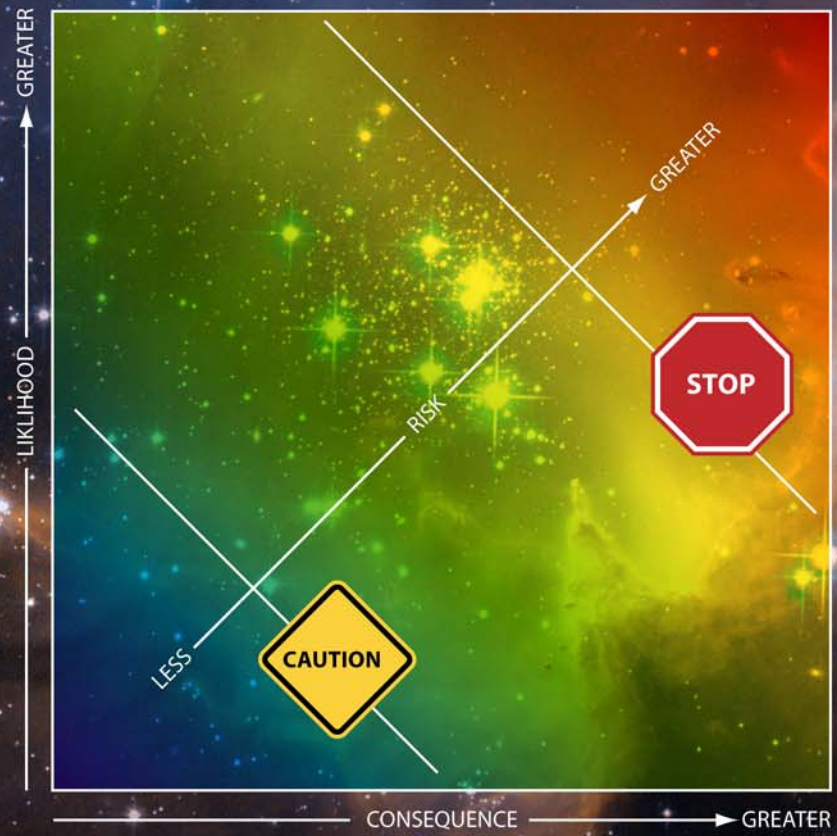
ROADSIGNS IN RISK SPACE



3rd IAASS Conference
Rome, Italy
October 21-23, 2008

Sponsored by:

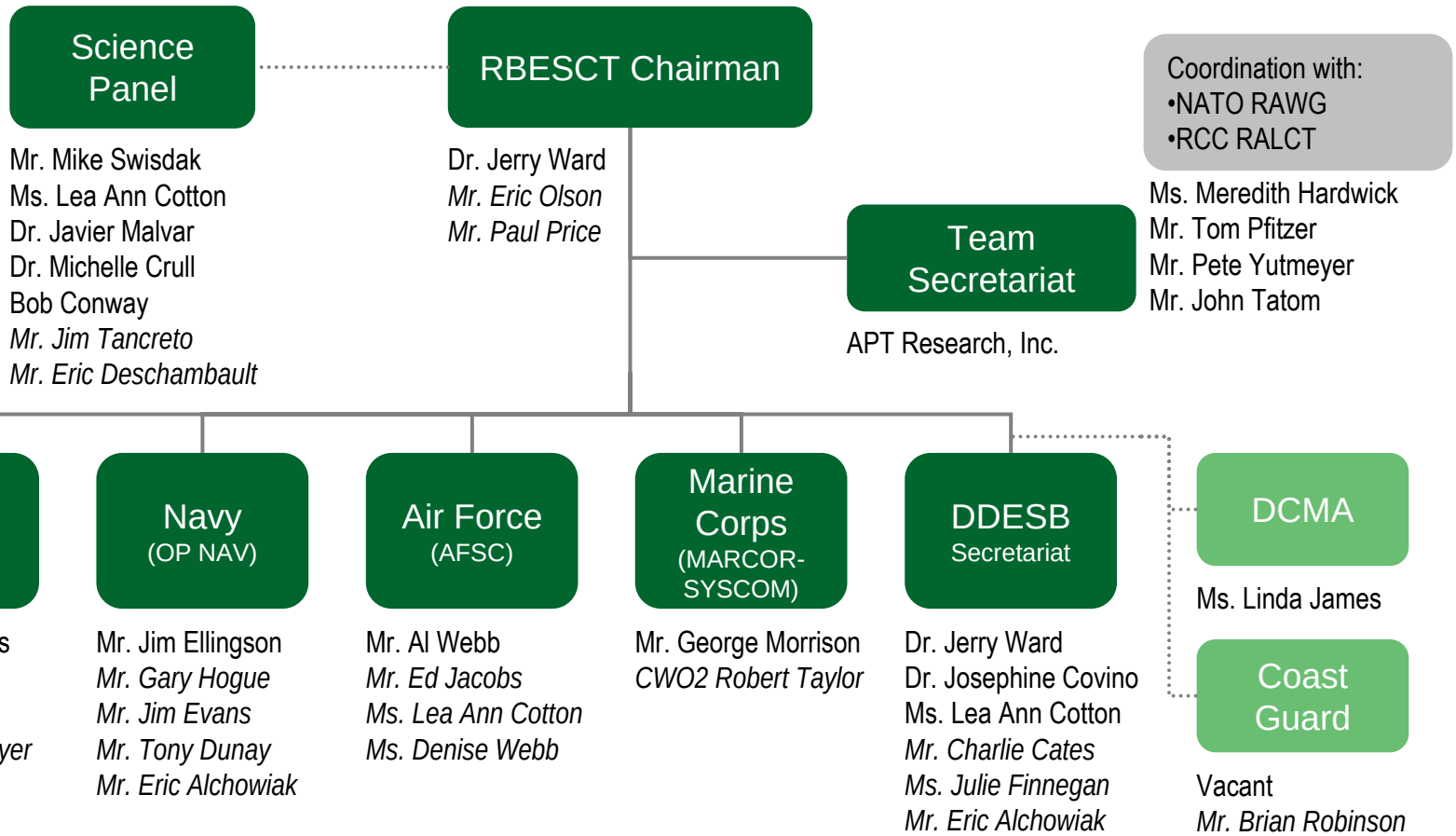
A-P-T Research, Inc.

Presented by:
Tom Pfitzer
APT Research, Inc.

Topics

- Background
- Two types of standards
- How safe is safe enough for risk management actions?
- 24 standards
- Rationale for standards selection
- Multiple uses
- Summary/conclusions
- Future work

RBESCT



Italics denotes former team members

Terms
as used in this presentation

A-P-T Research, Inc.

