NE529
RISK ASSESSMENT
Risk assessment & management overview
1

R. A. Borrelli

University of Idaho

University of Idaho
Department of Nuclear Engineering
and Industrial Management

Idaho Falls Center for Higher Education

Learning objectives

Classifying risk

Developing risk assessments

Critically analyze the implications of utilitarianism

This was my first class at Berkeley from Prof. W. E. Kastenberg, one of the pioneers in the field

Chapters 1 – 3 in the book

This is a little all over the place

Learning nodes

Risk

Three questions

Risk assessment

Classifying risk

Severity

Risk matrix

Risk management

Hazard assessment

Applications

Human factors

Risk for lifecycle assessment

Frequency

Uncertainty

Ethical theories

Context

More learning nodes

Case studies

Challenger

Ford Pinto

Repository

Dreamliner

Drawbacks

Alternatives

Fault trees

Event trees

Risk perception

Seminal literature

What is risk?

Risk has been around for a long time

. . . the appearance of disease in human populations is influenced by the quality of air, water, and food; the topography of the land; and general living habits.

– Hippocrates; Air, Water and Places

Make sure everyone knows who this guy is

Risk is the possibility of loss

A dangerous factor

Person or thing that is a specified hazard

A hazard is an existing or potential condition that can cause injury, illness, or death; damage to, or loss of equipment and property; or degradation of the mission

Hazard identification
Human studies
Animal studies
Cell/tissue studies
Exposure surveys

Risk is the probability of an event multiplied by its consequences

Exposure to injury or loss

Risk level is expressed in terms of hazard probability and severity

Probability = Frequency that an event will occur

Severity = Expected result of an event (degree of injury, property damage or other mission impairing factors)

Exposure = frequency and length of time soldiers, equipment, and missions are subjected to a hazard

Controls = actions taken to eliminate or reduce the risks identified

What are the risks for driving a car?

$$[120 \times 10^6 \ \frac{accidents}{year}] \cdot [\frac{1}{300} \ \frac{death}{accident}] = 40 \times 10^3 \ \frac{death}{year}$$

$$[40 \times 10^3 \ \frac{death}{year}] \cdot [\frac{}{250 \times 10^6 \ people}] = \frac{1}{6250} \ \frac{death}{person \cdot year}$$

$$[\frac{1}{6250} \ \frac{death}{person \cdot year}] \cdot [\frac{70 \ year}{}] = \frac{1}{89.3} \ \frac{death}{person}$$

Then ‘safe’ means free from risk‘

Secure from threat of danger, harm or loss

Affording safety from danger

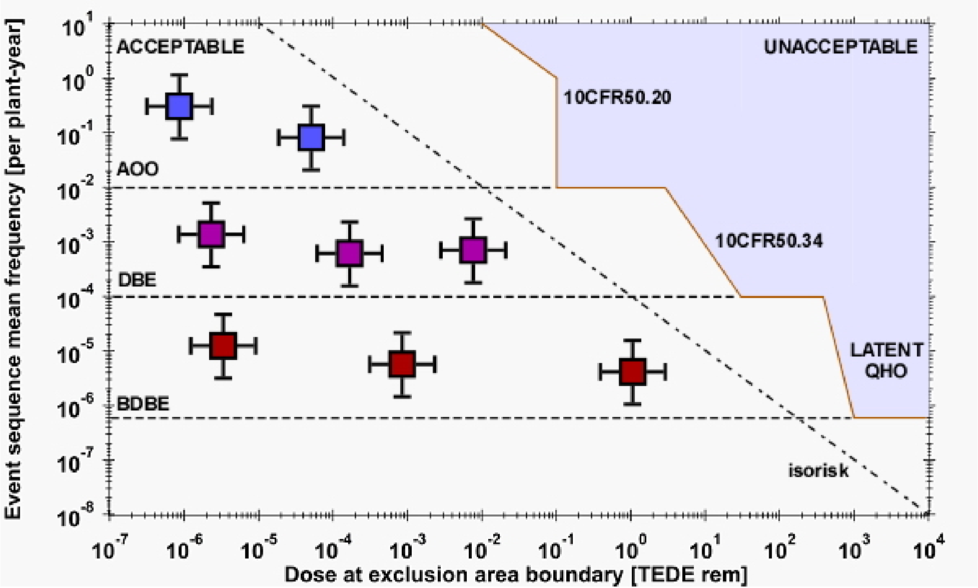
So can you really say anything is safe?

