Risk Assessment

John A. Paravantis
Professor
Department of International & European Studies
UNIVERSITY OF PIRAEUS

2023-10

Common hazards:

- Slips, trips, falls
- Illness (including food-borne), disease
- Animal attacks
- Car, motorbike, bicycle, pedestrian accidents
- Team (e.g. basketball) and individual (skiing) sports accidents
- Electricity-related accidents
- Fires
- Weather-related accidents
- Identity theft (Internet)

Hazards for heads of state (further to those of common men):

- Assasination
- Stress-related disease from decision making, war
- Transportation accidents, e.g. airplane crash

"Lech Kaczyński, the fourth President of the Republic of Poland, died on 10 April 2010, after a Polish Air Force Tu-154 crashed outside of Smolensk, Russia, killing all 96 aboard. His wife, economist and First Lady Maria Kaczyńska, was also among those killed." [Wikipedia]

Risk assessment analyzes complex systems, and (combinations of) tasks for hazards and associated risks

- Probability: A measure of how likely it is that some event will occur
- Hazard: A source of potential damage, harm or adverse health effects on something or someone under certain conditions (usually at work)
- Severity: The degree of something undesirable
- Consequence: The effect, result, or outcome of something occurring earlier
- Vulnerability: A weakness in a system or human that is susceptible to harm
- Threat: Source of danger (threat and hazard are considered analogous)