Standards – a quantitative measure indicating “safe enough” for a specified action level

Criteria – a logical group of “standards”

Individual risk – the annual risk to an individual

- **Worker –** directly involved with the hazard (hands on)
- **Associated –** indirectly involved or related to the hazard (not hands on)
- **Public –** no voluntary acceptance of risk (no knowledge of hazard)

Group risk – the annual risk to the group of people exposed to a single hazard

Event risk – the summation of individual risk resulting from a single event, activity

- **Event** – a planned action which involves risk of a short duration

ALAP – As low as possible

ALARP – As low as reasonably practicable

Risk management – a defined approach to reduce risk (e.g., IARA)

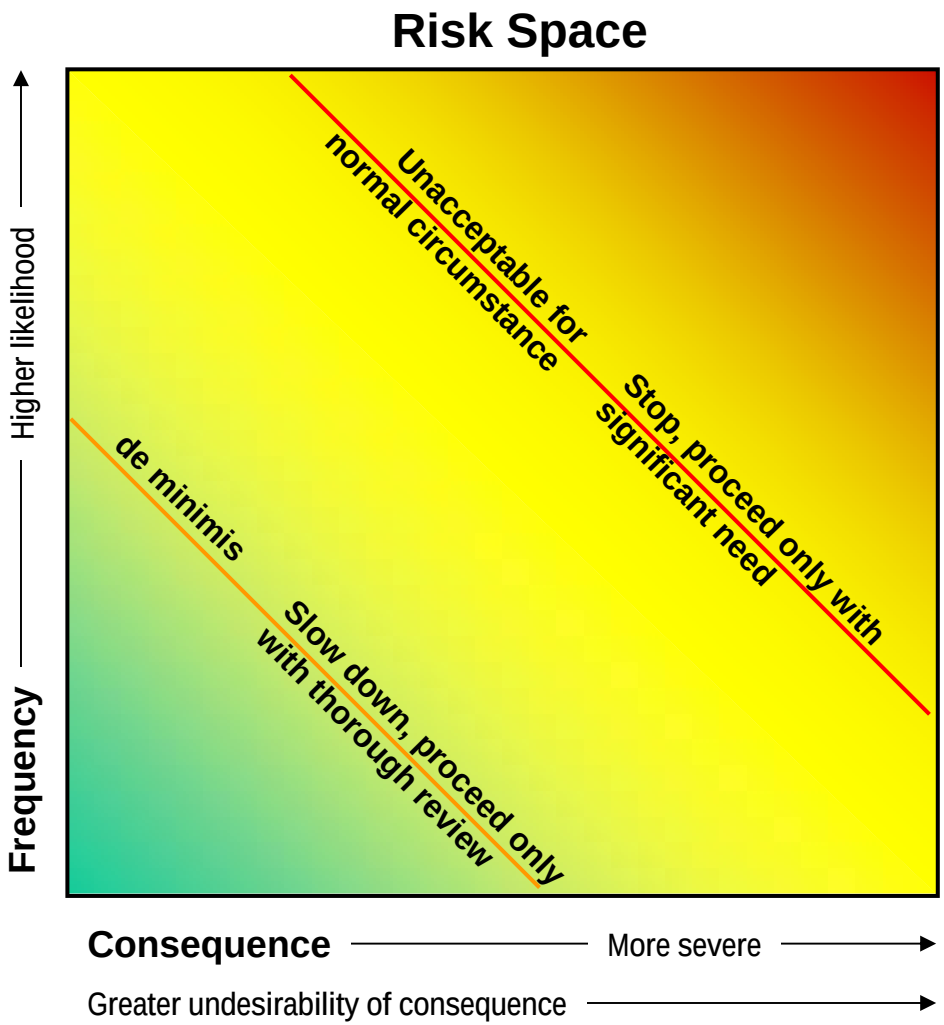
Risk acceptance – a go/no-go decision by properly authorized official

Roadsigns

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

A Collection of Caution Signs

Road Signs for Risk Space



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

Goals of Criteria

Goal: A set of criteria to aid risk management.

Risk Management Process

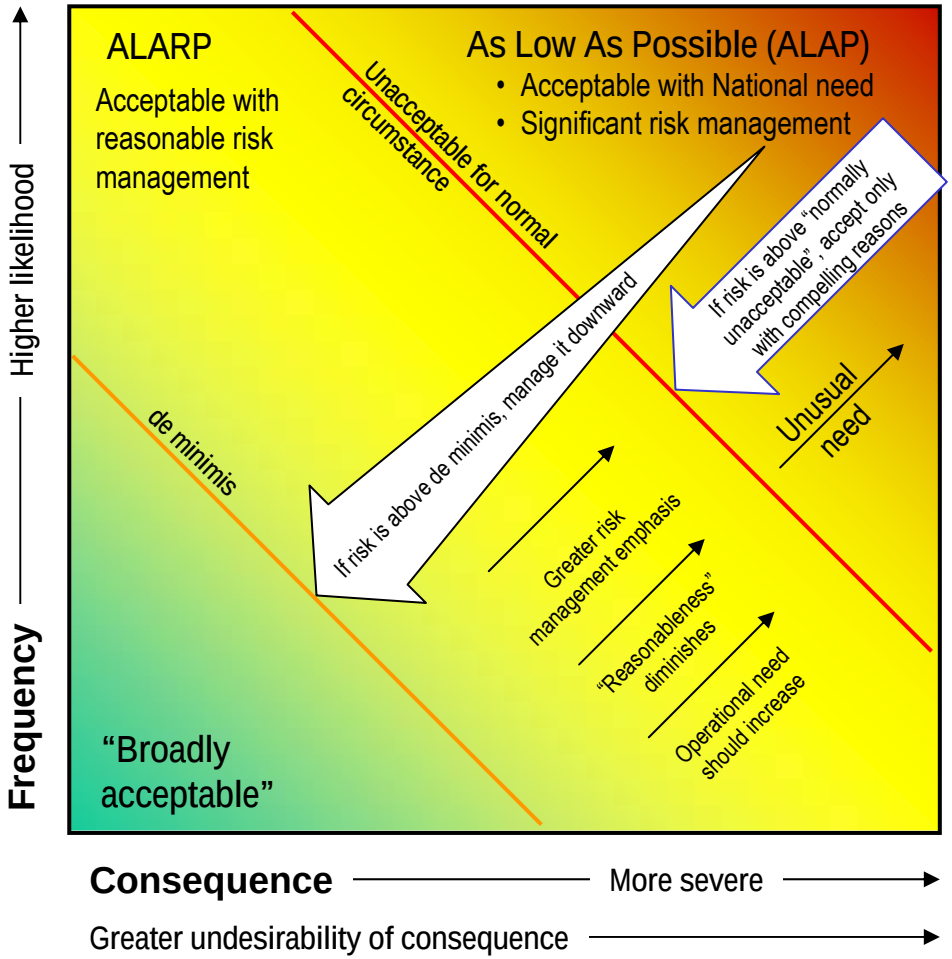
1. Identify hazards
2. Assess risks
3. Reduce, mitigate, control
4. Accept risk

Boundaries are needed to determine when each action is appropriate:

a) How much risk should trigger risk reduction?

b) How much risk is acceptable/unacceptable?

