RISK ANALYSIS AND MODELING

Mohammad Modarres
Minta Martin Professor of Engineering
Director, Reliability Engineering Program
Department of Mechanical Engineering
University of Maryland, College Park, MD 20742

Presented at the
Transportation Research Board's 92d Annual Meeting
January 13, 2012, Workshop

DEFINITION OF RISK

- Risk is a measure of potential of losses occurred due to natural or human activities.
  - Losses are adverse consequences in form of loss of human life, adverse health effects, loss of property, and damage to natural environment.
- Risk analysis is the process of characterizing, managing and informing others about existence, nature, magnitude, prevalence, contributing factors, and uncertainties of the potential losses.
  - the loss may be external to the system or internally caused by the system to one or more recipients (e.g., human, organization, economic assets, and environment).

CATEGORIES OF RISK ANALYSIS

Health risk analysis estimating potential diseases and losses of life affecting humans, animals and plants;

Safety risk analysis involves estimating potential harms caused by accidents occurring due to natural events (climatic conditions, earthquakes, brush fires, etc.) or human-made products, technologies and systems (i.e., aircraft crashes, chemical plant explosions, nuclear plant accidents, technology obsolescence or failure);

Security risk analysis involves estimating access and harm caused due to war, terrorism, riot, crime (vandalism, theft, etc.) and misappropriation of information (national security information, intellectual property, etc.);

Financial risk analysis involves estimating potential individual, institutional and societal monetary losses such as currency fluctuations, interest rates, share market, project losses, bankruptcy, market loss, misappropriation of funds, and property damage;

Environmental risk analysis involves estimating losses due to noise, contamination, and pollution in ecosystem (water, land, air and atmosphere) and in space (space debris);

RISK ANALYSIS METHODS IN ENGINEERING

Risk analysis can be used in all stages of design, development, construction, and operation of engineering systems:

- **Conceptual Design**
  - Compare alternative design options
- **Design**
  - Provide barriers to prevent, minimize or eliminate harm
  - Minimize life-cycle cost
  - Apportion risk limits and performance goals.
- **Development**
  - Identify systems or subsystems that contribute most to safety and risk
  - Test safety and risk significant elements of the design
  - Quality assurance
  - Warranty development

RISK ANALYSIS METHODS IN ENGINEERING (Cont.)

- **Regulation**
  - Regulate consistent with the significance of the elements of the system that contribute most to risk
  - Set monitoring and performance criteria
  - Perform inspections
- **Operation**
  - Optimize cost of maintenance and other operational activities
  - Define surveillance requirements and schedules
  - Replacement policies and decisions
  - Aging estimation and management
  - Developing security measures
- **Decommissioning**
  - Assess safety of possible decommissioning activities
  - Select most appropriate disposal method
  - Assess long-term liability issue

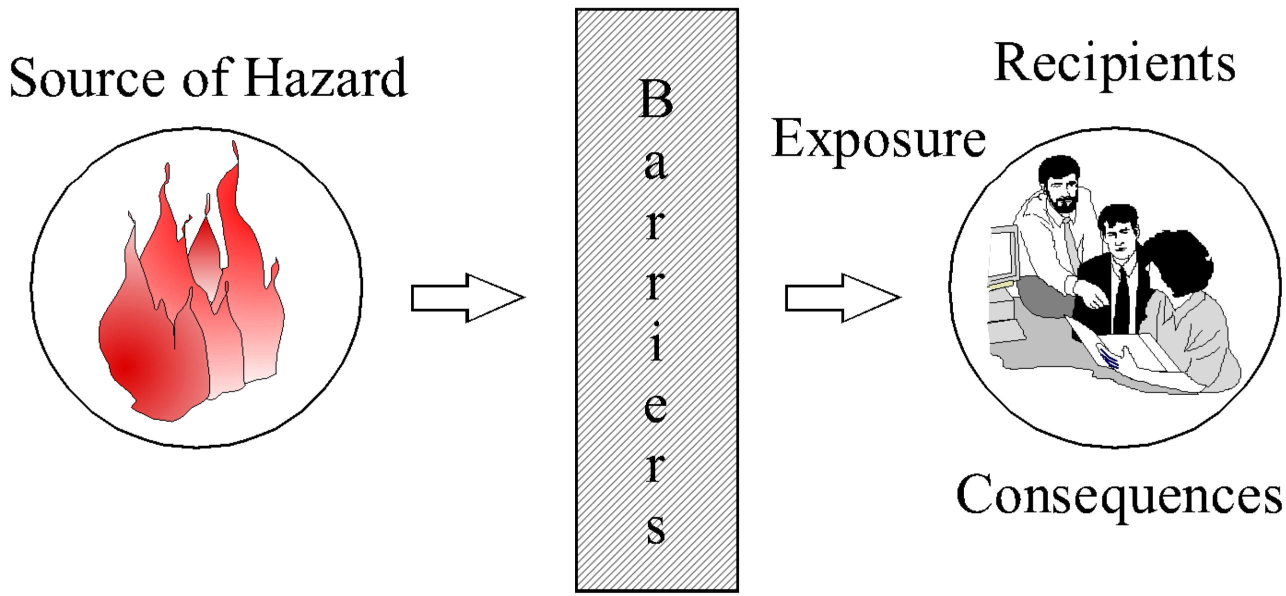
KEY ELEMENTS OF RISK ASSESSMENT

- Identification of Hazards
- Identification of Barriers (Human, Structures, Components, Systems, Natural Barriers, etc.)
- Assessment of the Likelihood of Loss of Barriers
- Estimation of the Consequences of Exposure of Hazards
- Evaluation of the Risk (Combination of the Likelihood and Consequence)