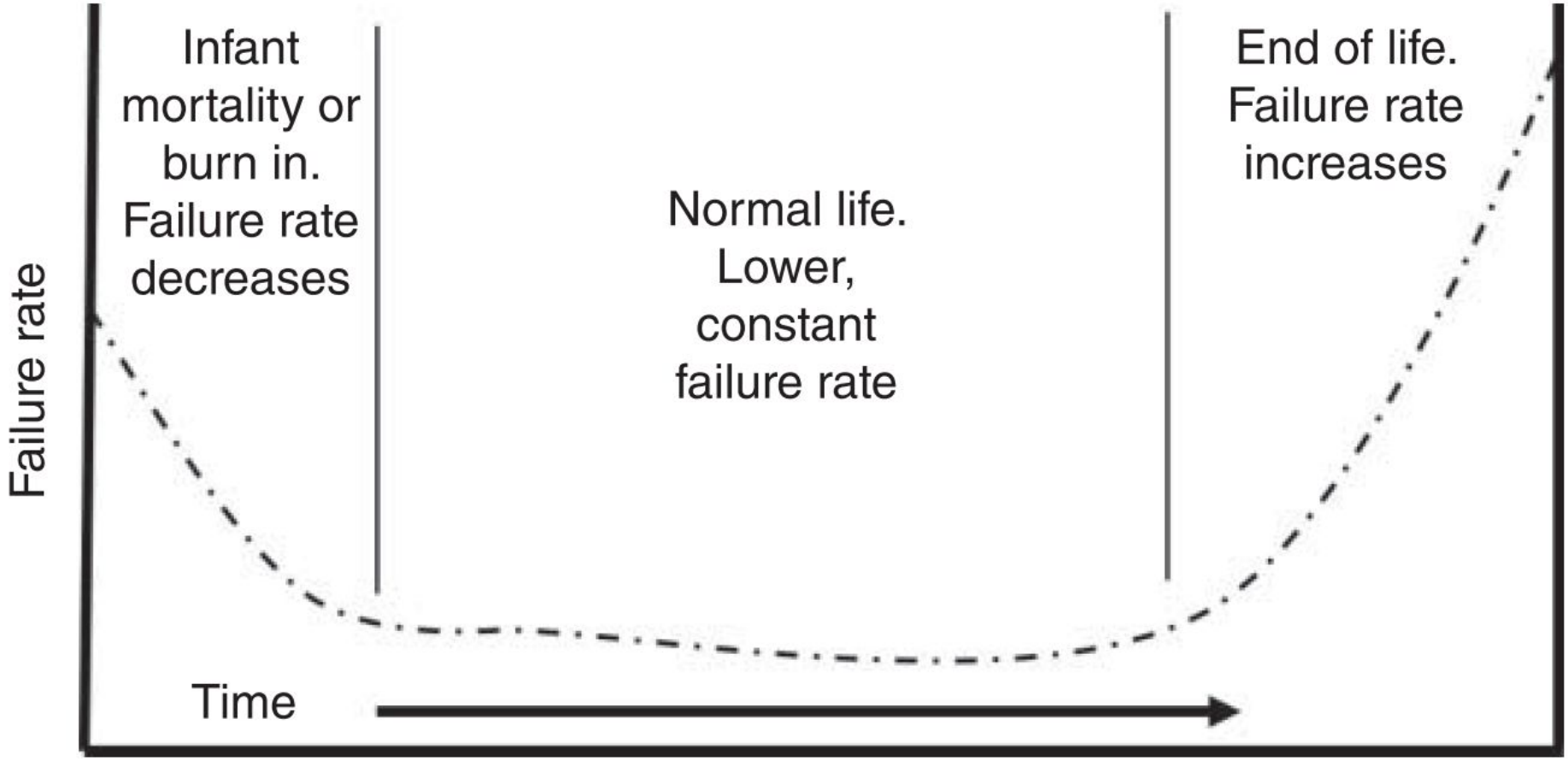


FIGURE 1.1 Bathtub curve.

Manufacturers usually provide a warranty for a system (e.g. a car) for the period of time from birth till just before system wears out

- This way they maximize their public image while minimizing their risks or obligations

Accidents may occur early in a system's life cycle because of reasons such as:

- Mismatch of materials
- Hardware/software incompatibilities
- Lack of system understanding
- Operator inexperience or lack of training

Risk = Negative consequence

Opportunity = Positive consequence

Three questions define risk:

1. What can go wrong?
2. How likely is it?
3. What are the consequences?

Techniques that enhance risk assessment:

- Task analysis
  - *Determines human actions in a process*
- Delphi method
  - *Elicits the probabilities for human errors*
- Critical incident technique
  - *Develops risk scenarios*

Preliminary hazard analysis (PHA)	This tool is used in the very beginning of a risk assessment and/or on a conceptual design of a new system, process, or operation. It is used to determine the potential hazards associated with or the potential threats poised to a system, process, or operation. This tool is also useful for organizations to evaluate processes that have been performed for years to determine the hazards associated with them

Failure mode and effects analysis (FMEA)	This tool is used in system, process, or operations development to determine potential failure modes within the system and provides a means to classify the failures by their severity and likelihood. It is usually performed after a PHA and before more detailed analyses

Failure mode, effects, and criticality analysis (FMECA)

FMECA extends FMEA by including a criticality analysis that is used to chart the probability of failure modes against the severity of their consequences. FMECA can be used instead of an FMEA, in conjunction with an FMEA, or after an FMEA has been performed

