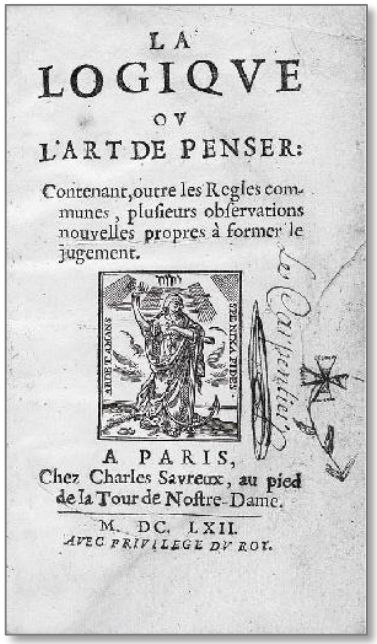
Nine Ideas for Our Discipline

Tom Pfitzer

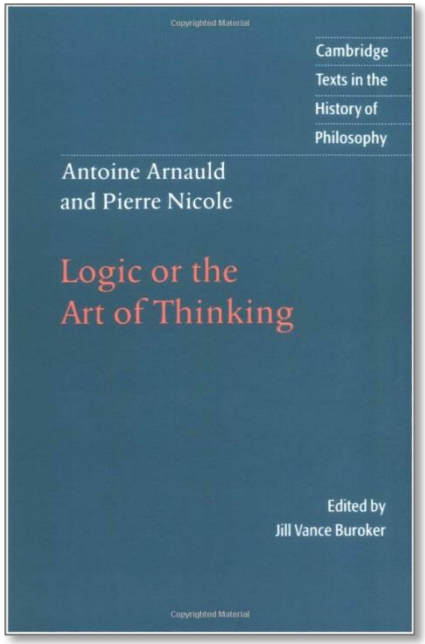
"If you want a new idea, read an old book."

~ Herman Melville &
Edward Demming

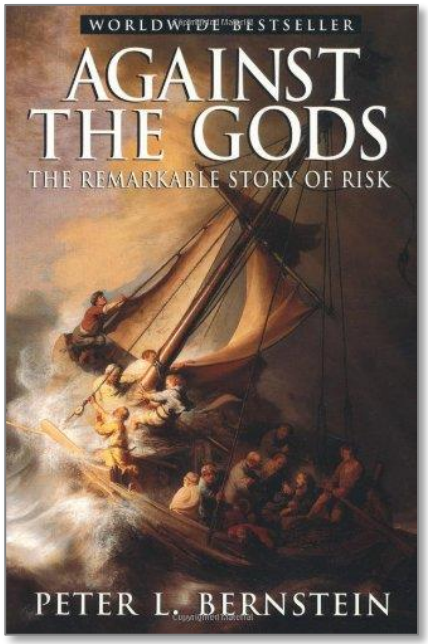
1662



1996



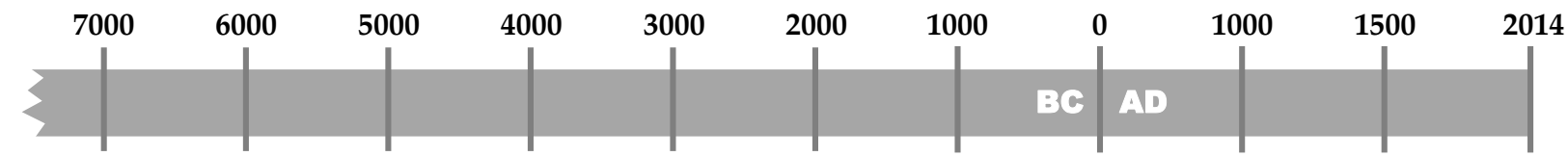
1998



What can history teach us?

Where did the risk management ideas we use today come from?

Many disciplines are ancient.



Counting Methods →

Gambling →
"eikos" = probable = likeness to truth
Abacus → calculus = pebble →
Geometry
Astronomy
Architecture →

"Greeks and Talmudic scholars were maddeningly close to discoveries made during the Renaissance"

- 825: Al Khorizmi arabic arithmetic
- zero → "cifr" = empty

- 1202: Fibonacci *LiberAbaci* Hindu/Arabic number system

Shift to Arabic Numbers

Some of the foundations of risk management originated thousands of years ago

Primary Source: *Against the Gods - The remarkable Story of Risk*
Peter L. Bernstein

Who developed these ideas and when?

