RISK MANAGEMENT FOR SAFETY ENGINEERING

PRESENTED TO THE ISSS-TVC
JULY 19, 2017

SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com

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

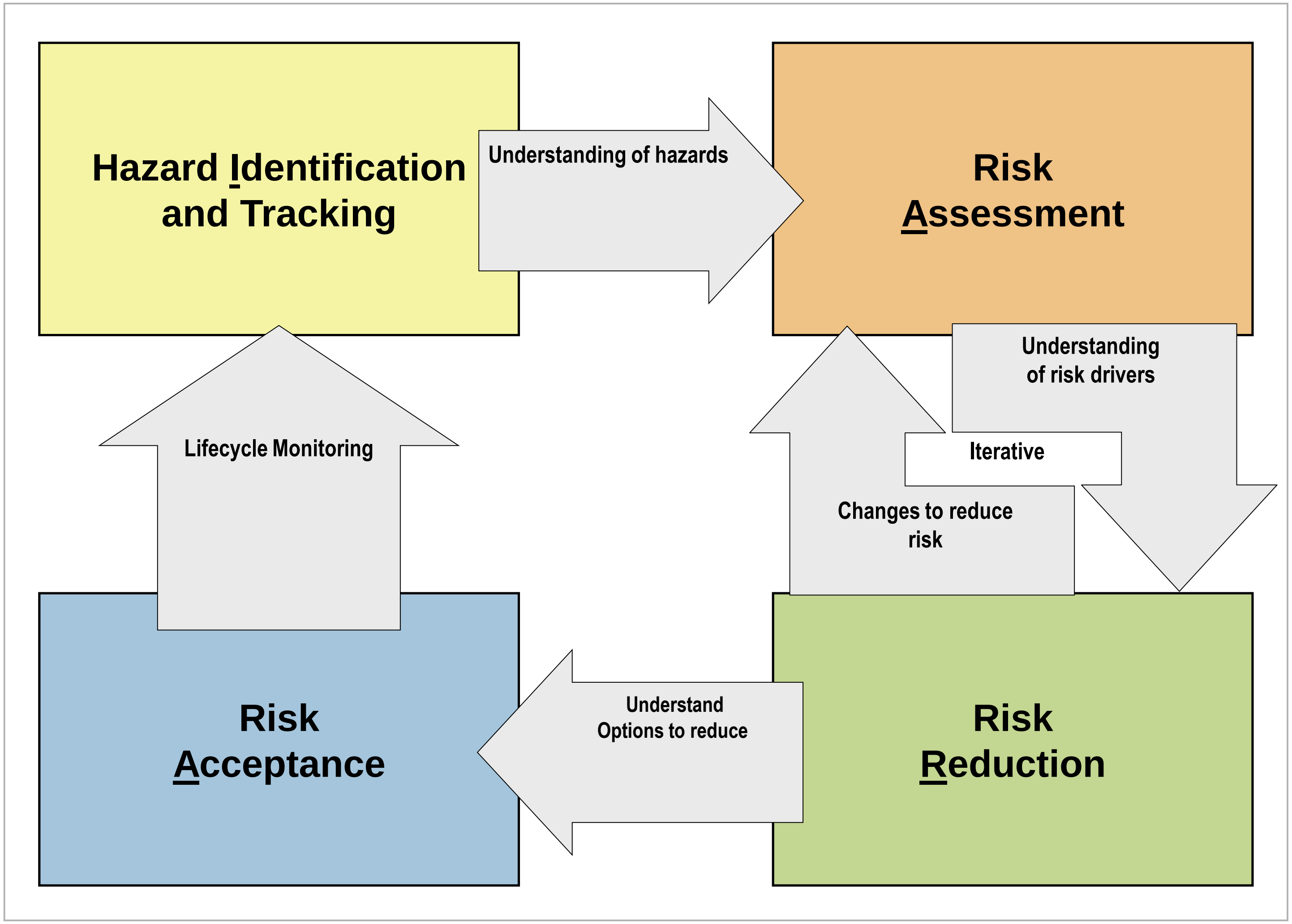
SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

1) Identify

2) Assess

3) Reduce

4) Accept



System Safety Engineering
The IARA Framework

	Identify Hazards	Assess Risk	Reduce Risk	Accept Risk
System Safety Process	Use various techniques to systematically identify hazards.	Analyze design. Assess risk.	Reduce risk to acceptable level. Use order of precedence.	Accept residual risk.
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

SEAC Courses

Risk Management

Applies to Multiple Disciplines

System Safety	Software System Safety	Explosives Safety	Reliability	Operational Risk Mgmt	Occupational Safety

System Safety	Software System Safety	Explosives Safety	Reliability (in development)	Operational Risk Mgmt (in development)	Occupational Safety (in development)

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.