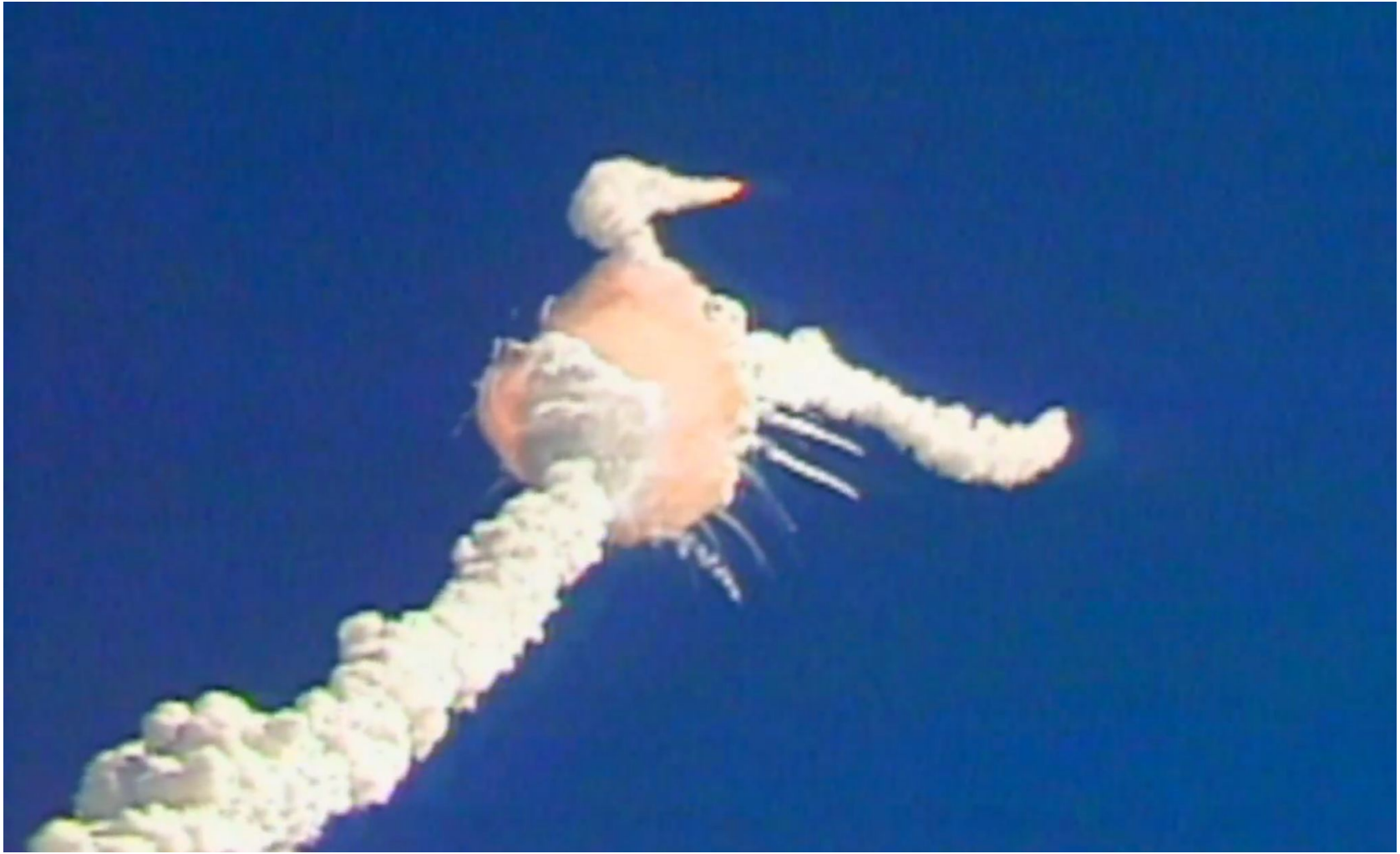
Event trees

Event trees are very useful tools to begin to analyze the sequence of events in potential accident sequences. They also have utility in analyzing accidents themselves. Many variations of event trees have been developed.

Fault tree analysis (FTA)	FTA is a risk analysis tool that uses Boolean logic to combine events. The lower-level events are called basic events, and they are combined with Boolean logic gates into a tree structure, with the undesired event of interest at the top. This event is called the top event. Though this analysis tool is used to quantitatively determine the overall probability of an undesired event, it is also useful from a qualitative perspective to graphically show how these events combine to lead to the undesired event of interest. FTA has a wide range of use from determining how one's checking account was over drawn to determining why a space shuttle crashed

Fault tree analysis (FTA)	FTA is a risk analysis tool that uses Boolean logic to combine events. The lower-level events are called basic events, and they are combined with Boolean logic gates into a tree structure, with the undesired event of interest at the top. This event is called the top event. Though this analysis tool is used to quantitatively determine the overall probability of an undesired event, it is also useful from a qualitative perspective to graphically show how these events combine to lead to the undesired event of interest. FTA has a wide range of use from determining how one's checking account was over drawn to determining why a space shuttle crashed