Most of the foundational ideas for our discipline were laid in the Renaissance era.

- 1494: Paccioli *Summa de arithmetic, geometria et proportinalità* - algebra, multiplication tables
- 1545: Cardano *Ars Magna* - algebra
- 1565: Cardano *Liber de Ludo Aleae* (book on games of chance)
  - Evidence & reason
  - Concept of probability
  - Probabilities for thrown dice (published 1663)

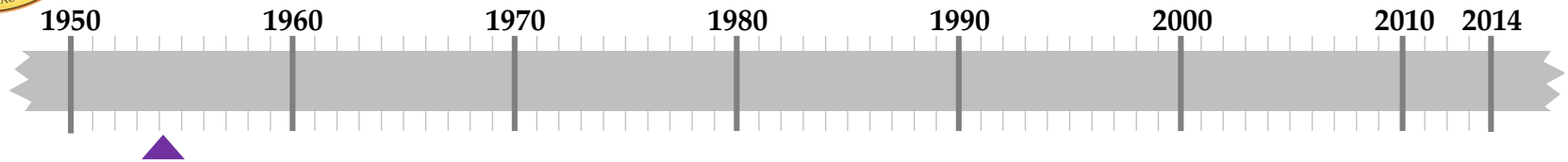
- 1619: Thomas Gataker - Natural laws define outcome
- 1620: Galileo *On Playing Dice*
- 1640 -1650: Pascal & Fermat
  - Pascal's triangle
  - Binomial probabilities
  - Statistical inference
  - Pascal's wager (1662)
- 1660: John Graunt & William Petty- sampling for mortality
- 1662: Port-Royal Monastery *Logic* - Fear of harm ought to be proportional to the gravity of the harm and also probability of the event
  - Hypothesis
  - Dendritics
- 1693: Edmund Halley *Life Expectancy Tables*

- Use of log scale, scientific notation
- 1696: Lloyd's List - Trade and shipping information
- 1771: Society of Lloyd's - first insurance
- 1713: Jacob Bernoulli
  - Law of large numbers
  - Jar of pebbles
  - Degrees of certainty
- 1731: Daniel Bernoulli *St. Petersburg Papers*
  - Expected value
  - Appetite for risk differs (e.g. utility & aversion)
- 1733: DeMoivre *Doctrine of Chances* - bell shaped curve, standard deviation
- 1764: Thomas Bayes - statistical inference

- 1809: Laplace Central Limit Theorem
- 1830: Judge Samuel Putnam - Prudent Man Rule "a trustee---is to observe how men of prudence conduct their affairs---considering probable safety---"
- 1835: Quetelet - average man concept
- 1848: Gauss - normal curve
- 1874: Frances Galton
  - Regression to the mean
  - "Quincunx" probability demonstrator
- 1880: Poincaré - natural causes of uncertainty

- 1921: Frank Knight *A Treatise on Probability*
  - Uncertainty and risk
- 1936: Keynes *General Theory*
  - Evidence seldom fits theory
  - Means change
- 1926 - 1953: John Von Newman
  - Gaming Theory
  - Utility analysis
- 1948: Harry Truman "There are three kinds of liars: liars, damn liars, and statisticians"

How have the ideas been vetted?



System Safety Defined as discipline 1954

System Safety Society

ISSS founded

1st SSS Conference

Conferences Share Ideas

32nd SSS Conference

G-48

Three Meetings Per Year

Incorporate Best Practices into MIL-STD

Summing Risk Workshop

ANSI/GEIA-STD-0010-2009

MIL-STD

MIL-STD-882 1st Edition

MIL-STD-882A

MIL-STD-882B

MIL-STD-882C

MIL-STD-882D

MIL-STD-882E

DDESB

DDESB embraces risk-based methods

DDESB embraces URS

International Use

New Ideas

System Safety Performance Level Workshop

RAC Matrix Improvements

Workshop on Public Safety Risk of Launch

IARA

Risk Summing

Safety Case Workshop

Web-Based Risk Assessment Workshop

Road Signs in Risk Space

Idea ⇒ Concept ⇒ Tools ⇒ Acceptance ⇒ Use

Ideas from History

IDEA #1:

» As a new discipline, we must be continuously open to new and expanded thinking.