Should the engineer say something is safe?

Like a car, reactor, plane, space shuttle

What can you do?

$Risk = frequency \times consequence$



Risk involves three essential questions

What can go wrong?
How likely is it to happen?
What are the consequences?

Risk assessment

Risk assessment starts with identification of hazards

Characterization of an individual hazard or all identified hazards combined to complete a task

Residual risk = level of risk remaining after controls have been implemented

Controls are altered until the residual risk is at an acceptable level or until it cannot practically be further reduced

Multiple hazards have varying residual risk

Kind of like ALARA in nuclear engineering problems

Risk assessment is a retrospective process

Developed by the US Space Program in 50s and 60s

Failure Modes & Effects Analysis (FMEA) to both correct missile and rocket failures

Reactor Safety Study WASH-1400

Only after about 75 NPPs designed, built, operating

First real PRA analysis

Came to prominence after Three Mile Island in 1979

Limited number of plant specific PRAs

Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants

First Level III full scope PRA

Level III assessments now done all the time to obtain operating license

NRC paradigm now ‘Risk-Informed Decision Making’

Risk assessment as one input into design and operational changes

Deterministic and reductionistic

Highly dependent on detailed system analysis

Data driven and now big big data is a big big thing

Unless you have no operational data cohorts like for pyroprocessing or cybersecurity

Where is risk assessment used?

Literally everywhere

Reactor safety

Space shuttle

Superfund sites

Insurance and banking

Information technology

Cyber-physical systems

Gambling and counting cards

Finding an apartment [analytical hierarchy procedure]

Finding my house

Deciding what dessert to have

Risk assessment contains several complex elements

Probabalistic risk assessment – risks imposed by technologies

Models needed due to lack of data (assumptions)

Risk/benefit – are the risks acceptable

Involuntary v voluntary

Option generation – risk reduction

Cost/benefit & value/impact – evaluate options

Typically greatest good for less cost

How much will society pay to reduce risk

Risk assessment is people-centered

Public health risk analysis

Determination of toxic material required to cause effect

Determination of the amount of exposure to the toxin

Environmental risk

Location and strength of source

Dispersion

Uptake

Dose + effects + response = Health effects

Population demographic at risk

Most assessments focus on acute fatalities and cancer deaths

Somatic effects = manifested in exposed individuals

Genetic effects = manifested in exposed individuals progeny

Deterministic effects = Severity proportional to dose

Stochastic effects = Incident rate of exposure proportional to dose

Risk analysis involves both technical and institutional issues

What are the risks? (assessment) – technical

Are the risks acceptable? – institutional, societal context, regulations

Can the risks be reduced? – (options) both but more technical

Evaluation of the options (risk/benefit, PRA) – technical

But the decisions (management) based on the PRA are institutional

Because we’re engineers here, we have to be technical experts

Classifying risk

The event doesn’t care about society
But the consequences are societal

Severity classified by varying degrees

CATASTROPHIC (I)

Loss of ability to accomplish the mission or mission failure

Death or permanent total disability (accident risk)

Loss of major or mission-critical system or equipment

Major property (facility) damage

Severe environmental damage

Mission-critical security failure

Unacceptable collateral damage

CRITICAL (II)

Significantly (severely) degraded mission capability or unit readiness

Permanent partial disability, temporary total disability exceeding 3 months time (accident risk)

Extensive (major) damage to equipment or systems

Significant damage to property or the environment

Security failure

Significant collateral damage

MARGINAL (III)

Degraded mission capability or unit readiness

Minor damage to equipment or systems, property, or the environment

Lost day due to injury or illness not exceeding 3 months (accident risk)

Minor damage to property or the environment

NEGLIGIBLE (IV)