Standards Needed



1. A de minimis standard is needed to trigger risk management actions
2. A "normally unacceptable" standard is needed:
   - Defines upper limit
   - Requires "unusual need"

Risk Region	Risk Management Requirement
Broadly acceptable	None
Accept with mitigation	ALARP
Accept with national need	ALAP while meeting the operational requirement

Goal of the Standards Development Task

A-P-T Research, Inc.

Develop a comprehensive set of criteria which should:

1. Be useful for risk management

and also:

2. Define the de minimis and “normally unacceptable” levels of risk which would withstand scrutiny
3. For continuous and peak exposures
4. For public, workers, and associated people
5. For individuals and groups
6. For risk of fatality or injury
7. In a self-consistent framework
8. Considering all known precedents
9. Be uncomplicated

Basic Question: How Safe is Safe Enough?

A-P-T Research, Inc.

This question is usually answered by considering:

–Legal precedents

–Societal expectations

Documented in "Universal Risk Scales – A Tool for Developing Risk Criteria by Consensus"

Measures used:

√ 1. Lives

√ 2. Injuries

3. $

4. Schedule

5. Mission

Five Steps in Developing the 24 Standards

Step 1: Determine *individual fatality* criteria for the public based on precedents.

Step 2: Determine *individual worker and associated persons* criteria based on individual fatality criteria and precedents.

Step 3: Develop *individual injury* criteria, based on fatality criteria (1. and 2. above), and on societal expectations.

12 Individual Risk Standards

3 standards

9 standards

Step 4: Determine *annual group* criteria based on summed individual risk (1, 2. and 3. above) considering precedents.

Step 5: Determine *event risk* based on annual group and individual risks (1. through 4. above) considering precedents.

12 Group Risk Standards

6 standards

6 standards

12 Individual Protection Standards

A-P-T Research, Inc.

~ Annual Risk ~

Fatality

Risk is considered broadly acceptable below:

1 Possible Standard #1 (Individual)

Annual risk of fatality to an individual in the public of less than $1x10^{-6}$ is considered broadly acceptable.

Risk is normally considered unacceptable above:

2 Possible Standard #2 (Individual Public)

Acceptance of risk of fatality above $3x10^{-6}$ is normally considered unacceptable.

3 Possible Standard #3 (Individual Worker)

Acceptance of risk of fatality above $3x10^{-4}$ is normally considered unacceptable.

4 Possible Standard #4 (Individual Associated)

Acceptance of risk of fatality above $3x10^{-5}$ is normally considered unacceptable.

Major Injury

5 Possible Standard #5 (Individual)

Risk of major injury to an individual below $1x10^{-5}$ is considered broadly acceptable.

6 Standard #6 (Individual Public)

Acceptance of risk of major injury above $3x10^{-5}$ is normally considered unacceptable.

7 Possible Standard #7 (Individual Worker)

Acceptance of risk of major injury above $3x10^{-3}$ is normally considered unacceptable.

8 Possible Standard #8 (Individual Associated)

Acceptance of risk of major injury above $3x10^{-4}$ is normally considered unacceptable.

Minor Injury

9 Possible Standard #9 (Individual)

Risk of minor injury below $1x10^{-4}$ is considered broadly acceptable.

10 Standard #10 (Individual Public)

Acceptance of risk of minor injury above $3x10^{-4}$ is normally considered unacceptable.

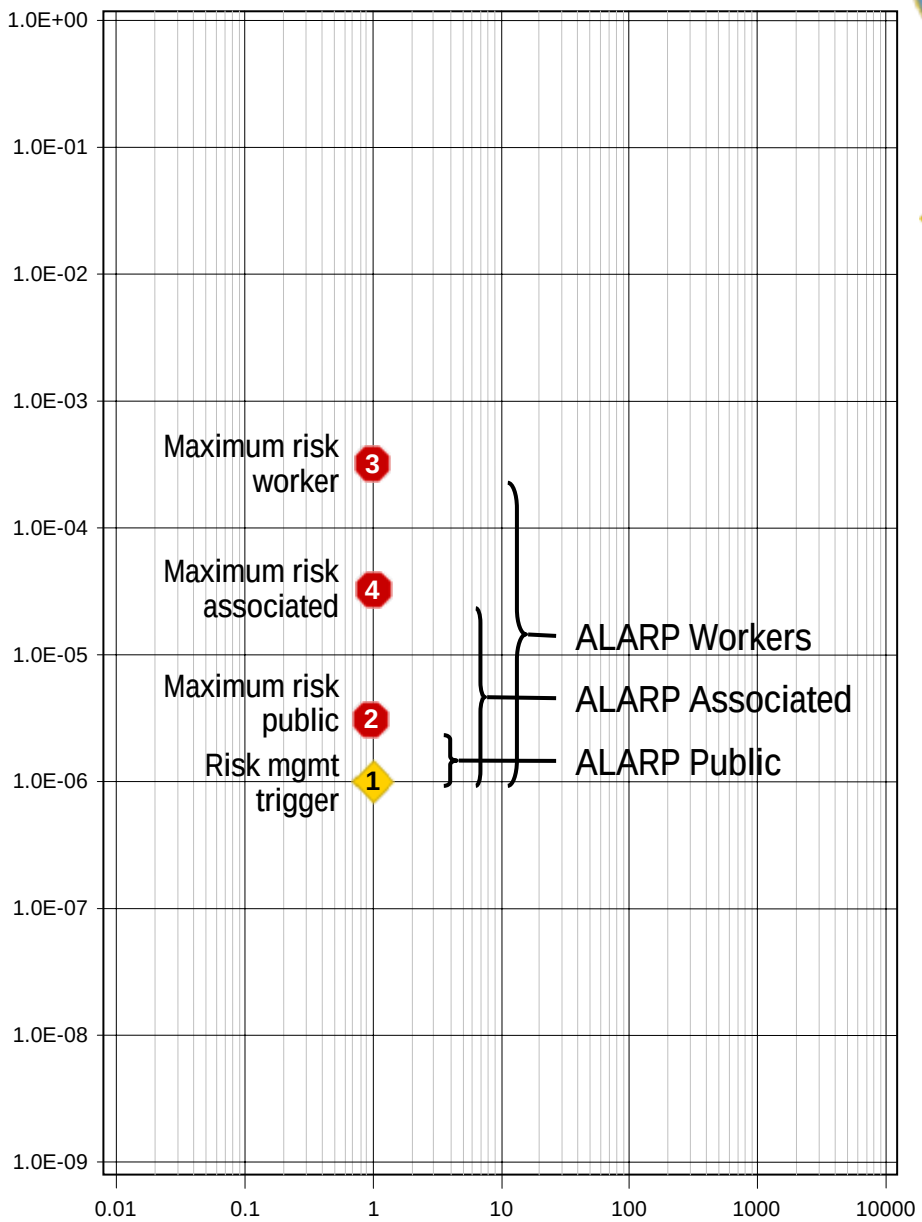
11 Possible Standard #11 (Individual Worker)

Acceptance of risk of minor injury above $3x10^{-2}$ is normally considered unacceptable.