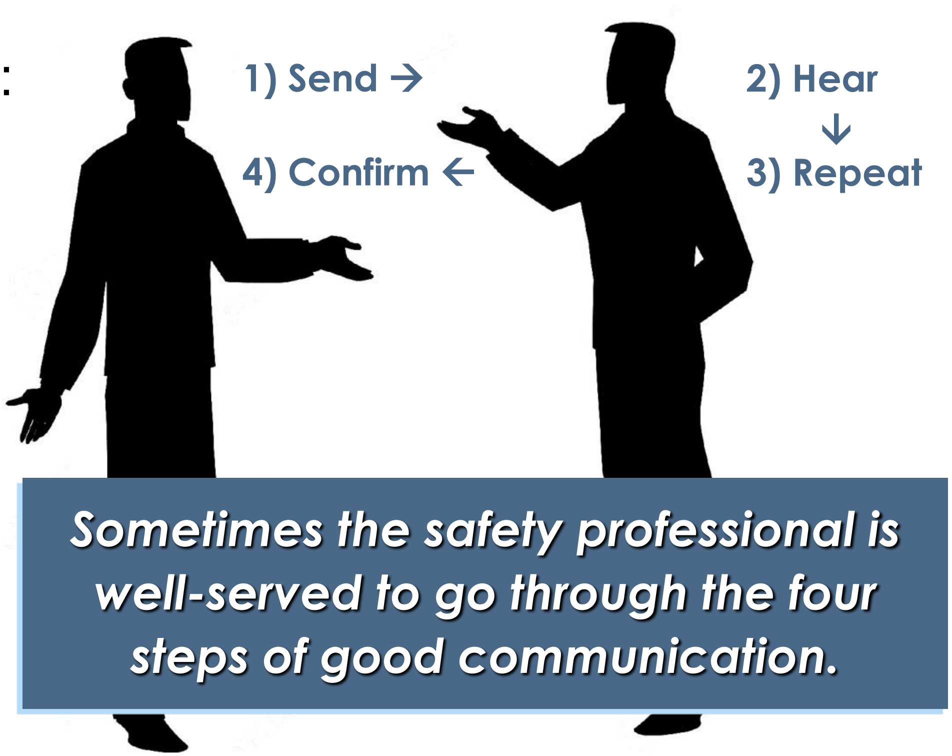
SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com

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.

SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com

What is a Decision Matrix

Outcomes

Potential Actions *(If I/we do this)*

	1	2	3	4
1				
2				
3				
4				

- 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.

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?

Important Historical Developments in Safety Engineering

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

RISK MANAGEMENT PROCESSES

A-P-T RESEARCH, INC.

SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com

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
2. Analyze and prioritize
3. Plan and schedule
4. Track and report
5. Control
6. Learn