IDEA #2:

» It takes decades for the best ideas to become accepted and implemented.

How is our profession perceived?

- Are we policemen?
- Do we offer restrictions or solutions?
- When we enter a room of system developers, are they glad to see us?

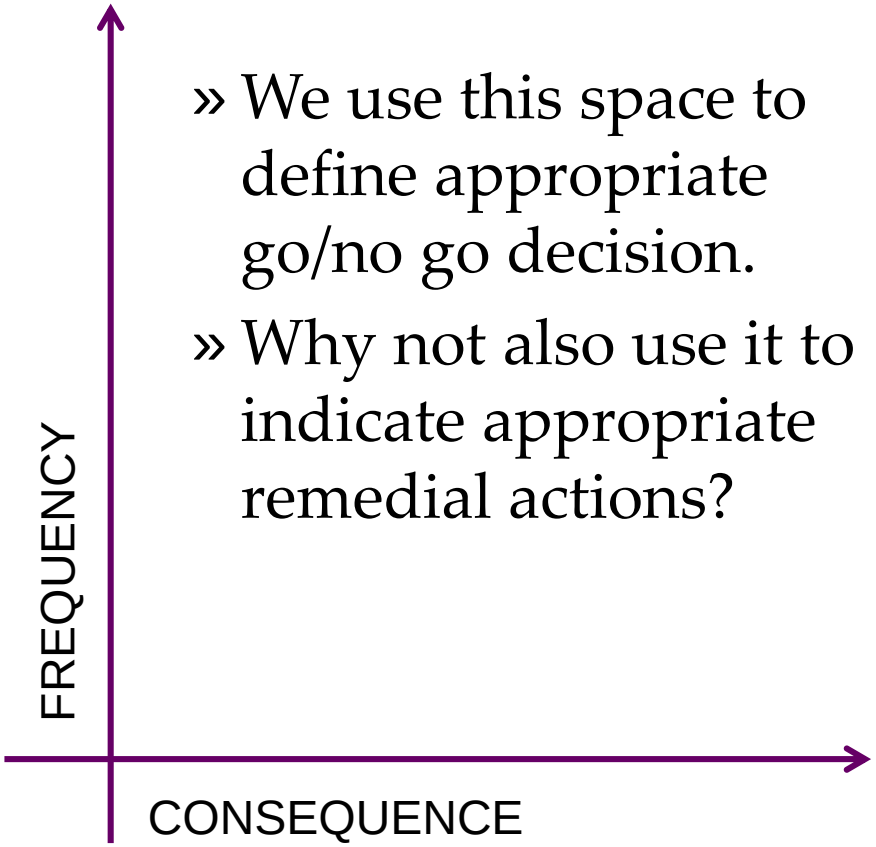
Use by Government Agencies

- Our discipline is used to aid in Agency decision making.
- We must be careful to avoid simple stop/go decisions.
- Our job is to reduce risk.
- If we are to be a discipline, we need a broad spectrum of solutions.

IDEA #3:

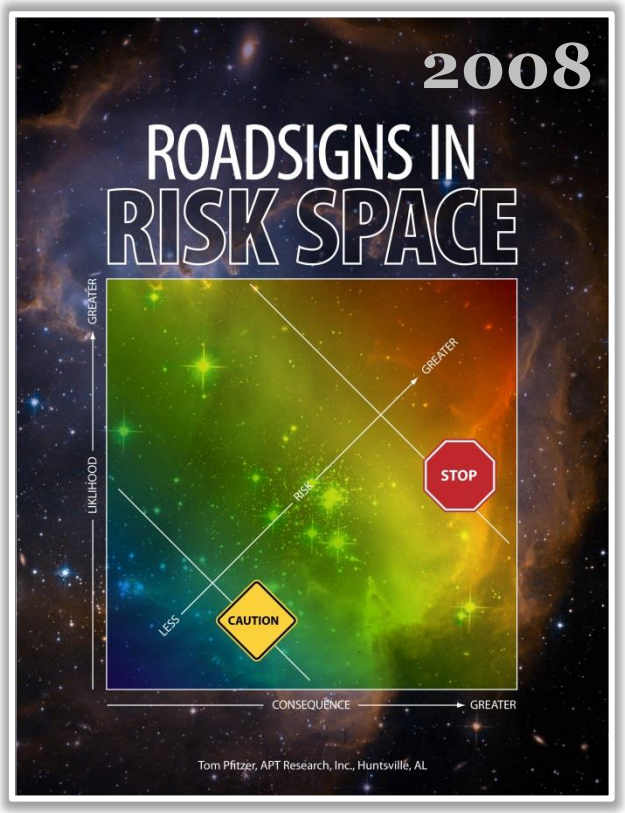
- Processes within a bureaucracy can be cross purpose with good practice of our discipline.