12 Possible Standard #12 (Individual Associated)

Acceptance of risk of minor injury above $3x10^{-3}$ is normally considered unacceptable.

Summary of Individual Fatality Risk Protection



1 Possible Standard #1 (Individual Public)

Annual Risk of fatality to an individual of less than $1x10^{-6}$ is considered broadly acceptable.

2 Possible Standard #2 (Individual Public)

Acceptance of risk of fatality above $3x10^{-6}$ is normally considered unacceptable.

3 Possible Standard #3 (Individual Worker)

Acceptance of risk of fatality above $3x10^{-4}$ is normally considered unacceptable.

4 Possible Standard #4 (Individual Associated)

Acceptance of risk of fatality above $3x10^{-5}$ is normally considered unacceptable.

Step 3: For the Purpose of Protection Criteria What Should the Injury/Fatality Ratio Be?

- Considering accident experience, societal expectations, and the granularity of risk models, the following ratios were selected:

- Protection from 1 fatality should be the same as 10 major injuries or 100 minor injuries.

Fatality to Injury Ratio (F/I)

A-P-T Research, Inc.

All Unintentional Injuries	Fatalities (F)	Disabling Injuries (I) [a]	F/I
All Classes	96,900	20,800,000	0.0046
Motor-vehicle (mv)	41,300	2,200,000	0.0188
- public non-work	38,900	2,100,000	0.0185
- work	2,200	100,000	0.0220
- home	200	[b]	
Work	5,100	3,800,000	0.0134
- non-mv	2,900	3,700,000	0.0078
- mv	2,200	100,000	0.0220
Home	28,800	6,900,000	0.0041
- non-mv	28,600	6,900,000	0.0041
- mv	200	[b]	
Public	24,100	8,000,000	0.0030

On/Off-the-Job (for workers only)	Fatalities (F)	Disabling Injuries (I)	F/I
On-the-job	5,100	3,800,000	0.0013
Off-the-job	40,600	6,600,000	0.0061
- public (non-mv)	9,100	3,000,000	0.0030
- home	10,500	2,500,000	0.0042
- motor-veh	21,000	1,100,000	0.0192

On-the-Job	Fatalities (F)	Disabling Injuries (I)	F/I
All Industries	5,100	3,800,000	0.0013
- Agriculture	770	150,000	0.0051
- Mining/quarry'g	130	20,000	0.0065
- Construction	1,190	400,000	0.0030
- Manufacturing	600	670,000	0.0009
- Trans/pub util	850	370,000	0.0023
- Trade	450	710,000	0.0006
- Services	640	900,000	0.0007
- Government	470	580,000	0.0008

Just MVAs	Fatalities (F)	Disabling Injuries (I)	F/I
Collisions - V→V	18,800	1,580,000	0.0118
- V→FO	11,100	330,000	0.0336
- V→Ped	5,800	95,000	0.0610
- V→P-cycle	900	70,000	0.0128
- V→Train	300	2,000	0.1500
- Other	100	13,000	0.0076
Non-collisions	4,300	110,000	0.0391
All MVAs	41,300	2,200,000	0.0188

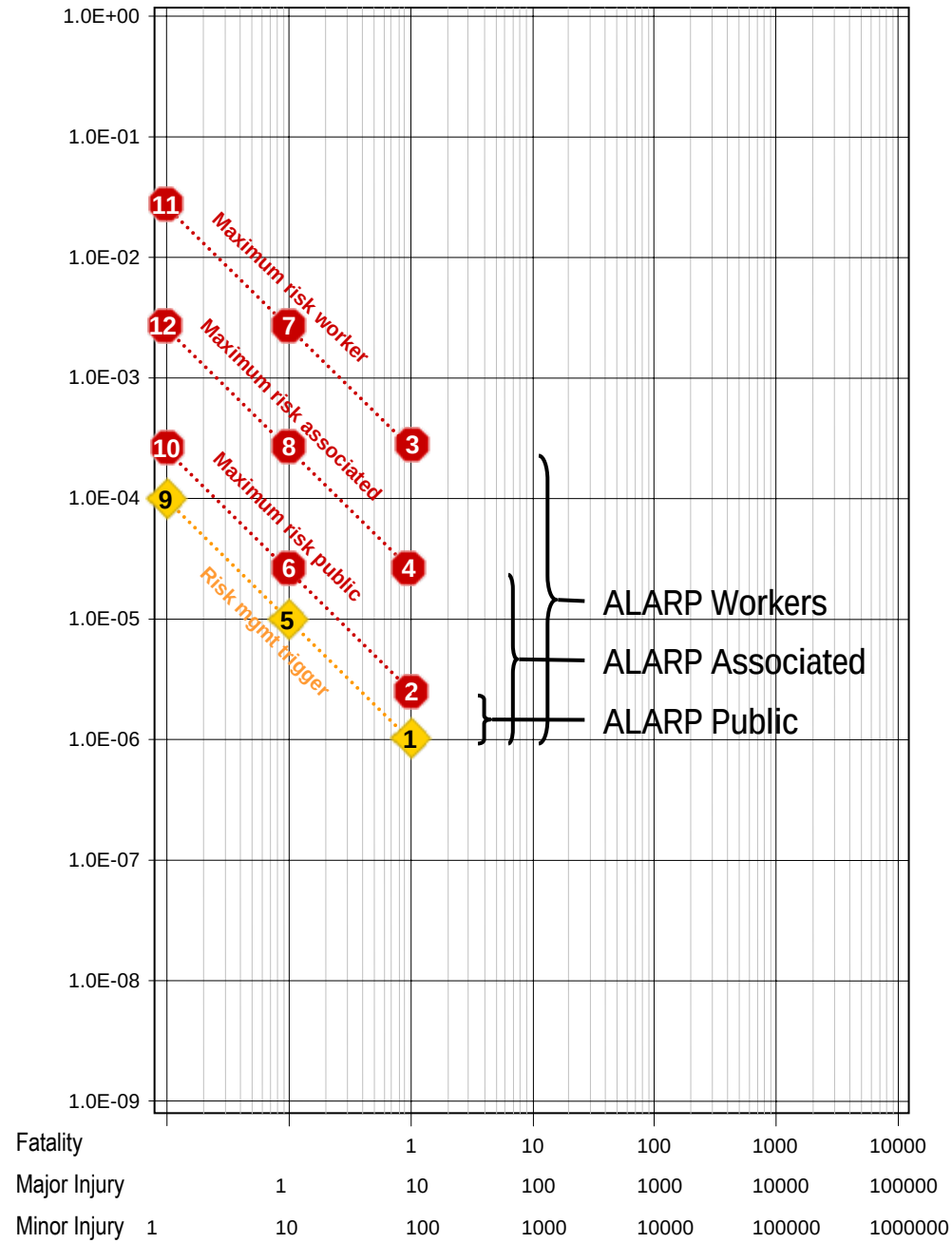
The experience reflects ~2 orders of magnitude is a reasonable ratio between minor injury and fatality.