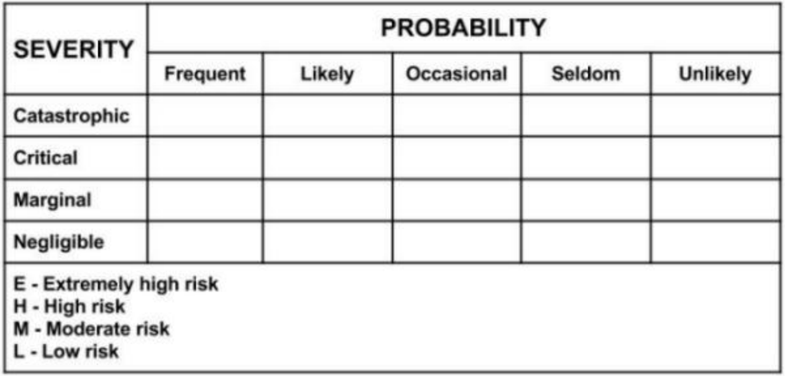
Little or no adverse impact on mission capability

First aid or minor medical treatment (accident risk)

Slight equipment or system damage, but fully functional and serviceable

Little or no property or environmental damage

Risk matrix



SEVERITY	PROBABILITY				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic					
Critical					
Marginal					
Negligible					
E - Extremely high risk H - High risk M - Moderate risk L - Low risk					

Severity	**Probability**				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic	E	E	H	H	M
Critical	E	E	H	M	L
Marginal	H	M	M	L	L
Negligible	M	L	L	L	L

E – Extreme Risk	M – Moderate Risk
H – High Risk	L – Low Risk

Risk management

Any engineering problem is inherently risk-based

(1) What are the risks imposed by human activities and natural phenomena on society and the environment?

(2) Are these risks acceptable? (regulations)

(3) What are there options for reducing these risks?

(4) On what basis should we choose among these options?

Risk management answers these questions

Process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs with mission benefits

Integrating risk management into mission planning, preparation, and execution

Making risk decisions at the appropriate level in the chain of command

Accepting no unnecessary risk

Risk-informed, performance based decision making as part of design process

Risk management is the process of identifying, controlling hazards to conserve combat resources

Identify hazards to people, property, mission

Past, present, future

Complexity and difficulty of the mission/task

Terrain and environment

Weather and visibility

Equipment on hand and status

Time available for preparation/execution

(Supervision, Experience, Training, Morale, Environment)

Hazard assessment

Assess hazards to determine risks

Defense in depth

Multiple barriers

Eliminate common failure modes (huge problem)

Safety margins to account for uncertainty

Develop controls

Implement controls

Supervise and evaluate

Risk assessment establishes situational awareness

Management also cost/benefit analysis

Leaders continuously assess the risk to the overall mission and to those involved in the task

Evaluate the effectiveness of controls

Provide lessons learned

Human factors

Risk assessment also involves human factors

In many cases a system being analyzed has very deterministic failures associated with it

Which is where we get PRA

In reality, system failures are never well identified and humans and the organizations we create change the failure rates of systems

And we have to live with a lot of uncertainty

Lifecycle assessment

Risk assessment should start early in life cycle and continue

Preliminary Hazards Analysis (PHA) early

Failure Modes & Effects Analysis (FMEA) and fault tree analysis for conceptual design phases

Probabilistic risk assessment and human reliability analysis for mature designs

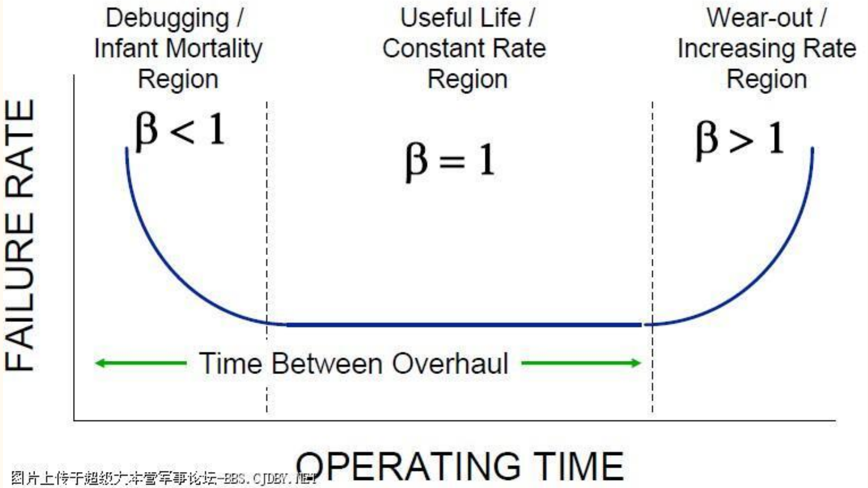
Continuing after system is real and is ongoing