Road Signs In Risk Space

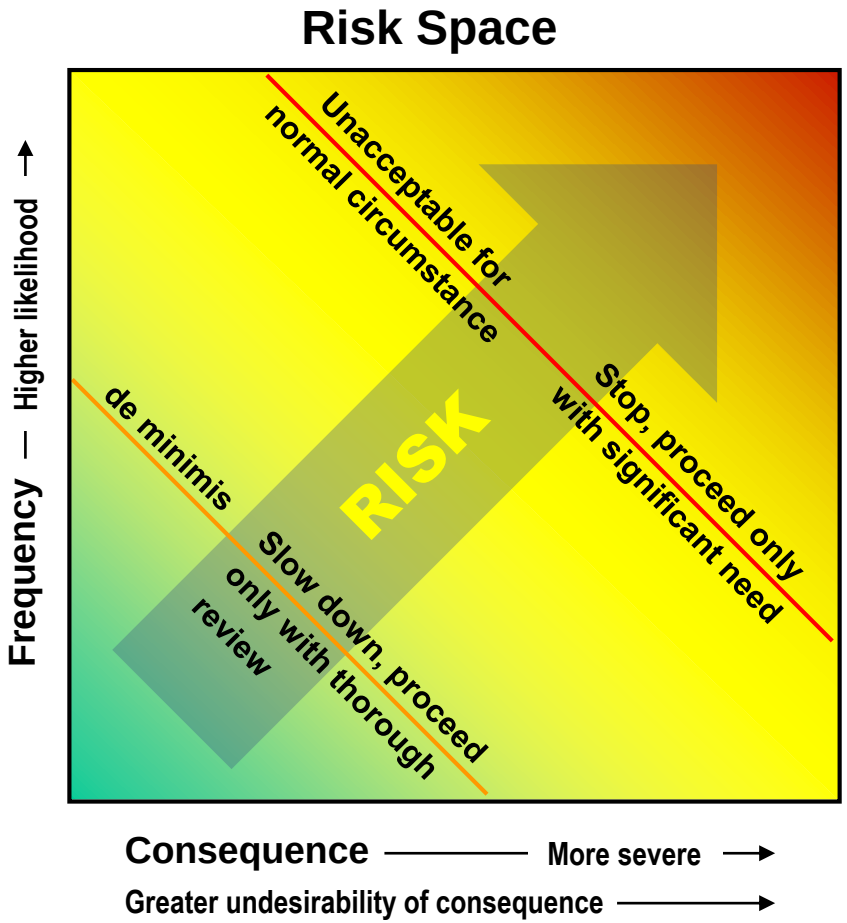


» We use this space to define appropriate go/no go decision.

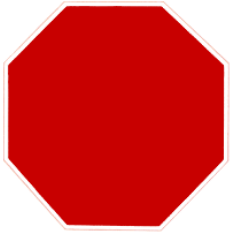
» Why not also use it to indicate appropriate remedial actions?



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
- Many actions may be indicated

IDEA #4: As practitioners, we should have a wide variety of solutions to reduce risk

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

There are only a few red signs. We need more solutions that prescribe risk reduction actions.

What is the preferred measure?