1. IDENTIFICATION OF HAZARDS

- Chemical (e.g., toxins, corrosive agents, smoke)
- Biological (e.g., viruses, microbial agents, bio-contaminants)
- Thermal (e.g., explosions, fire)
- Mechanical (e.g., impact from a moving object, explosions)
- Electrical (e.g., electromagnetic fields, electric shock)
- Ionizing radiation (e.g., x-rays, gamma rays)
- Nonionizing radiation (e.g., microwave radiation, cosmic rays)
- Information (e.g., propaganda, computer virus)

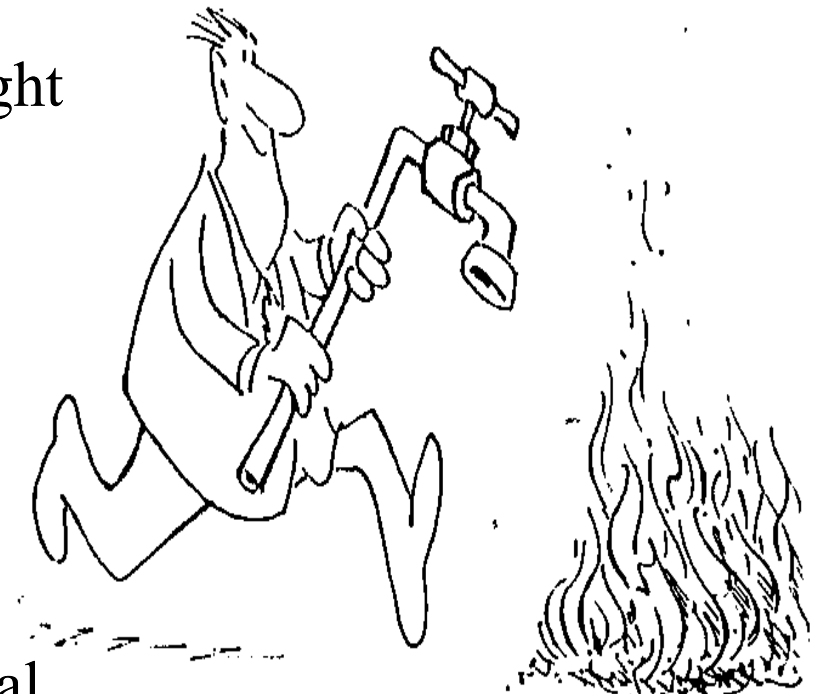
HAZARD IS *SOURCE OF DANGER*



- Contain
- Mitigate
- Control
- Protect

HUMAN ELEMENT AS A CRITICAL BARRIER

- **Nuclear** (Maintenance Error, Control Room Crew Error)
- **Aviation** (Maintenance Error, Flight Crew Error, Air Traffic Controller Error)
- **Chemical and Process** (Maintenance Errors)
- **Land and Sea Transportation** (Maintenance Structures and Operator Errors)
- **Healthcare Industries** (Procedural Error, Operator Error)
- **Telecommunication** (Procedural Errors)



2. IDENTIFICATION OF CHALLENGES TO BARRIERS

- Barrier strength or endurance degrades because of:
  - Reduced thickness (due to deformation, erosion, corrosion, ware, etc.),
  - Changes in material properties (e.g., fracture toughness, yield strength).
  - Human performance

- Stress or damage on the barrier increases by:
  - Internal agents such as forces or pressure,
  - Penetration or distortion by external objects or forces.