Nuclear reactors, technical specifications, performance goals

Always after accidents

Weibull & Risk Analysis

A Weibull Distribution can describe each portion of the Bathtub curve


Debugging / Infant Mortality Region
Useful Life / Constant Rate Region
Wear-out / Increasing Rate Region
$\beta < 1$
$\beta = 1$
$\beta > 1$
Time Between Overhaul
FAILURE RATE
OPERATING TIME

A Weibull distribution can describe each part of the curve

$\beta < 1$

No operational experience or real data cohort

Would want to minimize time period with extensive testing and modeling

$\beta = 1$

Random failures

$\beta > 1$

So you want to know when you are heading in to here and make decisions about when to replace parts, equipment, etc.

$$Q(t) = 1 - e^{-(\frac{t}{\eta})^{\beta}}$$

Frequency is not intuitive

Monty Hall problem

You’re given the choice of three doors – Behind one door is a car; behind the others, goats

You pick a door; 1, and the host, who knows what’s behind the doors, opens another door; 3, which has a goat

Do you want to switch and pick door 2? Or stay with 1?

Is it to your advantage to switch your choice? What is the probability?

When assessing frequency, intuition can be problematic

No spin Russian roulette

Important to fully characterize risk and understand the real problem

What could go wrong?

You have to shoot the gun

How likely is it to happen?

These are ‘dependent events’ not like the NCAA tourney

Because we are dependent on the chamber state AND player state

What are the consequences?

Gun goes off, you die; slow singing, flower bringing

Management options

Where should you sit to maximize you chance at life?

Risk is the expected value of an undesirable event

$$E[X] \equiv \int x f(x) dx \tag{1}$$

$$E[X] \equiv \sum_i x_i f(x_i) \tag{2}$$

This is the quantitative part of the risk analysis

Not always so easy due to uncertainties

E[DICE] = ?

Uncertainty

Uncertainties come in different flavors but are essential in risk

There are things we know we know

Then there’s things we know that we do not know

But there’s still things that we don’t know we don’t know

Aleatory uncertainty is statistical

Random variations and chance outcomes in the physical world, natural randomness in a process

If a parameter sometimes has one value and sometimes has another values

Epistemic uncertainty is systematic

Lack of knowledge about the physical world, scientific uncertainty in the model of the process

If a parameter always has either one value or another, but we are not sure which

Aleatory or epistemic? Does it matter?

Ethics

There is an ethical theory basis for risk

Based on universal rules and principles by Descartes (1596–1650)

Rights ethics by John Locke (not the guy from the Island) (1632–1704)

Duties ethics by Immanuel Kant (1724–1804)

Utilitarianism by Jeremy Bentham and John Stuart Mill (1748–1832),(1806–1873)

‘Greatest good for greatest number of people’ (Red Wedding)

PRA (WASH1400) comes from this – ‘economic determinism’; cost/benefit

Societal context

Society determines acceptable risks

As Low As Reasonably Achievable (ALARA) (1000/person/rem)

Versus precautionary principle

Contaminated [superfund] sites and cancer risks

Safety goals for reactors, 0.1% of background cancer risk

So it is the regulations that determine the acceptable levels

How is that codified?

NRC has qualitative safety goals

Individuals bear no significant additional risk to life and health

Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks due to electric generation by competing technologies and should not be a significant addition to other societal risks

There’s more, but you get the idea

What are some examples of utilitarianism in real life?

Insurance – How much am I willing to spend each year to insure my house, car, life and for what amount?

Energy – What risks am I willing to take for the benefit of 1000 MWe among a coal, natural gas, oil or nuclear power plant?

These are not strictly technically-based? Or not?