Data in the above tables is taken from NSC's 1999 *Injury Facts* publication. Injury and fatality data from other sources, and for years other than 1999, yield similar F/I ratios.

(a) A disabling injury is defined as one that results in death, some degree of permanent impairment, or renders the injured person unable to effectively perform their duties for a full day beyond the day of injury. This definition applies to all unintentional injuries. All injury totals labeled "disabling injuries" in *Injury Facts* are based on this definition.

(b) Deaths and injury above for the four separate classes add to more than the All Classes figures due to rounding, and because some deaths and injuries are included in more than one class. For example, 2,200 work deaths involved motor vehicles in transport and are in both the work and the motor-vehicle totals and 200 motor-vehicle deaths occurred on home premises and are in both home and motor-vehicle. The total of such duplication amounted to about 2,400 deaths and 100,000 injuries in 1999.

Comparison of Individual Risk Standards



By connecting the individual standards (a locus of points) comparisons can be made to the ALARP region.

Note: The ALARP region for individuals shown by the locus lines is not part of the standard per se. Rather it is used to develop consistency between the standards.

12 Group Protection Standards

A-P-T Research, Inc.

Annual

Risk is considered broadly acceptable below:

13 Possible Standard #13 (Public and Associated - Annual)

Annual risk of fatality to groups of people less than $1x10^{-5}$ is considered broadly acceptable.

14 Possible Standard #14 (Public and Associated - Annual)

Annual risk of major injury to groups of people less than $1x10^{-4}$ is considered broadly acceptable.

15 Possible Standard #15 (Public and Associated - Annual)

Annual risk of minor injury to groups of people less than $1x10^{-3}$ is considered broadly acceptable.

Risk is normally considered unacceptable above:

16 Possible Standard #16 (Public and Associated - Annual)

Annual risk of fatality to groups of people greater than $3x10^{-3}$ is normally considered unacceptable.

17 Possible Standard #17 (Public and Associated - Annual)

Annual risk of major injury to groups of people greater than $3x10^{-2}$ is normally considered unacceptable.

18 Possible Standard #18 (Public and Associated - Annual)

Annual risk of minor injury to groups of people greater than $3x10^{-1}$ is normally considered unacceptable.

Event

19 Possible Standard #19 (All people-event)

Risk of fatality from a single event to groups of people less $1/N^2 \times 10^{-5}$ is considered broadly acceptable.

20 Possible Standard #20 (All people-event)

Risk of major injury from a single event to groups of people less $1/N^2 \times 10^{-3}$ is considered broadly acceptable.

21 Possible Standard #21 (All people-event)

Risk of minor injury from a single event to groups of people less $1/N^2 \times 10^{-1}$ is considered broadly acceptable.

22 Possible Standard #22 (All people-event)

Risk of fatality from a single event to groups of people greater than $3x10^{-4}$ is normally considered unacceptable.

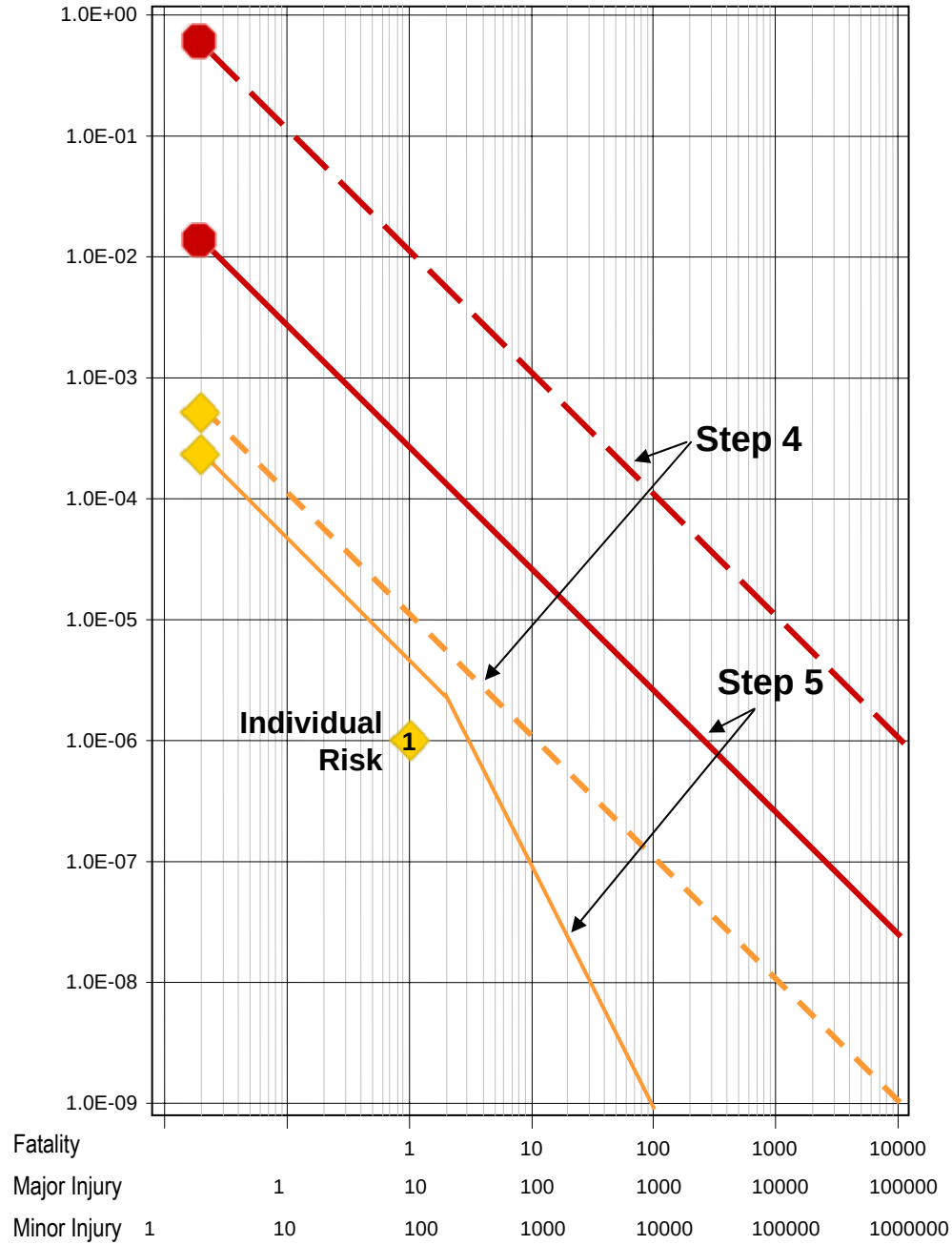
23 Possible Standard #23 (All people-event)

Risk of major injury from a single event to groups of people greater than $3x10^{-3}$ is normally considered unacceptable.