AP




NASA
NASA
NASA
NASA
NASA

Human reliability analysis (HRA)	HRA is related to the field of human factors engineering and ergonomics and refers to the reliability of humans in complex operating environments such as aviation, transportation, the military, or medicine. HRA is used to determine the human operators' contribution to risk in a system

Probabilistic risk assessment (PRA)	PRA is a systematic and comprehensive methodology to evaluate risks associated with complex engineered systems, processes, or operations such as spacecraft, airplanes, or nuclear power plant. PRA uses combinations of all the other risk assessment tools and techniques to build an integrated risk model of a system. A fully integrated PRA of a nuclear power plant, for instance, can take years to perform and can cost millions of dollars. It is reserved for the most complex of systems

Risk assessment team members:

1. Management
2. Engineers
3. Workers/operators/supervisors
4. Health and safety
5. Maintenance

Steps in risk assessment:

1. Identify (potential) hazards
2. Identify users and/or tasks
3. Determine the level of risk:
    a. Low: acceptable
    b. Medium: moderately acceptable
    c. High: not acceptable
4. Evaluate potential controls (elimination, substitution, engineering controls, administration controls, personal protective equipment)
5. Develop a report
6. Implement and review

Sensations ≠ Perceptions

- Sensations are physiological
- Perceptions are learned

There are no “facts”, only risk perceptions, shaped by factors such as

- Age
- Income
- Experience
- Education, etc.

Cases that seem like “black magic” to laypeople:

- Fission or fusion
- Secret laboratories
- Government weapon facilities

Decades of use and familiarity make people comfortable with hazards like propane (Liquid Petroleum Gas or LPG)

- For example, 6000 gallons (22712.5 liters or 6.68 tons) of propane in a tanker truck contain approximately 549 million BTUs
- These are equal to 138.4 tons of TNT or a small nuclear bomb
- *Still, it’s just propane, right?*
- Ships may carry tanks with 50,000 tons of propane!


DETWEILER'S
PROPANE
Gas Service, LC
1075
FLAMMABLE
COMPRESSED GAS
AT-UR-DOOR
GAS
SERVICE
755-2651
US DOT217679 FL

How do the experts perceive risk

- A low probability of an incident's occurrence is enough to quantify a risk as insignificant

This approach is mathematically valid, but does not consider the emotional components of the public

- Emotions are powerful
- Scientific apathy is a dangerous attitude

Experience is the greatest influence on a layperson's risk perception

- The impact of experience is greater than that of science

Influences on ideals (principles):

- Parental influence
- Religious posturing
- Peer pressure
- Social paradigm
- Economic stratification, etc.

Most people establish their ideals early in life and stick to them

Also, birds of the same feather flock together!

- A group (e.g. religious, “green”, technical) has anticipated ideals

Rules of thumb (*“cognitive heuristics”*) are unconsciously applied by most people daily

- Such rules of thumb though are like common sense in the sense that they’re not common – they change and adapt with use and over time!

What to do?

- Plan on providing the right information to the right ears
    - Select the facts each group (general public, elected officials, risk professionals, etc.) needs to hear

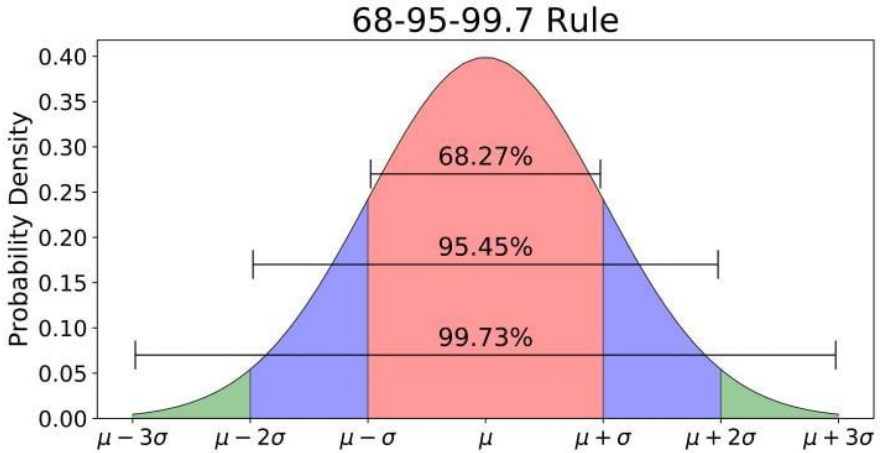
The public wants to hear what the hazards are and know how (and why) there's not a threat to their children when they are running about in the backyard