Cost/benefit is the typical risk reduction mode

Rational decision maker will choose the option that maximizes utility

Or largest benefit/cost ratio

Multiattribute utilty theory uses functions to express risk aversion

Use of decision trees

Relies on expert judgement

Game theory for two party decision making

Brief case study

Challenger

The Challenger disaster occurred in 1986

The Space Shuttle management prior to the Challenger disaster felt that a failure would occur about 1 every 100,000 flight

Engineers calculated the failure rates between 1 in 100 and 1 in 556 missions pre-Challenger

In actuality the failure rates were 1 in 137 on launch and 1 in 137 on re-entry or 2 in 137 flights

Human decision process gravely impacted the Challenger mission

How frequency is determined affects management options

Ford Pinto

The Ford Pinto case is a classic study of risk/benefit and ethics

During design and production, crash tests revealed a serious defect in the gas tank

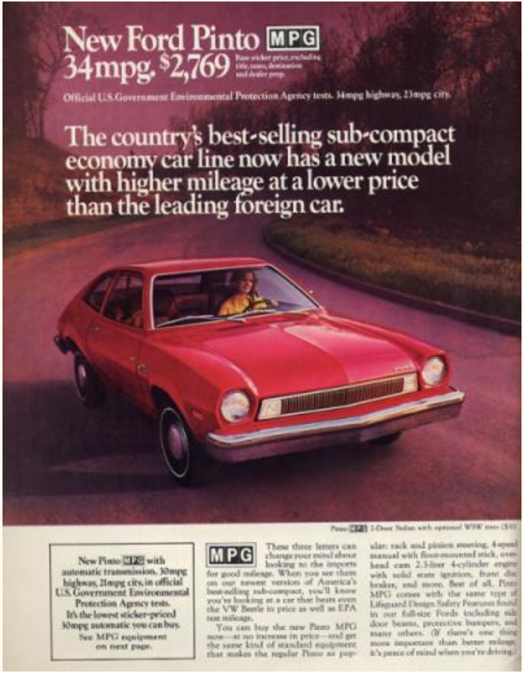
In crashes over *25 miles per hour*, the gas tank always ruptured

To correct it would have required changing and strengthening the design

So they didn’t

What other more contemporary examples are there?

NO ANIMALS OR GLASS CONTAINERS
Pinto



New Ford Pinto MPG
34mpg. $2,769 Base sticker price, excluding title, taxes, destination and dealer prep.

Official U.S. Government Environmental Protection Agency tests. 34mpg highway, 23mpg city.

The country's best-selling sub-compact economy car line now has a new model with higher mileage at a lower price than the leading foreign car.

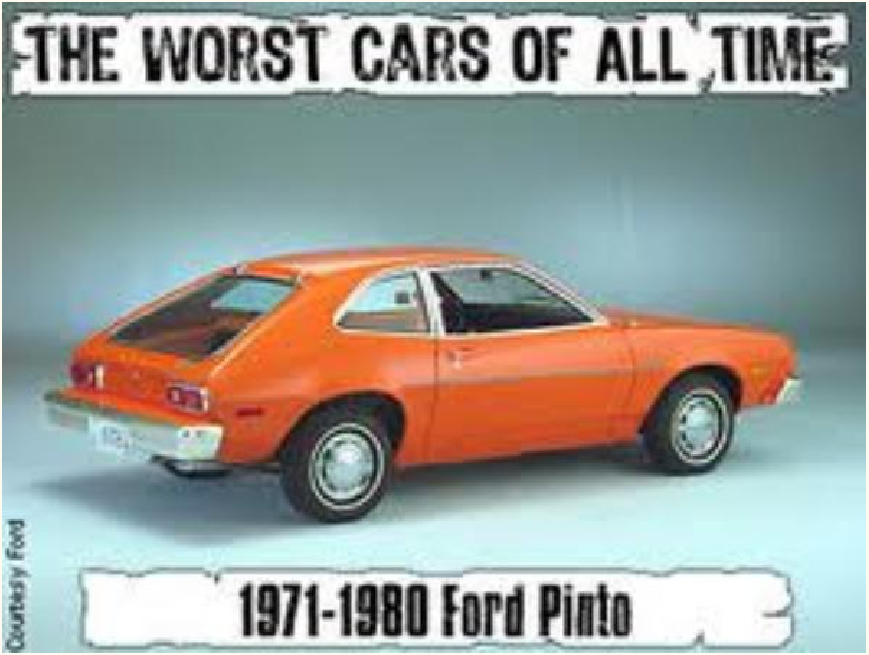
Pinto MPG 2-Door Sedan with optional WSW tires ($33)

New Pinto MPG with automatic transmission. 30mpg highway, 21mpg city, in official U.S. Government Environmental Protection Agency tests.
It's the lowest sticker-priced 30mpg automatic you can buy.
See MPG equipment on next page.

