RISK MANAGEMENT FOR SAFETY ENGINEERING

PRESENTED TO THE ISSS-TVC
JULY 19, 2017
Course Topics

- **Foundations**
  - The Language of Risk Management
  - The Math of Risk Management
  - Developing or Deriving the Appropriate Risk Measure
  - History of Modern Risk Management
  - The RAC Matrix

- **Risk management is a process, Which process is best?**
  - Review Risk Management Processes
  - How Safe is Safe Enough?
  - IARA Process
  - Safety Case Approach

- **Discipline Overviews**
  - System Safety
  - Reliability
  - Quality Engineering
  - Explosives Safety
  - Launch Safety
  - Software Safety
  - Operational Safety
  - OSHA/Industrial Safety
  - Cyber Security
Risk Management Process

1) Identify

Hazard Identification and Tracking

Understanding of hazards

Lifecycle Monitoring

Risk Assessment

Understanding of risk drivers

Iterative

Changes to reduce risk

Risk Reduction

Understand Options to reduce

Risk Acceptance

Understand Options to reduce

4) Accept
# System Safety Engineering
## The IARA Framework

<table>
<thead>
<tr>
<th>System Safety Process</th>
<th>Identify Hazards</th>
<th>Assess Risk</th>
<th>Reduce Risk</th>
<th>Accept Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use various techniques to systematically identify hazards.</td>
<td>Analyze design. Assess risk.</td>
<td>Reduce risk to acceptable level. Use order of precedence.</td>
<td>Accept residual risk.</td>
</tr>
</tbody>
</table>
| **Work**              | Perform Preliminary Hazard Analyses
Review design, test results, procedures, near misses, etc.                      | Assess probability & severity of each hazard. Identify high risk hazards    | Identify controls to reduce severity and/or probability of each hazard      | Obtain management decision on all hazards                                    |
| **Tools & Techniques**| Checklists, PHA Energy sources FMEA, O&SHA, Functional HA, Similar systems
Accident experience
Hazard Tracking System (HTS) | Fault Tree, Event tree, Probabilistic RA Risk Acceptance Matrix, HTS SSWG    | Design selection
Design alteration
Engineered safety features
Safety devices
Warning devices
Procedures/Training | SSRA
RAC Matrix
Balance risk and benefits |
| **Products**          | Hazard Analyses, PHL, PHA Populated HTS                                        | HTS with risk levels SSWG minutes                                          | Hazard list with acceptable risk levels                                    | Risk acceptance documentation                                              |
Risk Management
Applies to Multiple Disciplines

<table>
<thead>
<tr>
<th>System Safety</th>
<th>Software Safety</th>
<th>Explosives Safety</th>
<th>Reliability</th>
<th>Operational Risk Mgmt</th>
<th>Occupational Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Safety</td>
<td>Software Safety</td>
<td>Explosives Safety</td>
<td>Reliability</td>
<td>Operational Risk Mgmt</td>
<td>Occupational Safety</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(in development)</td>
<td>(in development)</td>
</tr>
</tbody>
</table>
Course Objectives

- Gain working knowledge of risk management as the overarching methodology for all Safety and Mission Assurance (SMA) and related disciplines (system safety, explosives safety, range safety, software safety, reliability, quality, operational risk management, industrial safety, etc.)
- Identify areas where cross fertilization and cross utilization between disciplines can be fruitful
- Gain ability to identify the best risk metrics
- Gain ability to apply risk methods in all SMA disciplines
- Provide forum to discuss real case studies and current work problems
- Provide sources of reference for Risk Management and related topics
THE LANGUAGE OF RISK MANAGEMENT
A-P-T RESEARCH, INC.
What are the lessons from this module?

1. The language of risk management is so imprecise that as safety professionals, we risk failure to communicate about risky situations unless we take the precaution to avoid risks by using concise risk language.

2. Words matter. Every risk-management program should have:
   1. A clearly stated purpose and goal
   2. Clear, concise, and complete definitions of “risk” and “risk management” as used by your organization.

Sometimes the safety professional is well-served to go through the four steps of good communication.
HISTORY OF MODERN RISK MANAGEMENT

A-P-T RESEARCH, INC.
What is a Decision Matrix

When the best decision is not obvious, this simple tool helps clarify:

1. What is the best risk mitigation?
2. Should the risk be accepted?

- Pascal’s Wager was the first known decision matrix, a 2×2.
- Risk analysts use decision matrices to clarify and communicate risk-based decisions.
- Matrices can be 2×2 or much larger.