Elected officials need the same information, but peppered with solid and supportable statistics, sound bites, and concise thoughts

Risk professionals need details

Statistically speaking, an organization's best return for their dollar will come from

- Targeting the center of the risk perception bell curve
- Finding a way to include as much of the standard deviation as responsible spending allows

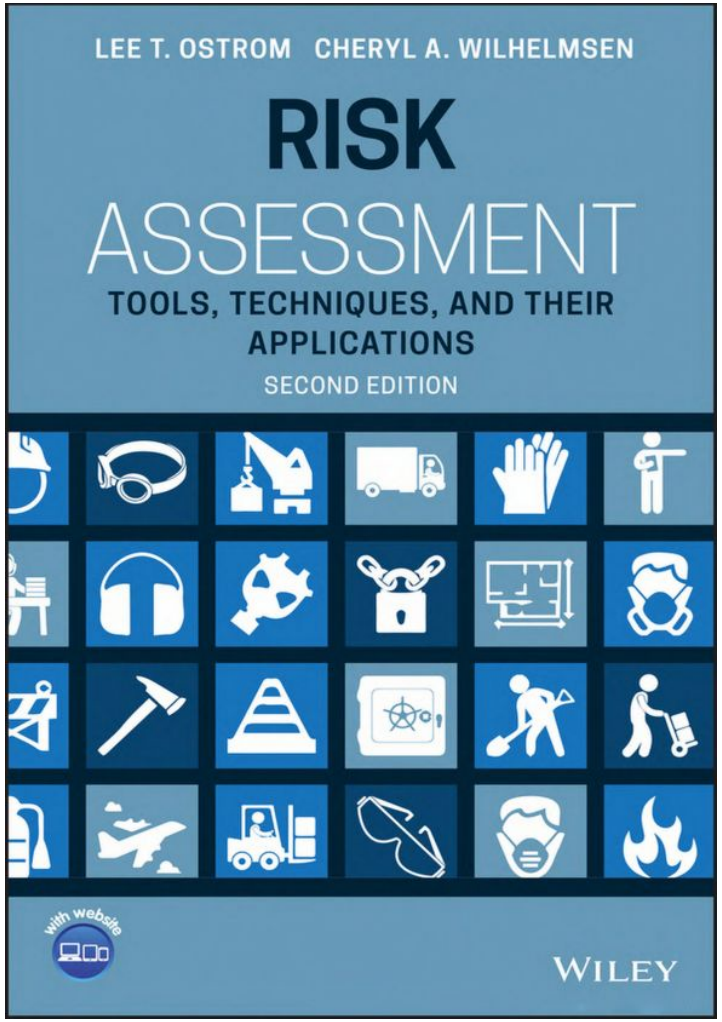


What to do about dissenters

- Remember: perspective is learned
- Undermining the dissenter’s teachings may be regarded as an attack on the person and not the idea
- Provide more powerful teachings
    - The best “high-road” option here would be to speak about the criticism of the detractors, but do so in a positive and fact-filled manner

In the end, the members of the public whose perception you wish to influence, will make their minds up based on ideals, ideas, and rules of thumb anyway…

- If you’ve given them the education they require, that’s the best you can hope for!


LEE T. OSTROM CHERYL A. WILHELMSEN
RISK
ASSESSMENT
TOOLS, TECHNIQUES, AND THEIR APPLICATIONS
SECOND EDITION
with website
WILEY