MPG These three letters can change your mind about looking to the imports for good mileage. When you see them on our newest version of America's best-selling sub-compact, you'll know you're looking at a car that beats even the VW Beetle in price as well as EPA test mileage.

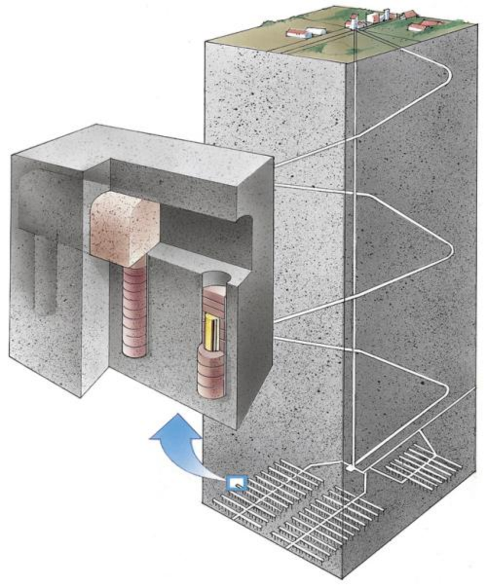
You can buy the new Pinto MPG now—at no increase in price—and get the same kind of standard equipment that makes the regular Pinto so popular: rack and pinion steering, 4-speed manual with floor-mounted stick, overhead cam 2.3-liter 4-cylinder engine with solid state ignition, front disc brakes, and more. Best of all, Pinto MPG comes with the same type of Lifeguard Design Safety Features found in our full-size Fords including side door beams, protective bumpers, and many others. (If there's one thing more important than better mileage, it's peace of mind when you're driving.)

KEEP OFF MY REAR
I'M EXPLOSIVE!
MICHIGAN
DVG010


THE WORST CARS OF ALL TIME
1971-1980 Ford Pinto
Courtesy Ford

Repository

How does a repository distribute risk?



Single location

Greatest good for whom?

Dreamliner

787
BOEING
DREAMLINER

Drawbacks

What are some drawbacks of utilitarianism?

Only the greatest good, as a singular body and not distributed among people

Difficulty in quantifying the greatest good

Plus there are always lots of uncertainties to trust one number

Anthropocentric

Utilitarianism judges by consequences rather than actions

Low probability–high consequence events carry as much weight as high probability–low consequence events

Emerging technologies exhibit nonlinearity [emergent quality]

Time scales

Yet utilitarianism is how we do risk in everything

Alternatives

What else can be used?

Justice ethics by Rawls (1971)

This is something else covered in detail in an ethics course

Each person is to have an equal right to equal basic liberties

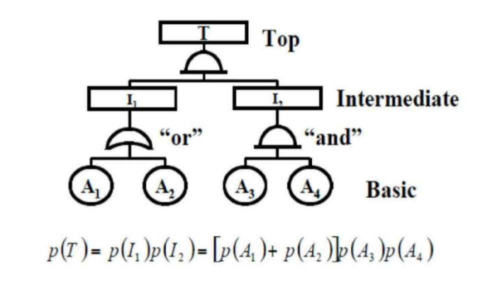
Social and economic inequalities are to the greatest benefit of the least–advantaged

Treating everyone equally is a challenge

Evironmental justice

Fault trees

Fault tree is a top down, deductive failure analysis tool



$$p(T) = p(I_1)p(I_2) = [p(A_1) + p(A_2)]p(A_3)p(A_4)$$

Logic diagram for the system

Top is ‘big system event’ like Loss of Coolant Accident (LOCA)