» Risk is the mathematical product defined by multiplying two independent metrics

Risk = Consequence × Probability

Area = Length × Width

Torque = Force × Length of Moment Arm

Momentum = Mass × Velocity

» **IDEA 5:** As a discipline, we need to be more comfortable quantifying risk and if risk is the preferred measure…

IDEA #6: Total system risk is the preferred metric

r = Partial risk = Hazard Severity × Hazard Probability

$$R_T \approx \sum_{i=1}^{i=n} r_i = r_1 + r_2 + r_3 + \ldots + r_n$$

where:

R_T = Total Risk

$$R_S \approx \sum_{i=1}^{i=n} M_i \sum_{i=1}^{i=n} A_i \sum_{i=1}^{i=n} (r_i = s_i \times p_i)$$

where:

R_T = Total Risk

s_i = Hazard Severity for the i^{th} identified hazard

p_i = Hazard Probability for the i^{th} identified hazard

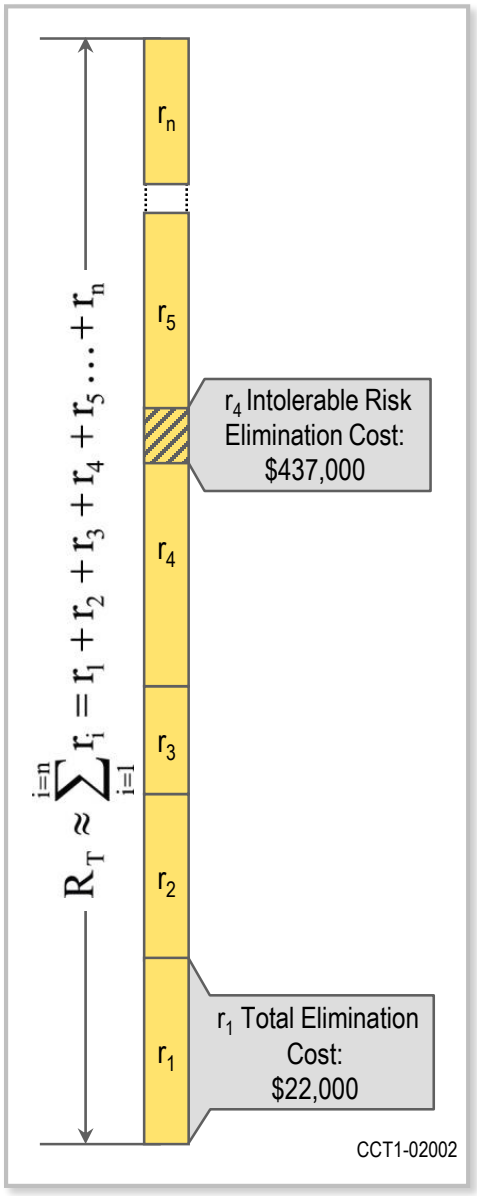
r_i = Risk posed by the i^{th} identified hazard

A_i = Identity of the i^{th} asset under threat

M_i = The i^{th} system Mission or Operational Phase under consideration

R_S = Total System Risk = the risk of all hazards, for all life cycle phases for all elements in our system