3. IDENTIFICATION OF CHALLENGERS TO BARRIERS

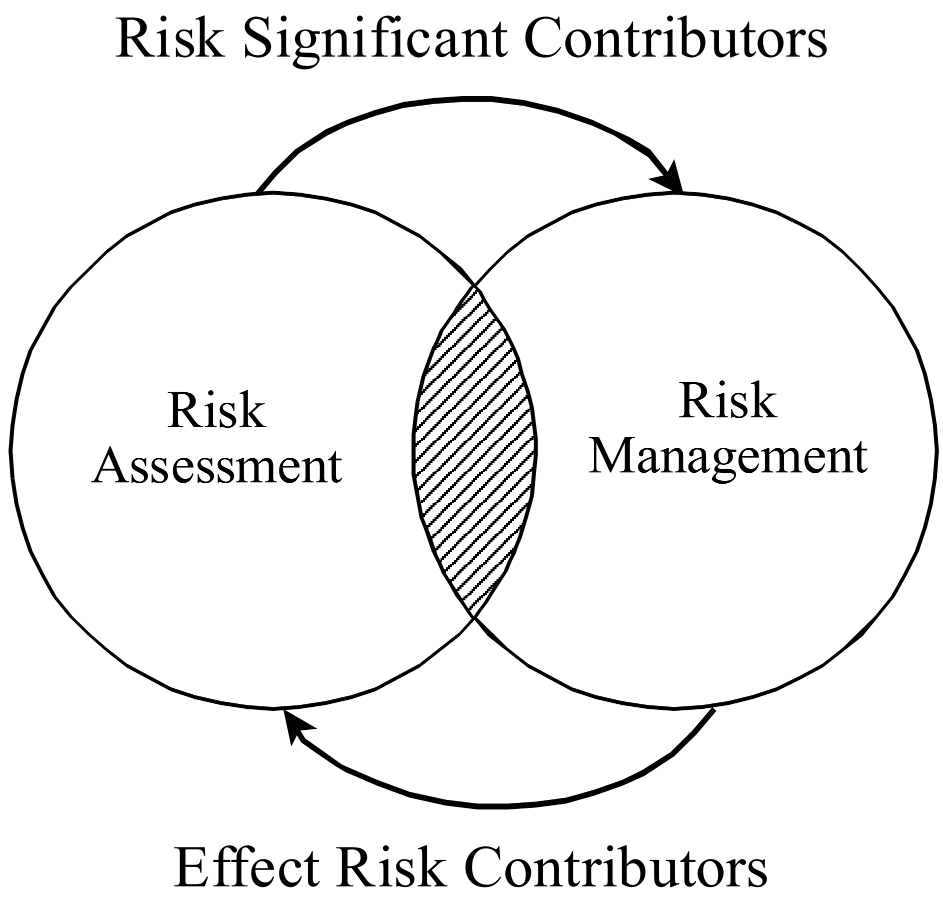
Challenges cause system degradation leading to one or more of the following conditions:

- Malfunction of process equipment (e.g., the emergency cooling system in a nuclear power plant)
- Problems with human-machine interface
- Poor design and maintenance
- Adverse natural phenomena
- Adverse human-made environments.

4. Estimation of Frequency or Probability of a Hazard Exposure

5. Consequences Evaluation

RISK ASSESSMENT-RISK MANAGEMENT



ENGINEERING RISK ASSESSMENT

Risk assessment answers the following questions (Kaplan and Garrick):

1. What can go wrong? (that could lead to a hazard exposure outcome)
2. How likely this can happen?
3. If it happens, what consequences (losses or injures) are expected.

The triplet R can express risk as $R_i = \langle S_i, P_i, C_i \rangle$

where

S_i is the scenario i (events leading to exposure of hazard)

P_i is the frequency or likelihood of S_i

C_i is the consequence of S_i (outcome)

ENGINEERING RISK ASSESSMENT (Cont.)

Answer to the three questions leads to to the table below

Scenario	Likelihood	Damage
S_1 S_2 S_3 . . . S_N	l_1 l_2 l_3 . . . l_N	X_1 X_2 X_3 . . . X_N

$$R = \text{RISK} = \{\langle S_1, l_1, X_1 \rangle\}$$

Risk "is" a set of triplets

ENGINEERING RISK ASSESSMENT (cont)

Mathematical representation of risk

$$\text{Risk}\left(\frac{\text{Consequence}}{\text{Unit of time or space}}\right) =$$

$$\text{Frequency}\left(\frac{\text{Event}}{\text{Unit of time or space}}\right) \times \text{Magnitude}\left(\frac{\text{Consequence}}{\text{Event}}\right)$$

One simple widely used model of risk value is ***linear expectation*** of the magnitude of outcome method:

$$R = \sum_i f_i \, c_i$$

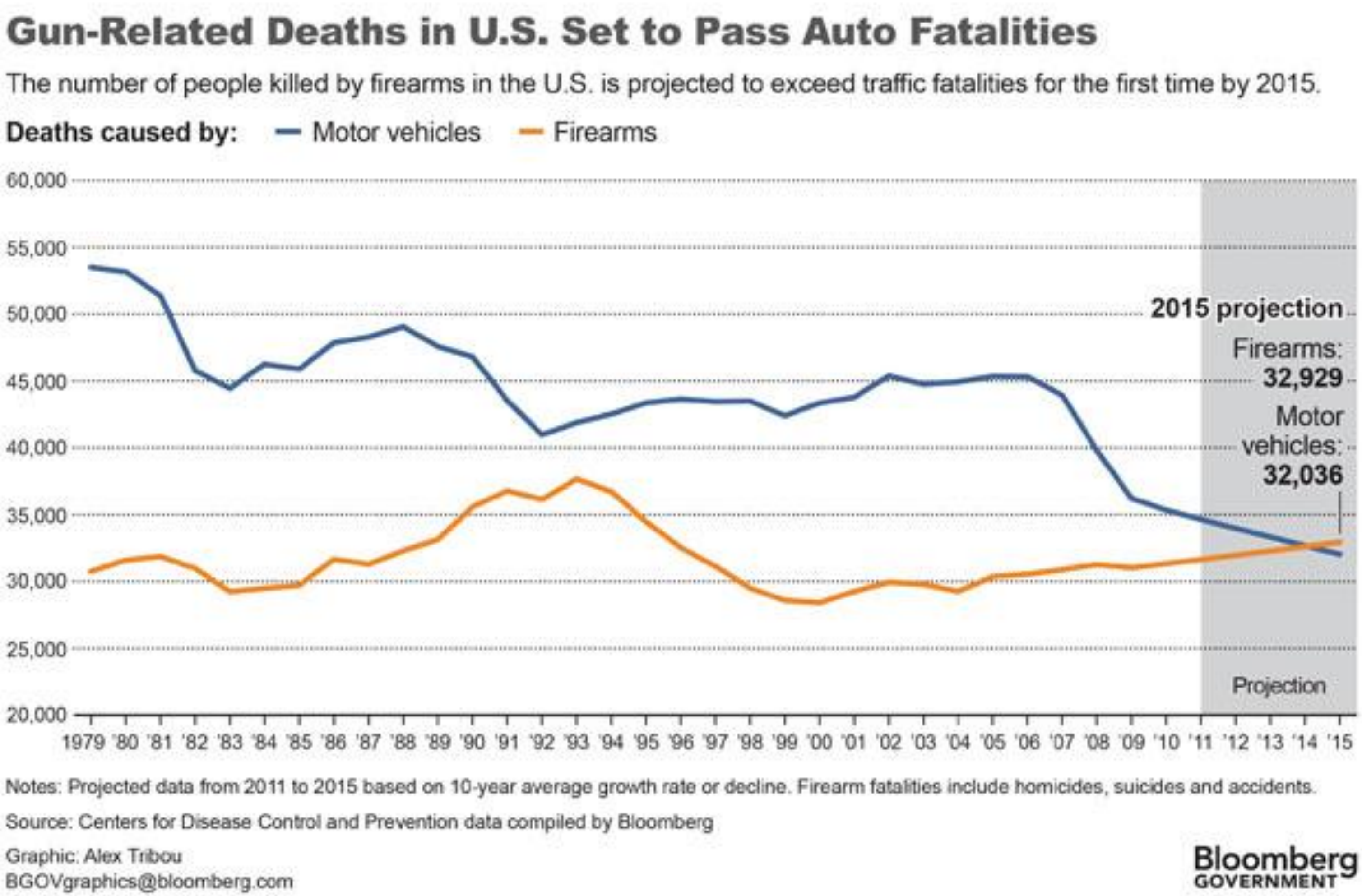
EXAMPLE: ENGINEERING RISK ASSESSMENT

- U.S. population exposed to automobile accidents is 250 million.
- According to the U.S. DOT, in 2003, there were 6.3 million automobile accidents in which
  - 1 in 3 resulted in injuries.
  - 1 in 165 resulting in death.
- Assume
  - Average loss of $450,000 per death
  - $25,000 of property damage per accidents involving fatality
  - $15,000 of cost per injury
  - Property loss of $10,000 per accident involving injury
  - Property loss of $3,000 for all other accidents
- Monetary risk (expected losses) of automobile accidents per driver in the United States?

EXAMPLE : ENGINEERING RISK ASSESSMENT (Cont.)

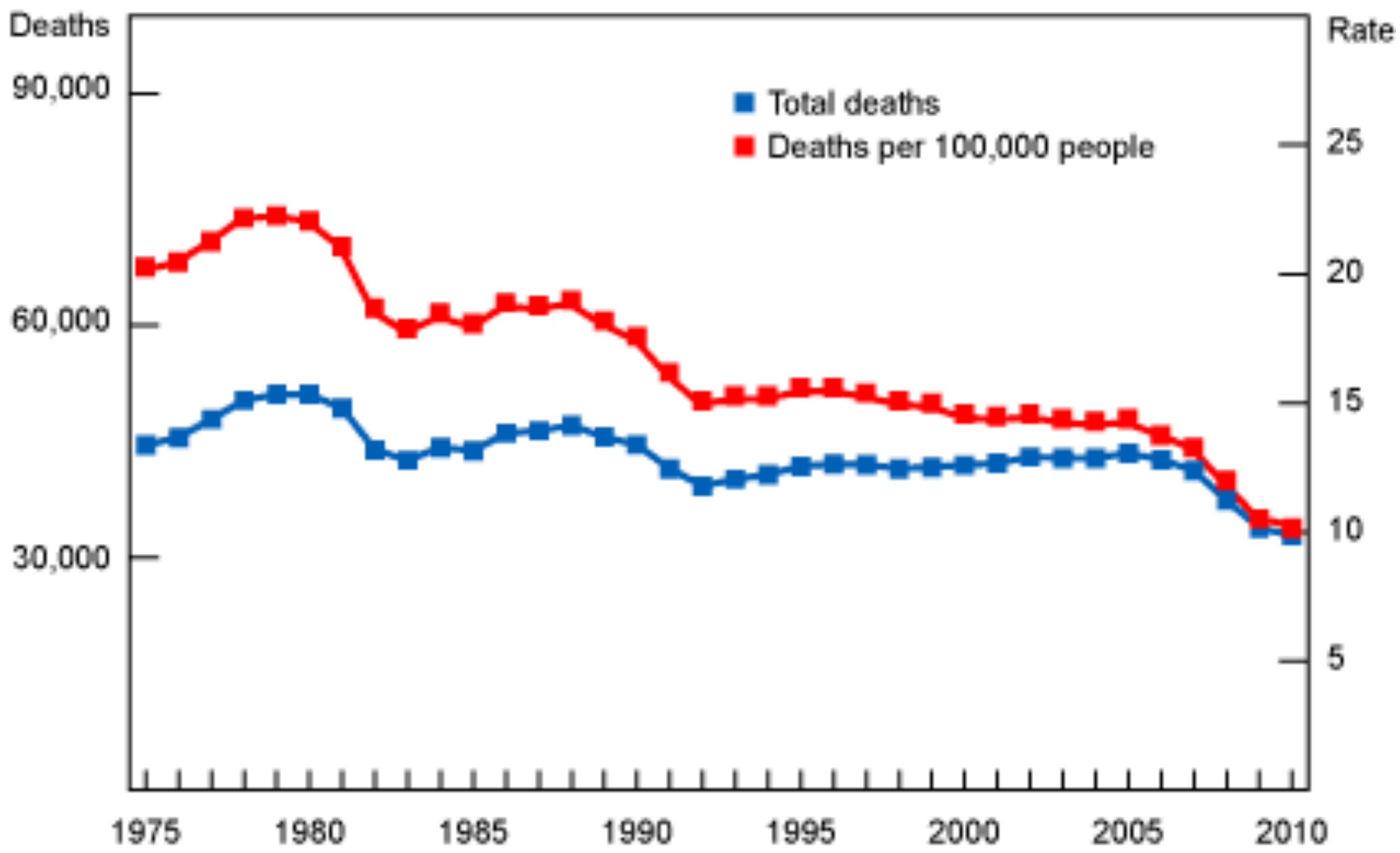
Risk Contributor	Fatality	Injury	Other	Total
Probability per Person per Accident	6.3×10^6 / (250×10^6) = 0.025	0.025	0.025	
Probability of events given Accident	1/165	1/3	(109)/(165)	
Probability of consequence per person	$1/165 \times 0.025$ $= 1.53\times10^{-4}$	8.4×10^{-3}	1.66×10^{2}	
Magnitude of Consequence ($ at Risk)	$450,000 + 25,000	$15,000 + $10,000	$3000	
Risk (expected loss)	$72.54	$210.00	$49.94	$332.49 per person-year