-- Microsoft Library

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

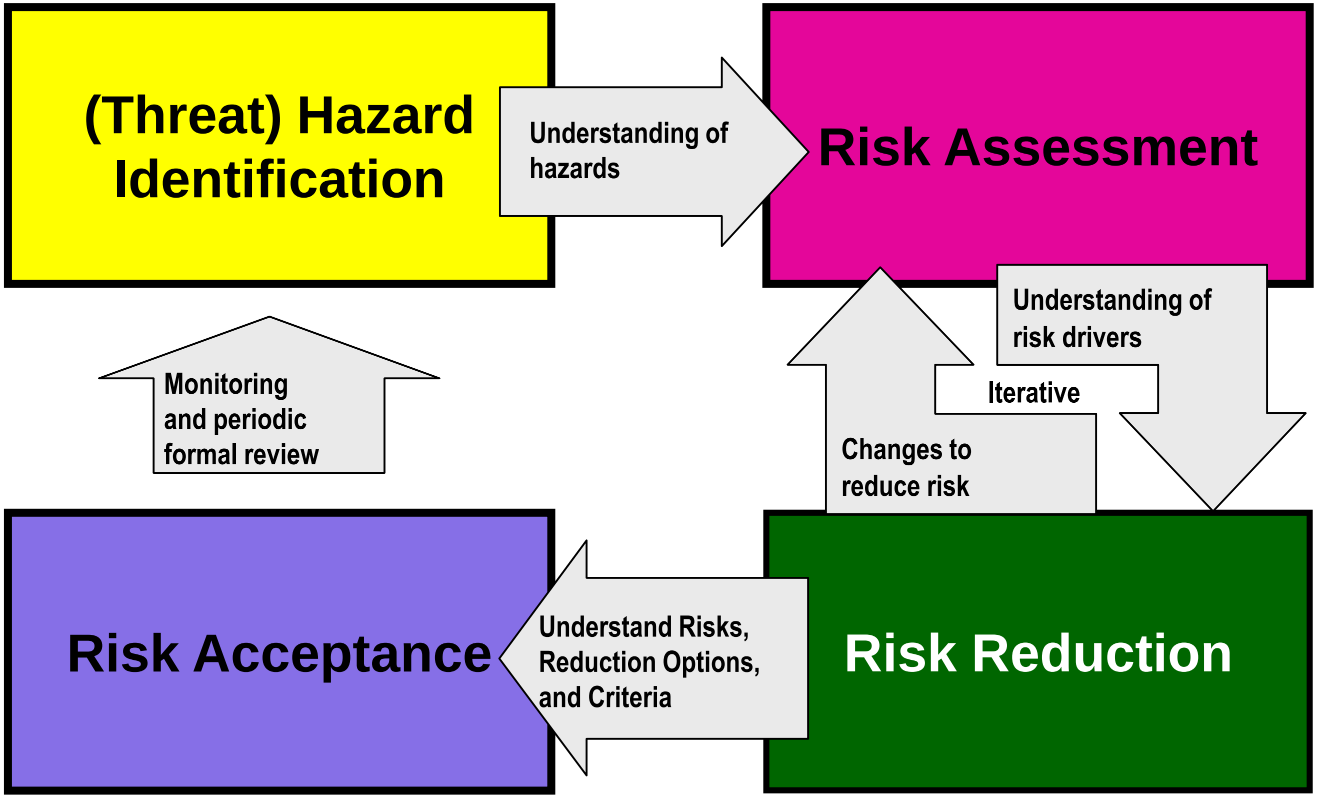
1. Identify potential risks
2. Measure frequency and severity
3. Examine all alternative solutions
4. Decide which solution
5. Monitor results

-- "Clear Risk"

Many methods can be found on the Internet.

IARA Includes Necessary Elements

All Risk Management Cycles have four essential elements.


(Threat) Hazard Identification
Understanding of hazards
Risk Assessment
Understanding of risk drivers
Iterative
Changes to reduce risk
Monitoring and periodic formal review
Risk Acceptance
Understand Risks, Reduction Options, and Criteria
Risk Reduction

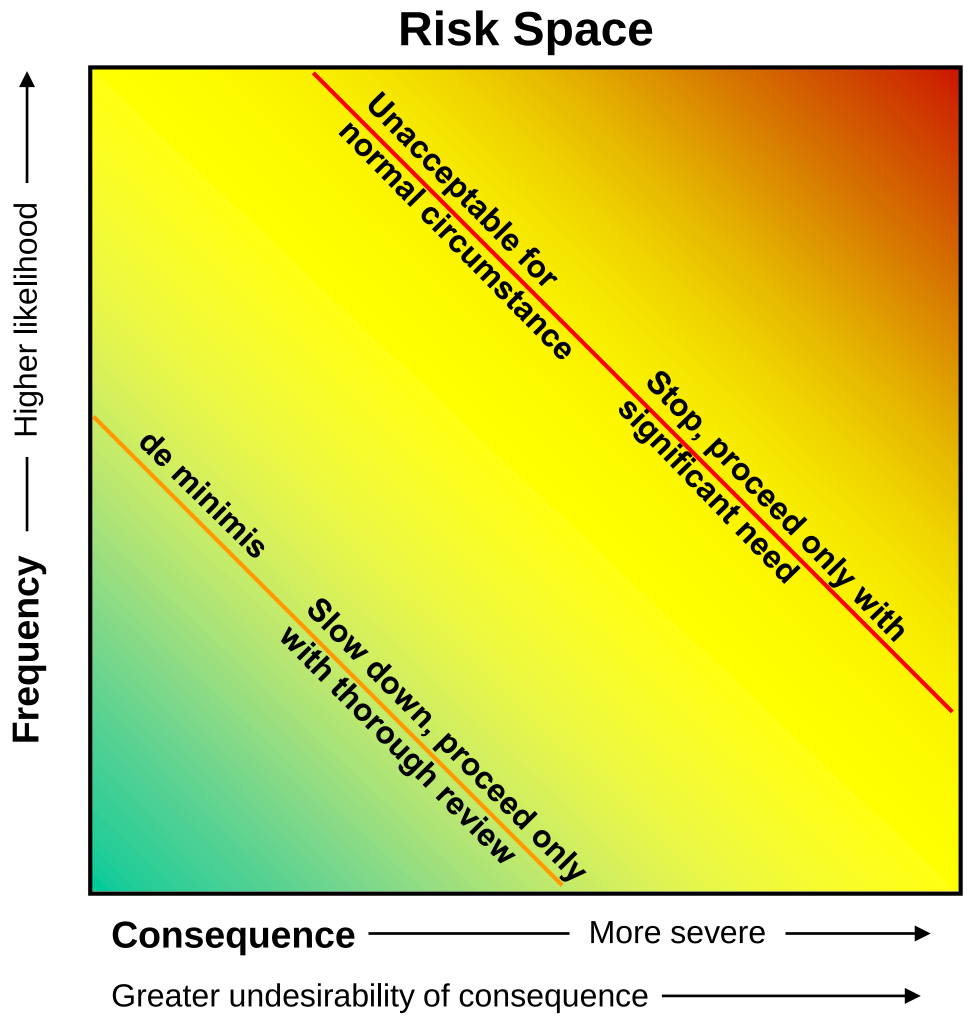
HOW SAFE IS SAFE ENOUGH?