Notional



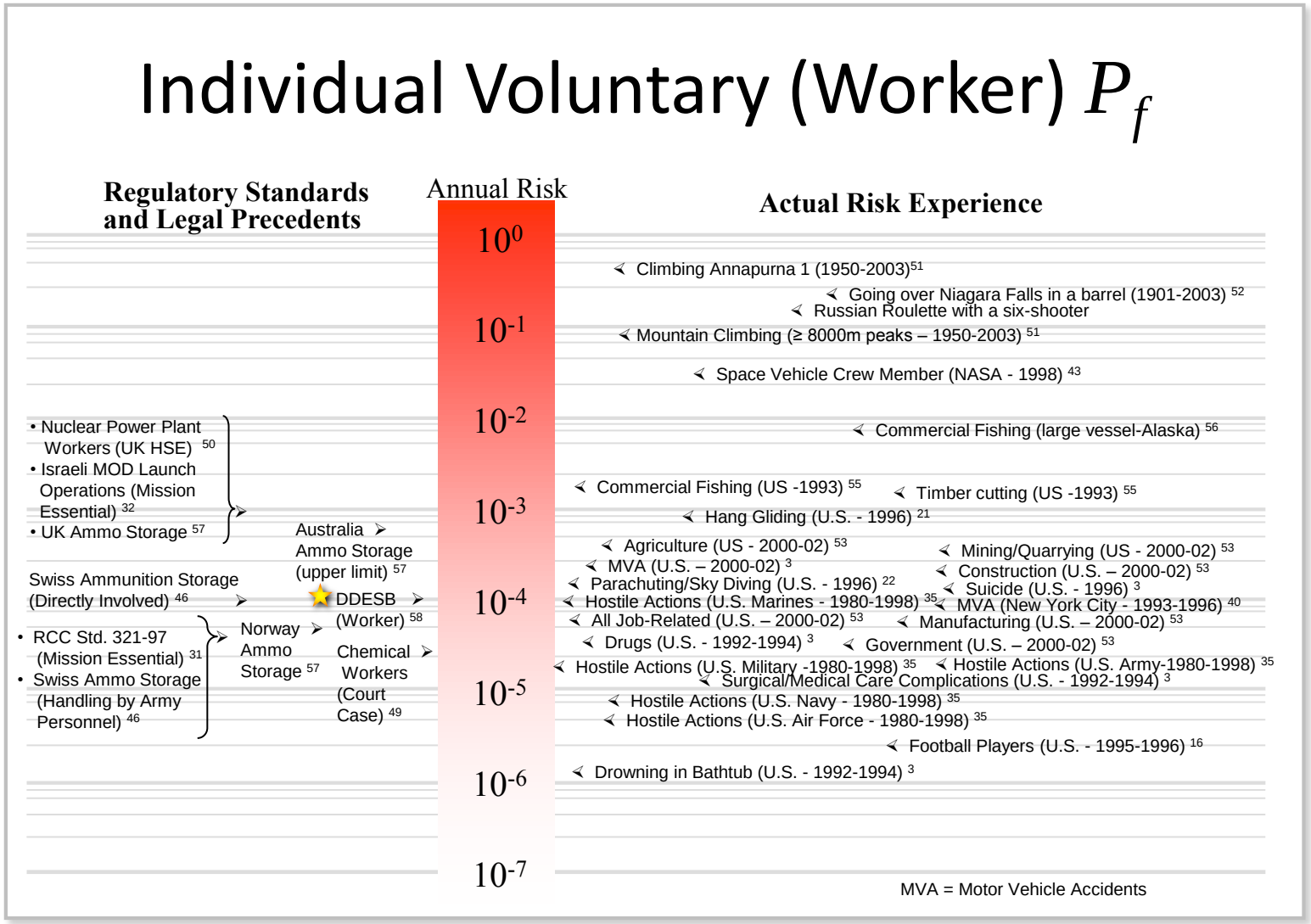
Estimating Total System Risk is Easy

	Hazard Name	Undesired Consequence	Probability	Risk (r)	Reduction Action	Final Risk (r)
1						
2						
3						
n						
			Total System Risk (R)			

- A conservative estimate can be defined by simple addition.
- In most cases, hazards can be defined to combine dependent hazards as a single hazard, thus eliminating dependencies.
- Detailed methodology is contained in the *Risk Summing Guidebook*.