RISK FROM HISTORICAL DATA
TOTAL FATALITIES PER YEAR DUE TO GUN AUTOMOBILE ACCIDENTS



RISK FROM HISTORICAL DATA

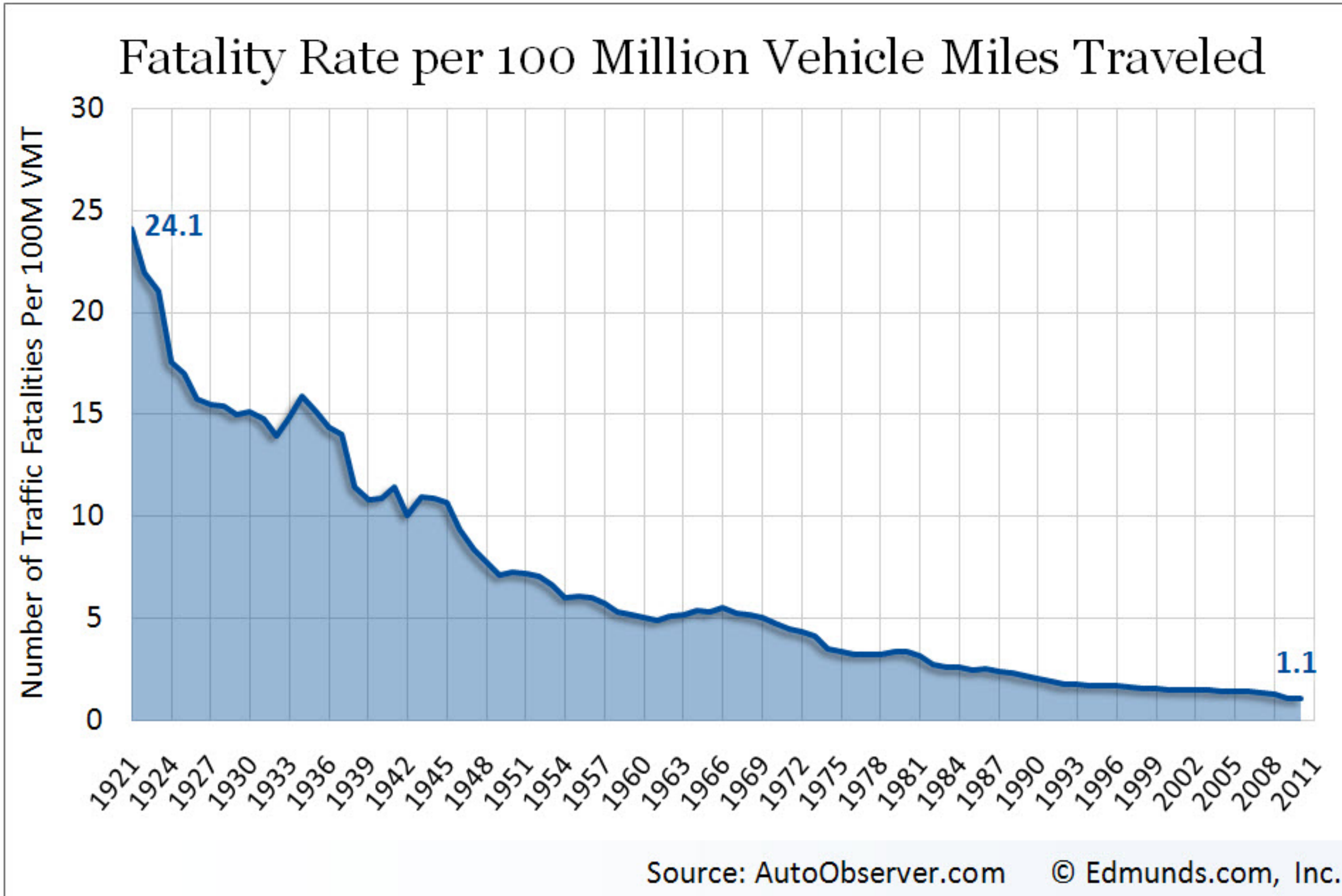
MOTOR VEHICLE FATALITY RATES PER 100,000 PEOPLE TRAVELLED, 1975-2010