A-P-T RESEARCH, INC.

SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com

Road Signs for Risk Space


Risk Space
Unacceptable for normal circumstance
Stop, proceed only with significant need
de minimis
Slow down, proceed only with thorough review
Frequency —— Higher likelihood
Consequence —— More severe
Greater undesirability of consequence

Road signs prescribe actions, provide information, and define limits.

- Risk is too high
- Proceed only with significant need
- Properly authorized approval required
- ALAP required

- Risk is a concern
- ALARP required

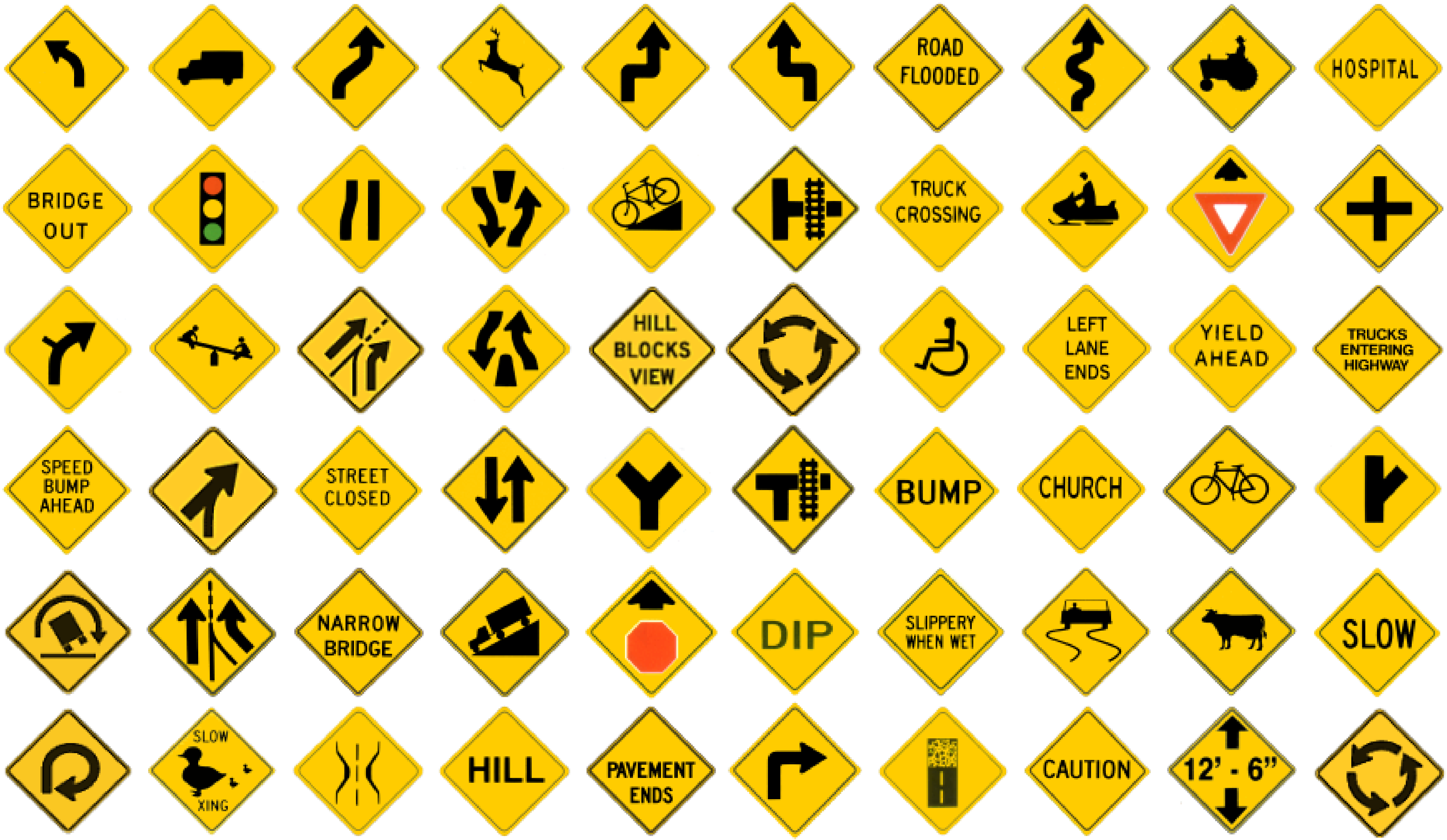
References
- “Road Signs in Risk-Space”, Tom Pfitzer, Bill Pfitzer, Meredith Hardwick; Briefing; August 2004
- Pfitzer, T., M. Hardwick, B. Pfitzer, “Are All Risk Criteria Created Equal and Used Equally? – Proposed QRA Standards for Risk Management,” DoD Explosives Safety Seminar, August 2004, CE1-09600.

