and assessment
  • Risk assessment matrix

Identify failure modes, their detectability, severity and probability of occurrence
  • Failure modes and effects analysis (FMEA)

Combining individual solutions to deal with these failure modes