Source: Insurance Institute for Highway Safety http://www.iihs.org/research/fatality.aspx

RISK FROM HISTORICAL DATA

MOTOR VEHICLE FATALITY RATES PER 100 MILLION VEHICLE MILES TRAVELED, 1921-2011



STEPS IN RISK ASSESSMENT

1. Hazard Identification

a) **Natural hazards**
- Flood
- Tornado
- Earthquake

b) **Man-made hazards**
- Chemical hazard (e.g., toxic chemicals released from a chemical processes)
- Thermal hazard (e.g., high-energy explosion from a chemical reactor)
- Mechanical hazard (e.g., kinetic or potential energy from a moving object)
- Electrical hazard (e.g., potential difference, electrical and magnetic fields, electrical shock)
- Ionizing radiation (e.g., radiation released from a nuclear plant)
- Nonionizing radiation (e.g., radiation from a microwave over, sun)
- Biological Hazards

STEPS IN RISK ASSESSMENT

2. Barrier Identification

a) **Physical (passive)**

- Walls (and natural physical barriers, mountain)
- Pipes
- Valves
- Casing
- Protective clothing
- Bunkers

b) **Physical (active)**

- Hazard removal actions
- Safety systems

STEPS IN RISK ASSESSMENT

3. Barrier Performance Assessment

- Accumulated damage to the barrier (e.g., crack growth due to fatigue) exceeds endurance (e.g., fracture toughness of the tank).
- Barrier strength (or endurance) degrades because of some underlying chemical or mechanical mechanisms:
  - reduced thickness (for example due to geometrical change caused by mechanisms such as fatigue, erosion, or corrosion)
  - change in material properties (e.g., reduction toughness due to radiation damage mechanism).
- Malfunction of process equipment (e.g., the emergency cooling system of a nuclear plant fails because its pumps did not start when needed)
- Human errors due to poor man-machine interface
- Human errors due to poor organizational communications
- Poor maintenance which does not restore the machinery properly
- Adverse natural phenomena
- Adverse operating environment.

STEPS IN RISK ASSESSMENT

4. Exposure Assessment

If the barriers to hazard exposure are compromised, then some or all hazards will be release and potentially expose recipients.

Assess the amount and characteristics (toxicity, concentration, temperature, etc.) resulted by the release of the hazards.

Order of magnitude type calculations is possible , or
Entirely relying on expert judgment.

In quantitative assessment,

Models of barrier failure developed and the amount of exposure estimated.

Characterization of uncertainties associated with the risk values.

STEPS IN RISK ASSESSMENT

5. **Risk Characterization**

- Correlations of hazard exposure to damage: e.g., dose-to-fatality such as 10,000 person-rem = 1 cancer
- Extrapolation issues

QUALITATIVE RISK ASSESSMENT

Frequency and Consequence are Measured Qualitatively Such as:

- Frequent-Likely to occur often during the life of an individual item or system or very often in operation of a large number of similar items.
- Probable-Likely to occur several times in the life of an individual item or system or often in operation of a large number of similar items.
- Occasional-Likely to occur sometime in the life of an individual item or system or will occur several times in the life of a large number of similar components.
- Remote-Unlikely, but possible to occur sometime in the life of an individual item or system, or can reasonably be expected to occur in the life of a large number of similar components.
- Improbable-Very unlikely to occur in the life of an individual item or system that it may be assumed not to be experienced, or it may be possible, but unlikely, to occur in the life of a large number of similar components.
- Incredible-Considered as an 'Act of God' or Physical events that are not expected.

QUALITATIVE RISK ASSESSMENT MATRIX

Risk is represented by a risk matrix such as the one below:

Frequency of Occurrence	**Indicative Frequency (per year)**	**Severity of Consequence**			
		Catastrophic	**Critical**	**Marginal**	**Negligible**
Frequent	> 1	H	H	H	I
Probable	$1\text{-}10^{-1}$	H	H	I	L
Occasional	$10^{-1}\text{-}10^{-2}$	H	H	L	L
Remote	$10^{-2}\text{-}10^{-4}$	H	H	L	L
Improbable	$10^{-4}\text{-}10^{-6}$	H	I	L	T
Incredible	$< 10^{-6}$	I	I	T	T