IDEA #7: URS can become a decision aid

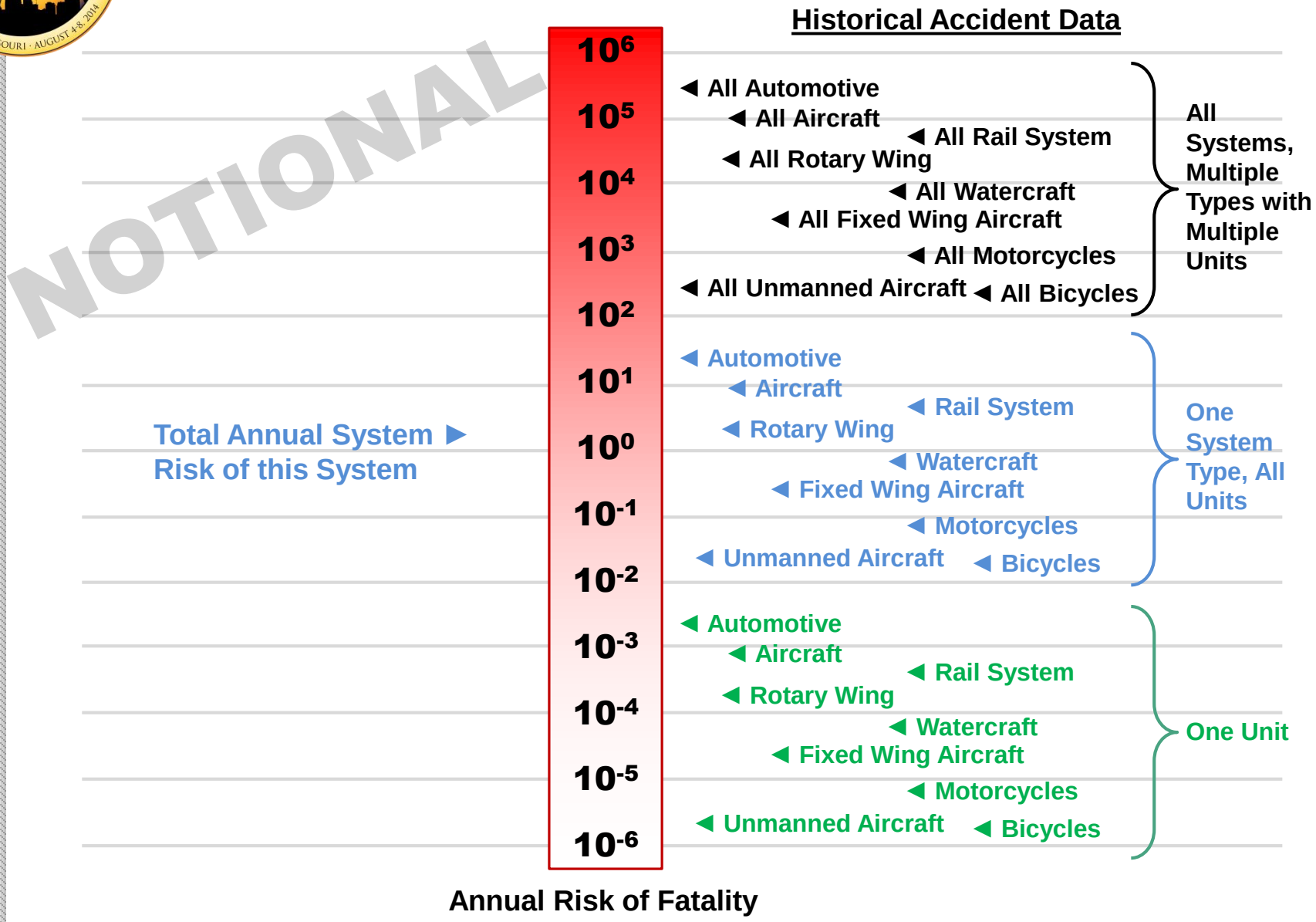
The risk of our "system" can be compared to other known risks.



Helps make more informed decisions.

URS for Total System Risk

for US Populations – Transportation Systems



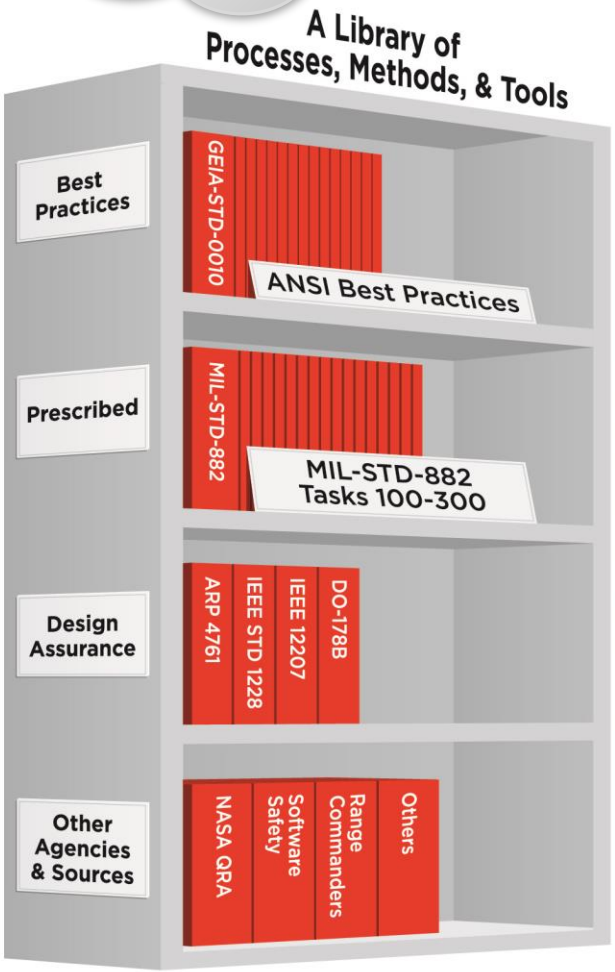
IDEA #8: Total System Risks are comparable to many other types of risk