<table>
<thead>
<tr>
<th>Potential Actions (If I/we do this)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Outcomes

When the best decision is not obvious, this simple tool helps clarify:
### Important Historical Developments in Safety Engineering

<table>
<thead>
<tr>
<th>Development</th>
<th>How Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>1660 Pascalian methods</td>
<td>Provided risk concept, scientific method, decision matrices, dendritic methods, careful language</td>
</tr>
<tr>
<td>1700 Proportional logic and scientific notation</td>
<td>Tools to manage, calculate, and communicate</td>
</tr>
<tr>
<td>1731 Probability and statistics developed the concept of “expected value”</td>
<td>The most logical, single basis for decision making and communication</td>
</tr>
<tr>
<td>1733 Standard deviation developed</td>
<td>Examines variation about expected value</td>
</tr>
<tr>
<td>1809 Central limit theorem</td>
<td>Large samples tend toward the center</td>
</tr>
<tr>
<td>1830 Prudent man rule</td>
<td>Common sense should prevail</td>
</tr>
<tr>
<td>1848 Gaussian normal curve</td>
<td>Mathematical treatments for probability distributions</td>
</tr>
<tr>
<td>1880 Natural causes of uncertainty</td>
<td>Natural existence of uncertainty</td>
</tr>
<tr>
<td>1936 Uncertainly alters expected value</td>
<td>The shape of the distribution changes the mean</td>
</tr>
<tr>
<td>1966 Safety engineering becomes recognized discipline</td>
<td>Universities recognize discrete aspects and perspectives of safety</td>
</tr>
<tr>
<td>1967, ’79, ’86 Apollo, Three Mile, Challenger</td>
<td>The nation’s perspective became more cautious</td>
</tr>
<tr>
<td>1980s Modeling uncertainty &amp; QRAs, Risk Assessment Matrix, ALARP</td>
<td>Epistemic and aleatory uncertainty, math/computer modeling, RAC in vogue, ALARP legally recognized</td>
</tr>
<tr>
<td>Risk Summing</td>
<td>Total system risk vs. hazard risk</td>
</tr>
<tr>
<td>Safety Case Approach</td>
<td>This system is safe because _____. Now prove it with objective evidence.</td>
</tr>
</tbody>
</table>
Other Published Methods

1. Identify the risks
2. Identify the causes
3. Identify the controls
4. Establish likelihood and consequence descriptions
5. Establish risk-rating descriptions
6. Add other controls
7. Make a decision
8. Monitor and review

-- Southern Cross University

1. Identify issues
2. Identify risks
3. Risk analysis
4. Risk treatment

-- Central and Eastern Europe Nuclear Energy Policy

1. Identify the risk
2. Analyze the risk
3. Evaluate or rank the risk
4. Treat the risk
5. Monitor and review

-- RM Online

1. Identify potential risks
2. Measure frequency and severity
3. Examine all alternative solutions
4. Decide which solution
5. Monitor results

-- “Clear Risk”

Many methods can be found on the Internet.
All Risk Management Cycles have four essential elements.

1. **(Threat) Hazard Identification**
   - Understanding of hazards
   - Monitoring and periodic formal review

2. **Risk Assessment**
   - Understanding of risk drivers
   - Changes to reduce risk
   - Iterative

3. **Risk Acceptance**
   - Understand Risks, Reduction Options, and Criteria

4. **Risk Reduction**
   - Changes to reduce risk
Road Signs for Risk Space

Risk Space

- More severe consequence
- Higher likelihood
- Stop proceed only with significant need
- Risk is too high
- Proceed only with significant need
- Properly authorized approval required
- ALAP required
- Risk is a concern
- ALARP required
- Road signs prescribe actions, provide information, and define limits.

References

- “Road Signs in Risk-Space”, Tom Pfitzer, Bill Pfitzer, Meredith Hardwick; Briefing; August 2004
Road signs prescribe actions, provide information, and define limits.
A Collection of Caution Signs
THE RAC MATRIX
A-P-T RESEARCH, INC.
They lack engineering appeal, but are widely used in many fields...