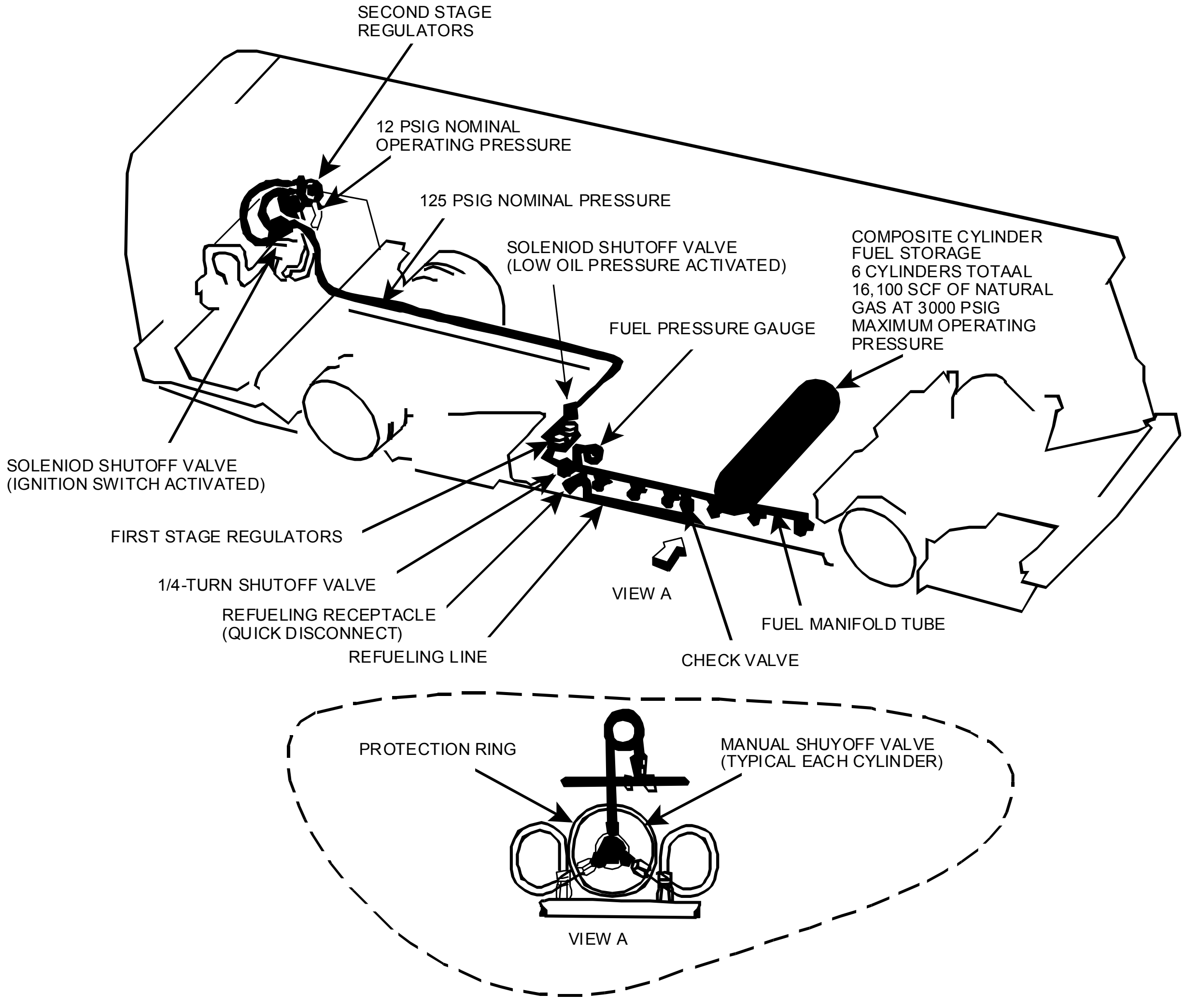
Note: The category definitions and values used in this matrix are illustrative only.
H = High risk
I = Intermediate risk
L = Low risk
T = Trivial risk

QUALITATIVE RISK ASSESSMENT (cont)

For this example the severity of the consequence categories are defined as:

- Catastrophic-involving many deaths, loss of system or plant, such that significant loss of production, significant public interest regulatory intervention occurs or reasonably could occur
- Critical- involving a few severe injuries, major system damage or other event which causes some loss of production, affects more than one department, or could have resulted in catastrophic consequences under different circumstances.
- Marginal-minor injury, minor system damage, or other event generally confined to one department.
- Negligible-less than the above.

EXAMPLE: QUALITATIVE RISK ASSESSMENT



EXAMPLE: QUALITATIVE RISK ASSESSMENT

Solution:

Step 1 Hazards

The hazard is the natural gas (primarily methane gas) fire and explosions leading to passenger and non-passenger fatalities.

Step 2 Barriers

Barriers are CNG storage tanks, pressure control systems, operators, warning and gas detection devices, and preventive maintenance activities.

EXAMPLE: QUALITATIVE RISK ASSESSMENT (cont)

Step 3 Barrier Performance

Several possible failures of barriers leadings to fire are possible. Barriers performance in critical risk scenarios:

- CNG tank or control system catastrophic failures (internally caused failures) leading to instantaneous release of CNG in the presence of an ignition source.
- CNG tank or control system degraded failures (e.g., internally caused leak) resulting in gradual release of CNG in the presence of an ignition source.
- CNG tank, control system, or human errors leading to release of CNG and ignition due to Electrostatic discharge sparks.
- Accidental impact of CNG tank and other hardware with external bodies (e.g., due to collisions with other vehicles) resulting in gas release in the presence of an ignition source.
- Operator/Driver error resulting in the release of CNG in the presence of an ignition source.