24 Possible Standard #24 (All people-event)

Risk of minor injury from a single event to groups of people greater than $3x10^{-2}$ is normally considered unacceptable.

Group Risk



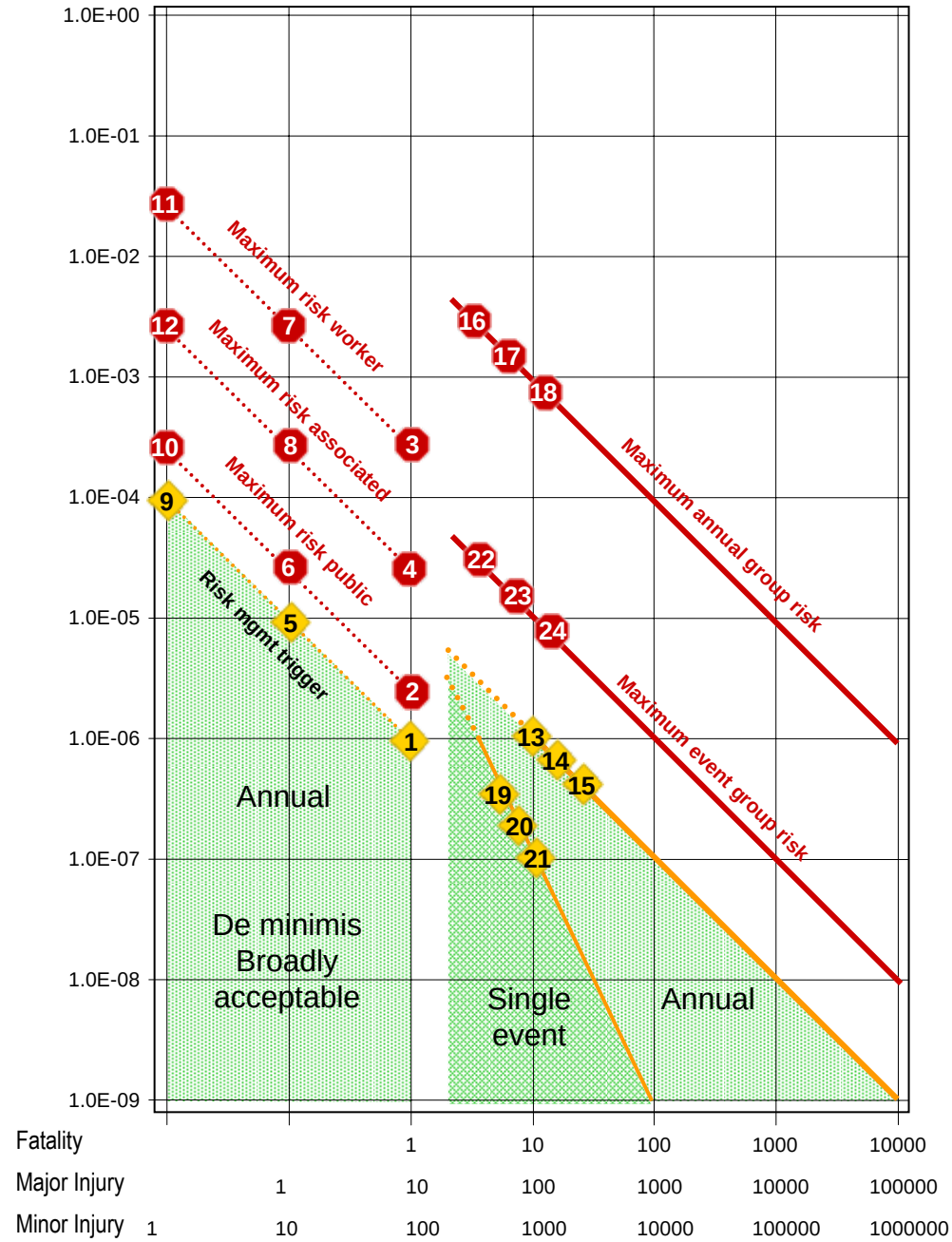
Step 4: Determine annual group risk based on summed individual risk considering precedents (dotted lines).

Step 5: Determine event risk based on annual group and individual risks considering precedents (solid lines).

Features:

- Precedents considered
  - RCC standards
  - DDESB interim guidance
  - FAA standards
  - NATO country standards
- Consequence aversion for risk reduction (steeper slope)

Comparison of 24 Standards



Road signs in risk space

The 24 strawman criteria standards should be self consistent.

By extending the definitions over the full range of consequence a composite definition of the *de minimis* and "normally unacceptable" can be achieved.

Generic System Safety Process

1) Hazard Identification

Develop PHL and RAC Matrices

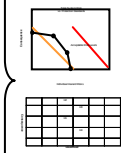
1) Process: The initial step produces a complete definition of the hazards associated with the system. This can be achieved by a variety of techniques shown below. Key elements of the risk assessment matrix are also defined.

1a) Identify Hazards → 1b)Tailor RAC matrix for Phases 2 & 4

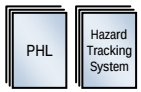
2) Methods and Techniques

1) Checklists
2) System Energy Source Inventory
3) Prior Work with Similar Systems
4) Operating Scenario Walkthroughs
5) Operational Phase Review
6) Codes/Standards/Regulations

1) Define Risk Targets (e.g., Fatalities, Injuries, Monetary Loss , Others…
2) Scale Consequence and Likelihood Axes to Desired Range
3) Subdivide each Axes into appropriate Intervals
4) Assign decision authority for each cell



3) Products:



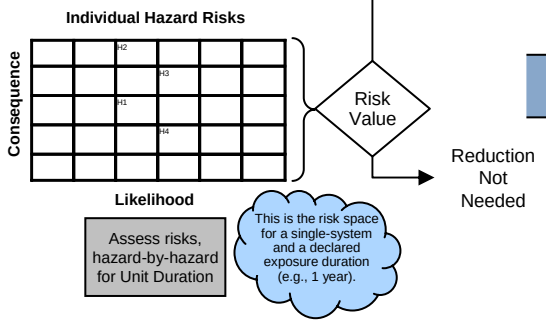
2) Risk Assessment

Assess Each Hazard's Risk(s)

1) Process:

For each identified hazard the severity and likelihood are established. The RAC Matrix is used to assess and display the risk.

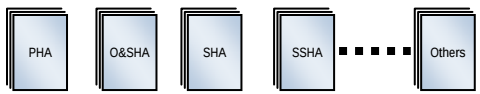
2) Methods and Techniques:



Risks Are Assessed by:

1) Expert Judgment Based on Historical Risk Experience, System Knowledge, Engineering Judgment, what is known/not known.
2) Numerical Analysis
3) Computer Models

3) Products:



3) Risk Reduction

1) Process: Risk Reductions are achieved by understanding the risk, countermeasuring the risk according to an order of precedence, and reassessing risks.