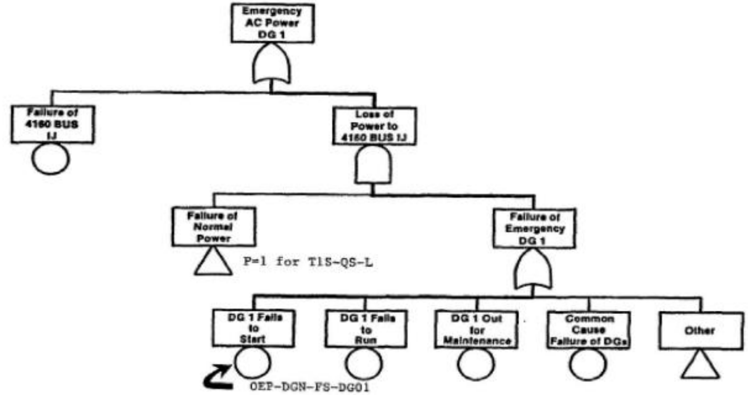
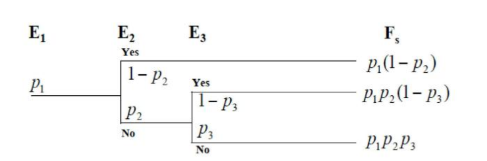


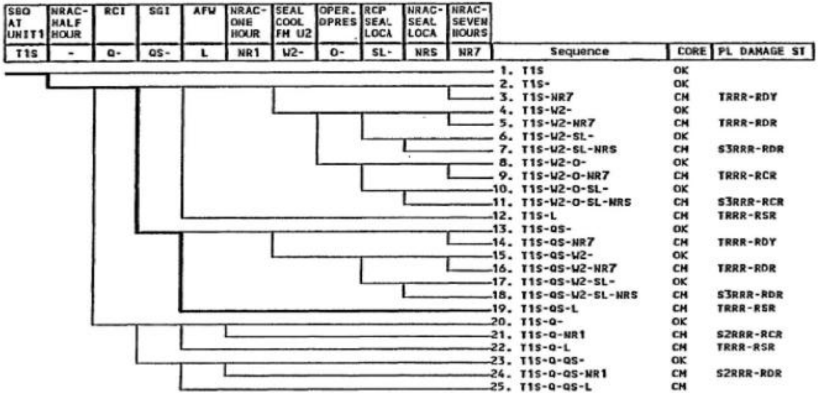
Figure B.2 Reduced fault tree for DG 1 at Surry Unit 1. (This figure is a greatly simplified version of the fault tree given in Appendix B.2 of Ref. B.3. P = 1 indicates that the failure probability is 1.0.)

Event trees



Consequence is associated with the final state

Dose/response models



SBO AT UNIT1	NRAC-HALF HOUR	RCI	SGI	AFW	NRAC-ONE HOUR	SEAL COOL FM U2	OPER. DPRES	RCP SEAL LOCA	NRAC-SEAL LOCA	NRAC-SEVEN HOURS
T1S	-	Q-	QS-	L	NR1	W2-	O-	SL-	NRS	NR7

Sequence	CORE	PL DAMAGE ST
1. T1S	OK	
2. T1S-	OK	
3. T1S-NR7	CM	TRRR-RDY
4. T1S-W2-	OK	
5. T1S-W2-NR7	CM	TRRR-RDR
6. T1S-W2-SL-	OK	
7. T1S-W2-SL-NRS	CM	S3RRR-RDR
8. T1S-W2-O-	OK	
9. T1S-W2-O-NR7	CM	TRRR-RCR
10. T1S-W2-O-SL-	OK	
11. T1S-W2-O-SL-NRS	CM	S3RRR-RCR
12. T1S-L	CM	TRRR-RSR
13. T1S-QS-	OK	
14. T1S-QS-NR7	CM	TRRR-RDY
15. T1S-QS-W2-	OK	
16. T1S-QS-W2-NR7	CM	TRRR-RDR
17. T1S-QS-W2-SL-	OK	
18. T1S-QS-W2-SL-NRS	CM	S3RRR-RDR
19. T1S-QS-L	CM	TRRR-RSR
20. T1S-Q-	OK	
21. T1S-Q-NR1	CM	S2RRR-RCR
22. T1S-Q-L	CM	TRRR-RSR
23. T1S-Q-QS-	OK	
24. T1S-Q-QS-NR1	CM	S2RRR-RDR
25. T1S-Q-QS-L	CM	

Figure B.1 Event tree for T1S-SBO at Surry Unit 1. (This figure is adapted from Section 4.4 of Ref. B.3. No PDS assignment is indicated for sequence 25 because the sequence frequency fell below the cutoff value.)