Road Signs

DEAD END
DETOUR
SPEED LIMIT 50
YIELD
EXIT
25
M.P.H.
SLOW
DO NOT ENTER
ROAD CLOSED

Road signs prescribe actions, provide information, and define limits.

A Collection of Caution Signs



THE RAC MATRIX

A-P-T RESEARCH, INC.

SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

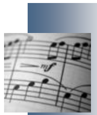
Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com

Those Subjective Scales

They lack engineering appeal, but are widely used in many fields…

Music

(Loudness)



Eight Steps

ppp
pp
piano
mp
mf
forte
ff
fff

(Tempo)

Five Steps

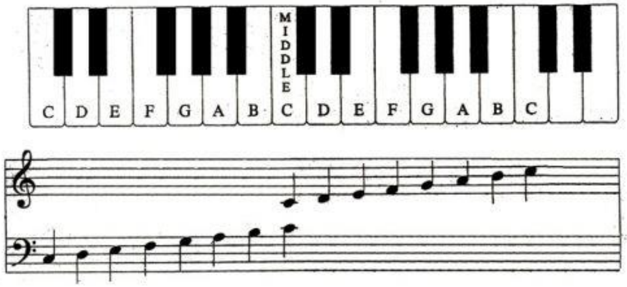
Lento
Adagio
Moderato
Allegro
Presto

Beef

Seven Steps

Very Well Done
Well Done
Medium Well Done
Medium
Medium Rare
Rare
Very Rare

(Tone)



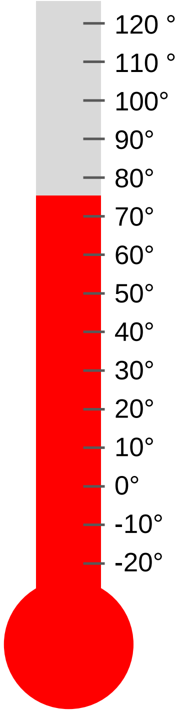
Medicine

(Status-Related Terms)

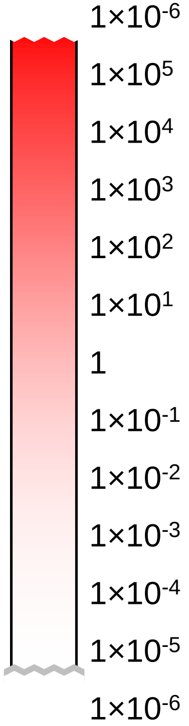
Eight Steps

Excellent
Good
Satisfactory
Fair
Poor
(Guarded)
(Serious)
Critical

Perceived Temperature



Log Scale



- 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.

APT Risk Management Scales

- 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)

Qualitative	Very Likely	Likely	High	Moderate	Possible	Low	Very Low	Unlikely	Extremely Unlikely	Near Zero
Quantitative	>3E-1	1E-1	3E-2	1E-2	3E-3	1E-3	3E-4	1E-4	3E-5	<1E-5

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