<table>
<thead>
<tr>
<th><strong>Music</strong> (Loudness)</th>
<th><strong>Beef</strong></th>
<th><strong>Medicine</strong> (Status-Related Terms)</th>
<th><strong>Perceived Temperature</strong></th>
<th><strong>Log Scale</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Eight Steps</td>
<td>Seven Steps</td>
<td>Eight Steps</td>
<td>-120°</td>
<td>1 x 10^-6</td>
</tr>
<tr>
<td>ppp</td>
<td>Very Well Done</td>
<td>Excellent</td>
<td>-110°</td>
<td>1 x 10^-5</td>
</tr>
<tr>
<td>pp</td>
<td>Well Done</td>
<td>Good</td>
<td>-100°</td>
<td>1 x 10^-4</td>
</tr>
<tr>
<td>piano</td>
<td>Medium Well Done</td>
<td>Satisfactory</td>
<td>-90°</td>
<td>1 x 10^-3</td>
</tr>
<tr>
<td>mp</td>
<td>Medium</td>
<td>Fair</td>
<td>-80°</td>
<td>1 x 10^-2</td>
</tr>
<tr>
<td>mf</td>
<td>Medium Rare</td>
<td>Poor</td>
<td>-70°</td>
<td>1 x 10^-1</td>
</tr>
<tr>
<td>forte</td>
<td>Rare</td>
<td>(Guarded)</td>
<td>-60°</td>
<td>10</td>
</tr>
<tr>
<td>ff</td>
<td>Very Rare</td>
<td>(Serious)</td>
<td>-50°</td>
<td>1 x 10^-1</td>
</tr>
<tr>
<td>fff</td>
<td></td>
<td>Critical</td>
<td>-40°</td>
<td>1 x 10^-2</td>
</tr>
</tbody>
</table>

(Tempo)

<table>
<thead>
<tr>
<th>Five Steps</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lento</td>
<td></td>
<td></td>
<td></td>
<td>1 x 10^-3</td>
</tr>
<tr>
<td>Adagio</td>
<td></td>
<td></td>
<td></td>
<td>1 x 10^-4</td>
</tr>
<tr>
<td>Moderato</td>
<td></td>
<td></td>
<td></td>
<td>1 x 10^-5</td>
</tr>
<tr>
<td>Allegro</td>
<td></td>
<td></td>
<td></td>
<td>1 x 10^-6</td>
</tr>
<tr>
<td>Presto</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Tone)

- Accuracy of subjective judgments vary widely with the skill and experience of the individual.
- The ability to subjectively judge difference increases with corresponding anchor point and quantitative tools allowing judgement to become highly calibrated.
We define an 10-step risk scale for likelihood and risk separated by half order of magnitudes, including: very likely (>3E-1), likely, high, moderate, possible, low, very low, unlikely, extremely unlikely, and near zero (<1E-5)

<table>
<thead>
<tr>
<th>Qualitative</th>
<th>Very Likely</th>
<th>Likely</th>
<th>High</th>
<th>Moderate</th>
<th>Possible</th>
<th>Low</th>
<th>Very Low</th>
<th>Unlikely</th>
<th>Extremely Unlikely</th>
<th>Near Zero</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantitative</td>
<td>&gt;3E-1</td>
<td>1E-1</td>
<td>3E-2</td>
<td>1E-2</td>
<td>3E-3</td>
<td>1E-3</td>
<td>3E-4</td>
<td>1E-4</td>
<td>3E-5</td>
<td>&lt;1E-5</td>
</tr>
</tbody>
</table>
Course Topics

- **Day 1 Foundations**
  - 1A: The Language of Risk Management
  - 1B: The Math of Risk Management
  - 1C: Developing or Deriving the Appropriate Risk Measure
  - 1D: History of Modern Risk Management
  - 1E: The RAC Matrix

- **Day 2 Risk management is a process, Which process is best?**
  - 2A: Review Risk Management Processes
  - 2B: How Safe is Safe Enough?
  - 2C: IARA Process
  - 2D: Safety Case Approach

- **Day 3 Other Useful Processes**
  - 3A: Discipline 1: System Safety
  - 3B: Discipline 2: Reliability

- **Day 4 Discipline Overviews (cont’d)**
  - 4A: Discipline 3: Quality Engineering
  - 4B: Discipline 4: Explosives Safety
  - 4C: Discipline 5: Launch Safety
  - 4D: Discipline 6: Software Safety

- **Day 5 Discipline Overviews (cont’d)**
  - 5A: Discipline 7: Operational Safety
  - 5B: Discipline 8: OSHA/ Industrial Safety
  - Quiz