Human Injury/ Illness	Environmental Damage	Cost to Repair /Recover	Schedule Delays	Mission Damage	Adverse Program Publicity
Multiple Deaths > 30	> $100M or Clean-up Recovery Unachievable	> $100M or Recovery Not Possible	Factor of 100 Overrun	All Major Goals Aborted	> $100M or Irreparable Harm
Multiple Serious Injuries/Illnesses > 10	> $30M or Clean-up Cost	> $30M	Factor of 30 Overrun	Half Major Goals Aborted	> $30M to Repair
Permanent Total Disability	> $10M or Clean-up Cost	> $10M	Factor of 10 Overrun	> One Major Goal Aborted	> $10M to Repair
Permanent Partial Disability	> $3M or Clean-up Cost	> $3M	Factor of 3 Overrun	One Major	> $3M to Repair
Protracted Hospitalization > 3 wks	> $1M or Clean-up Cost	> $1M	> 100% Overrun	A	
> 5 Man Weeks Lost Time	> $300K or Clean-up Cost	> $300K	> 30% Overrun	H	
> 1 Man Week Lost Time	> $100K or Clean-up Cost	> $100K	> 10% Overrun	>	
OSHA Recordable Injury/Illness	> $30K or Clean-up Cost	> $30K	> 3% Overrun	C	
Nuisance Contusion/Abrasion	> $10K or Clean-up Cost	> $10K	> 1% Overrun	S	
None	None	None	None	N	

IDEA #9: The Safety Case Approach

A bottom-up process policed by safety professionals to assign risks to each hazard.

The developer makes top-down claims which must be proven with tests and data.



Can Incorporate any Technique

- Information Defining Risk
- Mitigations
- Verifications (Pros & Cons)
- Unknowns: Known & Unknow
- Assumptions/ Constraints/ Limitations

The Safety Case

Makes a Success Oriented Case for Key Decision Points
(this system is acceptably safe because: claims a-z)

- Attributes
  - Structured Arguments
  - Evidence
  - Compelling
  - Comprehensive
- Reviewed Independently
- Summary Report Presented to Decision Makers as Part of an Informed Decision Making Process

Summary of 9 Ideas with Merit

1. As a new discipline, we must be continuously open to new and expanded thinking.
2. It takes decades for the best ideas to become accepted and implemented.
3. Processes within a bureaucracy can be cross purpose with good practice of our discipline.
4. As practitioners, we should have a wide variety of solutions to reduce risk.
5. As a discipline, we need to be more comfortable quantifying risk.
6. Total system risk is the preferred metric.
7. URS can become a decision aid.
8. Total system risks are comparable to many other types of risk.
9. The safety case approach.

Good ideas need development, advocacy, time, and an open-minded spirit of continuous improvement to reach fruition.

References

1. "Logic, or, The Art of Thinking," Antoine Arnauld and Pierre Nicole, 1996 (originally published in 1662).
2. "Against the Gods: The Remarkable Story of Risk," Peter L. Bernstein, 1998.
3. "Roadsigns in Risk Space," T. Pfitzer, 2008.
4. "Risk Summing Guidebook – Understanding and Implementing Risk Summing as a Practical Element of Risk Management," A-P-T Research, Inc., 2011.
5. "Universal Risk Scales – A Tool for Developing Risk Criteria by Consensus," B. Pfitzer, M. Hardwick, T. Pfitzer, Dr. J. Ward, 2004.
6. "ART – APT Risk-Management Tool for Performing Risk Assessments," N. Donath, T. Pfitzer, 2009.


INTERNATIONAL SYSTEM SAFETY TRAINING SYMPOSIUM
GATEWAY TO SAFETY
ST. LOUIS, MISSOURI · AUGUST 4-8, 2014

Questions