Understand Risk Drivers → Develop Candidate Countermeasures → Select Countermeasures → Re-Assess and Accumulate Risks

2) Methods and Techniques:

Understanding of causation of risk may lead to prioritizing hazard reductions and/or direct counter-measure selection.

Countermeasure Techniques *Order of Precedence:*
1) Design Changes
2) Engineered Safety Features
3) Safety Devices
4) Warning Devices
5) Procedures/Training

Countermeasures shouldn't:
1) Introduce new hazards
2) Unacceptably Impair system performance

Countermeasure Selection Criteria
- Cost (vs., accepting risk)
- Effectiveness (In reducing risk)
- Feasibility
  - Means
  - Schedule

- Total system risk should be accumulated by proper mathematical protocol.
- Reductions are to be validated.

3) Products (typical):

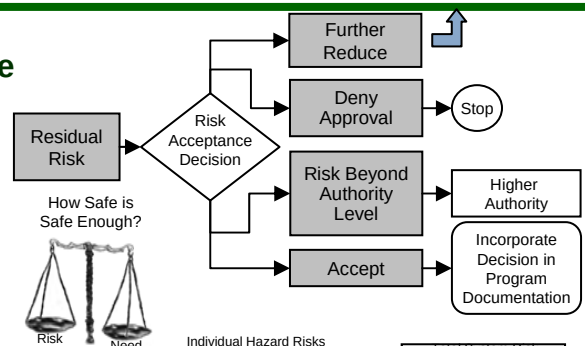
4) Risk Acceptance

1) Process:

Properly designated decision-makers are provided sufficient information to make an informed decision concerning the acceptability of residual risk. All decisions are to be documented.

2) Methods and Techniques:

1) Compare to Protection Standards for
   a) Personnel:
      1) Public
      2) Worker
   b) Groups:
      1) Long-term (annual or life cycle)
      2) Peak Risk (Catastrophe, or events)
2) Balance Risk with Needs

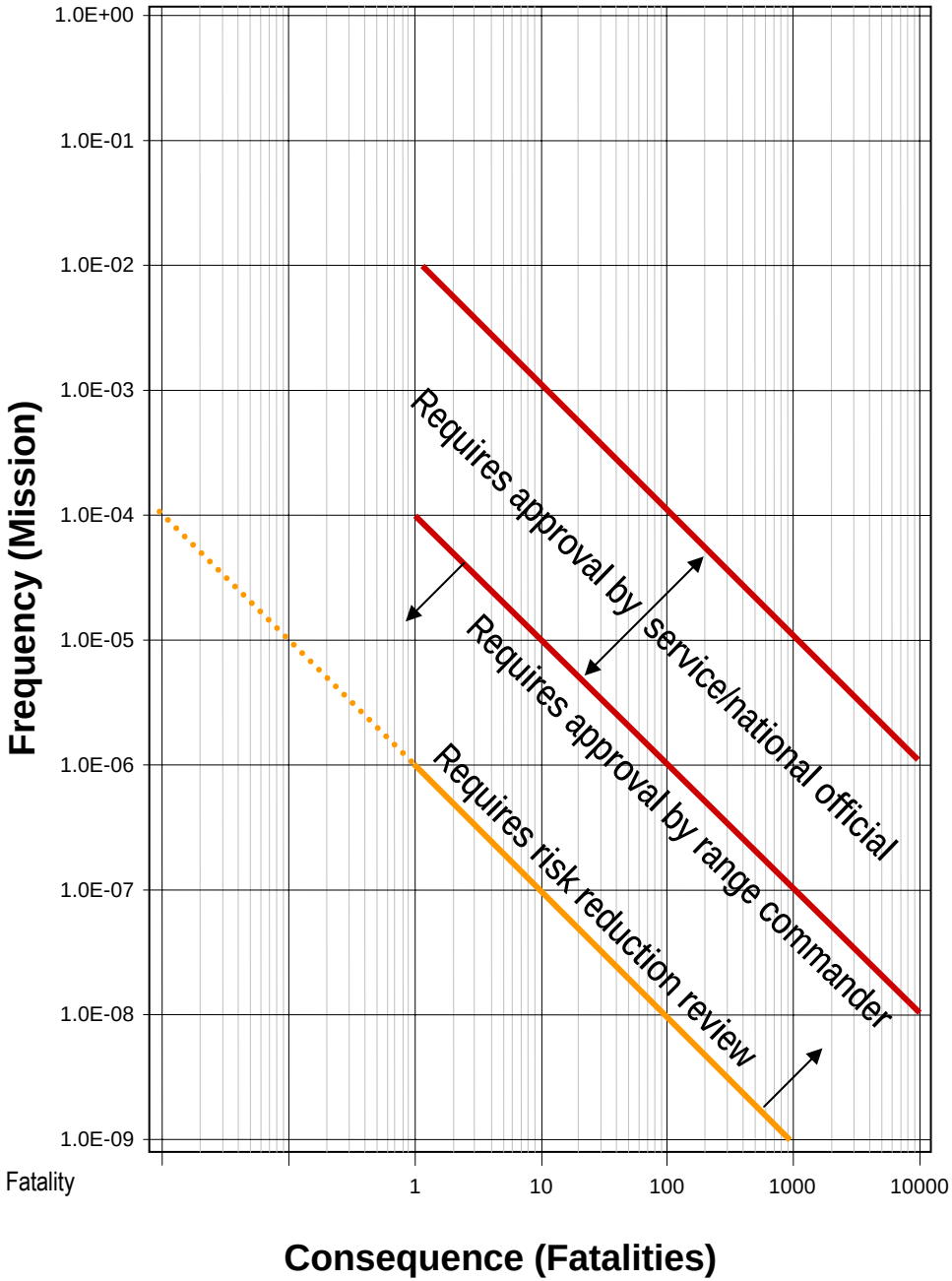


3) Product:

Documented Risk-Based Decision

Other Uses: Range Safety and System Safety

Strawman Launch Approval Approach (based on 24 criteria)