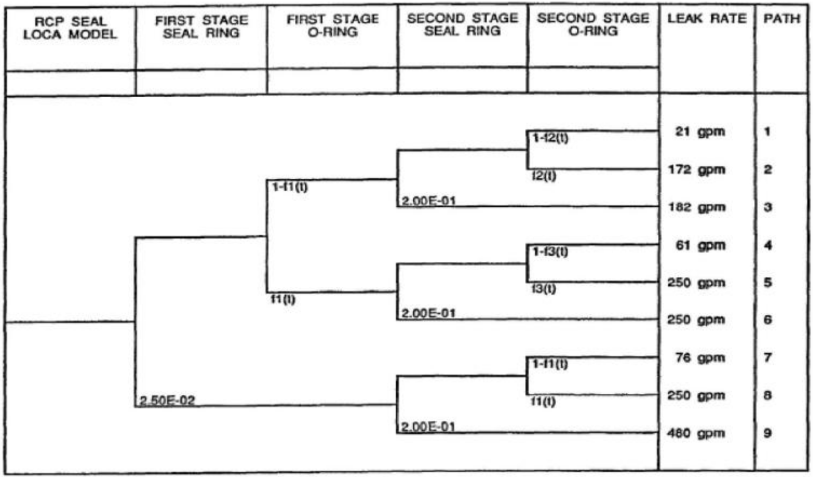


Figure B.5 Event tree used by all three experts in determining the probabilities of different leak rates for a single reactor coolant pump. The branch fractions shown are for Expert A. (This figure is adapted from Section C.4 of Ref. B.8.)

Risk perception

Risk/benefit is just a tool, the result alone is not the decision, this requires societal context and ethics

Inherently, there is the issue of risk perception by different stakeholders

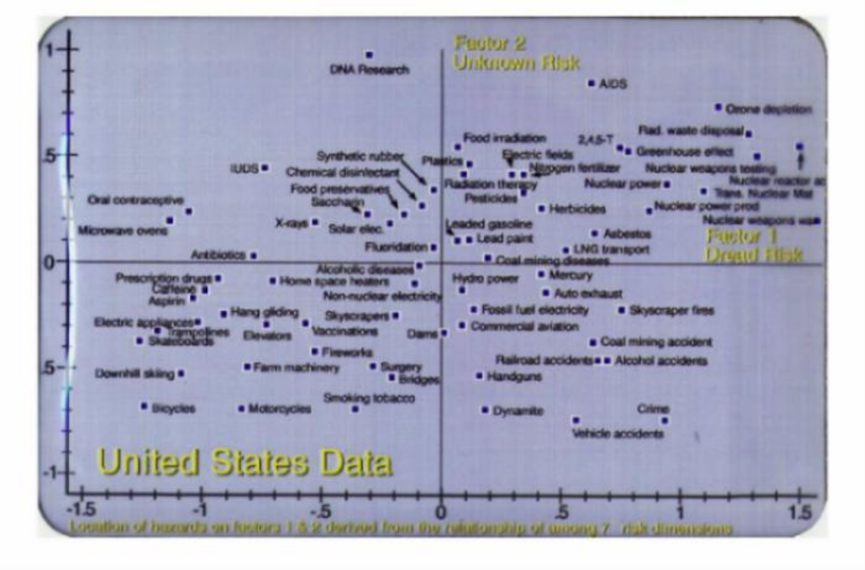
Particularly with anything nuclear related

Historical inertia

Social scientists say quantification is insufficient to address risk

Risk–informed approaches

Risk perception is a challenge to overcome



Seminal literature

On the quantitative definition of risk

The Hyatt Horror

The Pinto Case

Reactor accident scenarios – LOCA

Media