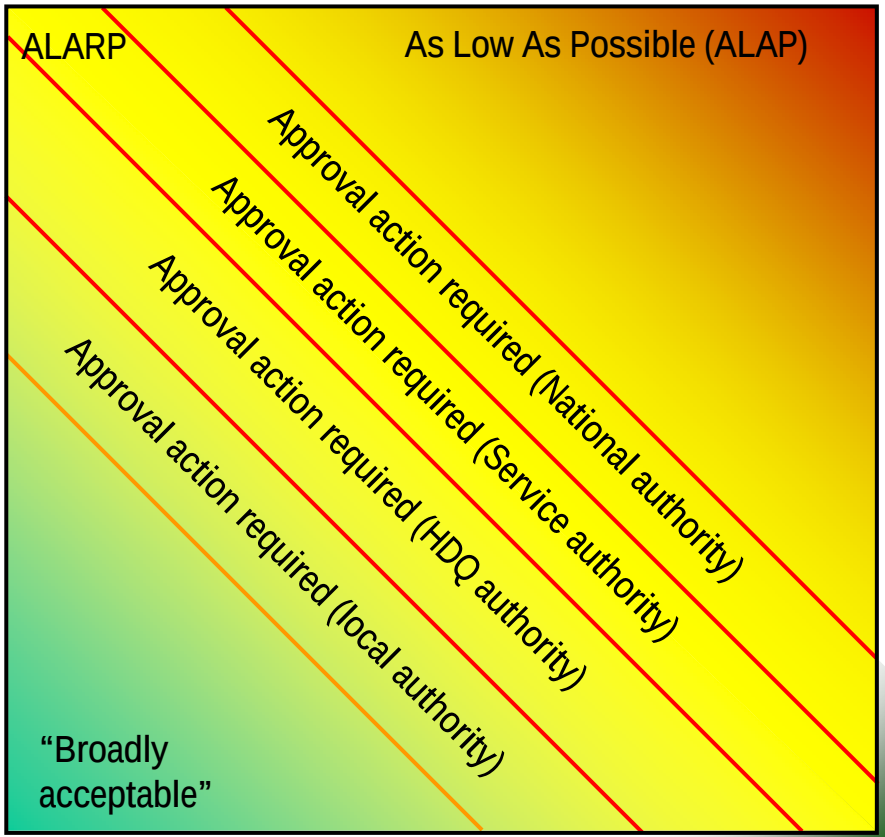


1. **A mandated risk reduction review would:**
   - Be solution oriented increasing advocacy of safety reviews
   - Provide for greater overall safety
   - Communicate to non-safety personnel the role of safety professionals
2. **Approval by higher authority recognizes reality that:**
   - Higher risk may be warranted
   - Better liability protection: discretionary decision process formally undocumented

Action required	Risk level*
Mission risk reduction review	Ef > 1E-6
Approval by range commander	Ef < 1e-4
Approval by Service/national official	1E-4 < Ef < 1e-2

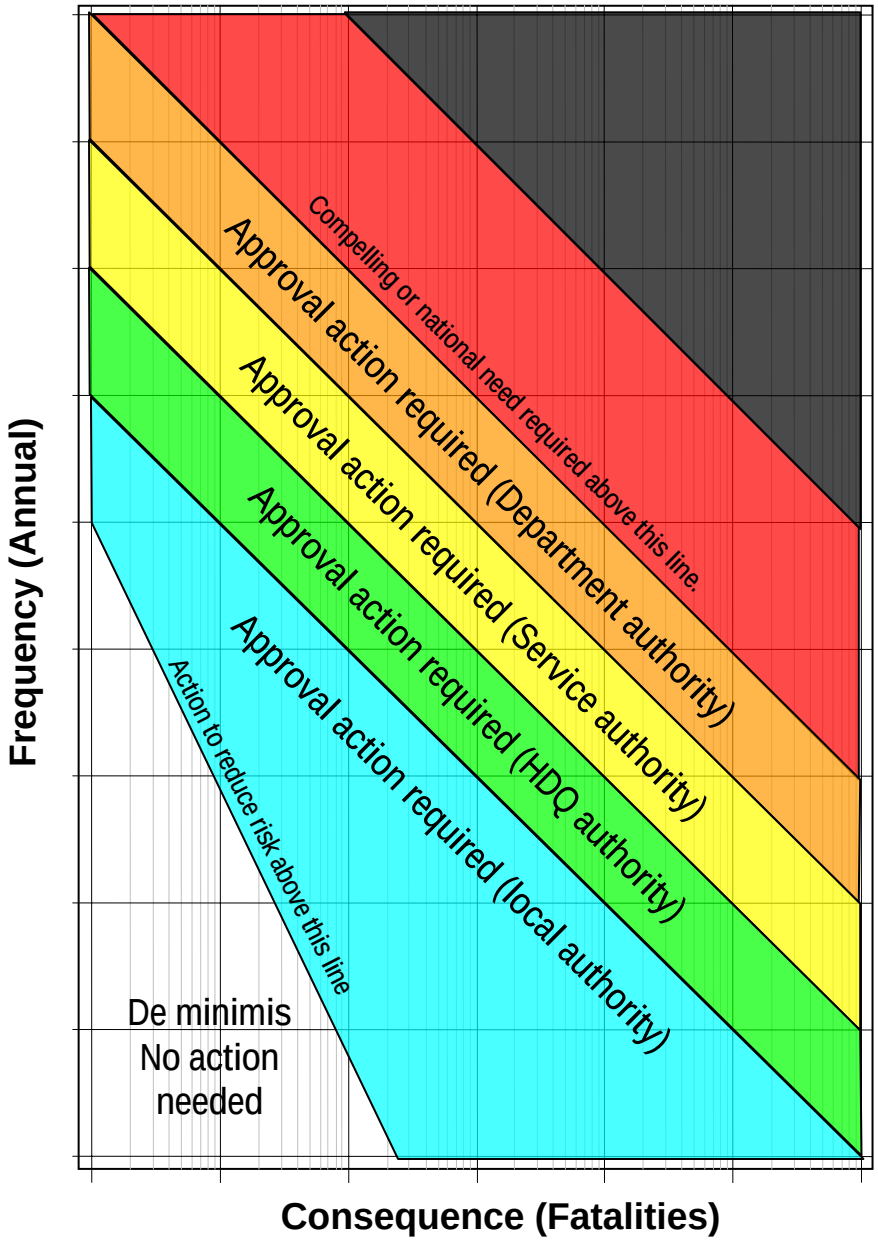
***** Risk levels shown are based on fatalities. Corresponding risk levels exist for major and minor injuries.

What about Multiple Levels of Approval?

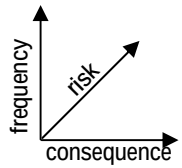


Especially within the system safety community, a conceptual expansion of the "normally unacceptable" standard facilitates multiple decision levels at higher authority.

A Strawman RAC Matrix Based on the 24 Criteria



Major features:



- Consistent protocol
- A defined space: consequence = 6 orders of magnitude, frequency = 9 orders of magnitude
- Iso-risk lines have more logic than either iso-consequence or iso-frequency lines
- Defines “mission” of risk reduction
- Recognizes need for higher review for higher risks
- Consistent with Pascalian concept of risk
- Risk reduction actions are consequence averse

Summary / Conclusions

- Quantitative standards are under development using a systematic, disciplined approach based on societal expectation and legal precedents. They can provide a supportable foundation for:
  - Decision making
  - Triggering risk management actions
  - Tailoring RAC codes

- Potential future work includes:
  - Develop consensus on levels of acceptable risk
    - National
    - International
  - IAASS to coordinate / encourage risk management