EXAMPLE: QUALITATIVE RISK ASSESSMENT (cont)

Step 4 Exposure

Failures described can lead to one of the four possible fire characteristics

CNG release mode	Ignition mode	Expected consequence
Instantaneous	Immediate	Fireball
	Delayed	Vapor cloud explosion or flash fire
Gradual	Immediate	Jet flame
	Delayed	Vapor cloud explosion or flash fire

SEVERITY DESCRIPTION FROM EXPOSURE OF THE FIRE

Severity Category	Severity Category Description
Catastrophic	CNG release involving catastrophic fire or explosion.
Critical	Unconfined CNG release with critical fire or explosive potential.
Marginal	Small CNG release with marginal ignition potential or fire effects.
Minor	Failure with minor fire potential and only loss of system operation.

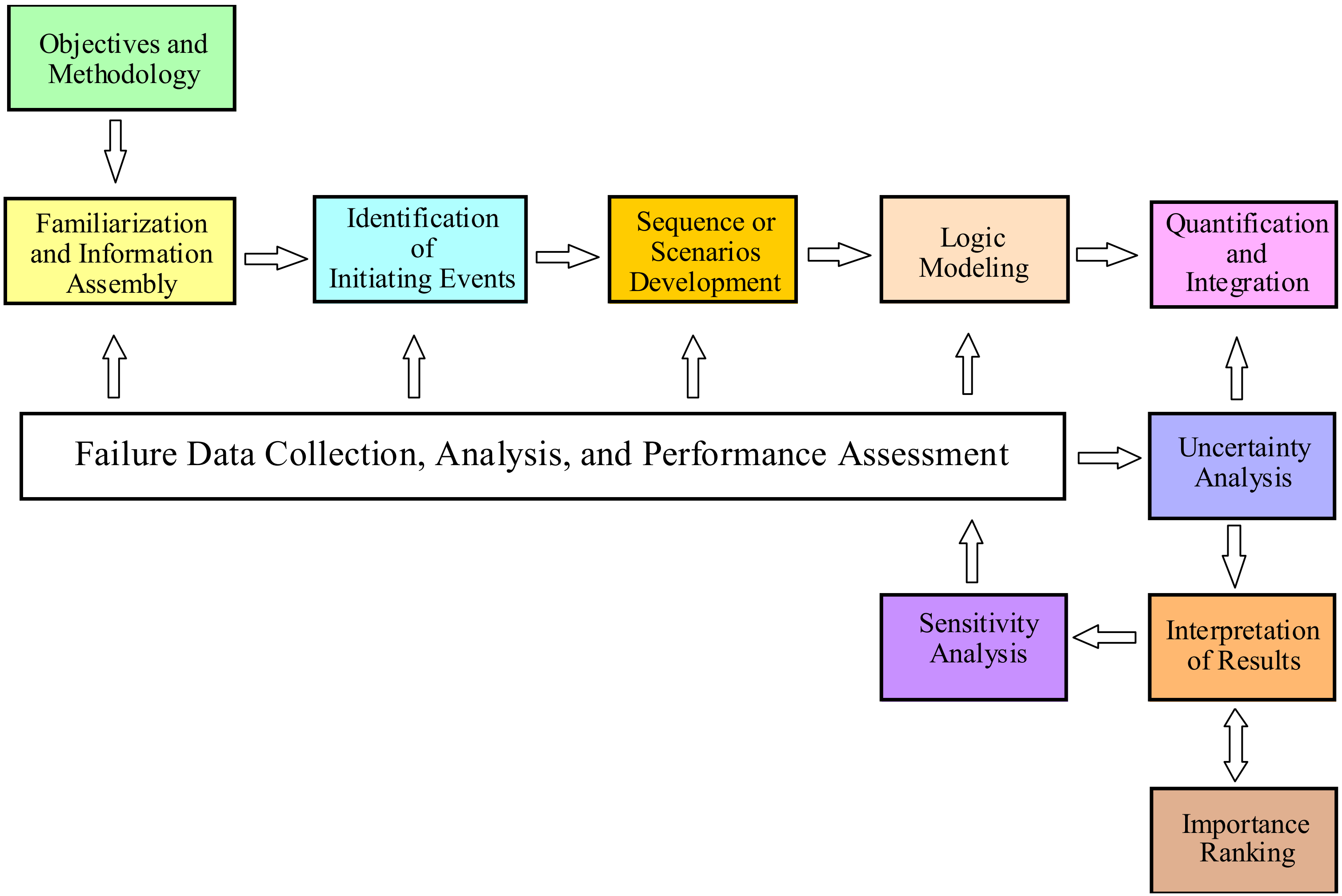
RELATIVE FREQUENCY CATEGORIES FOR FIRE SCENARIOS

Frequency Category	Frequency Category Description
A - Frequent	Likely to occur within 1 year or less.
B - Probable	Likely to occur within 10 years or less.
C - Unlikely	Probable within the expected life of 20 years for a bus or station.
D - Remote	Possible but not likely during the expected life of 20 years.

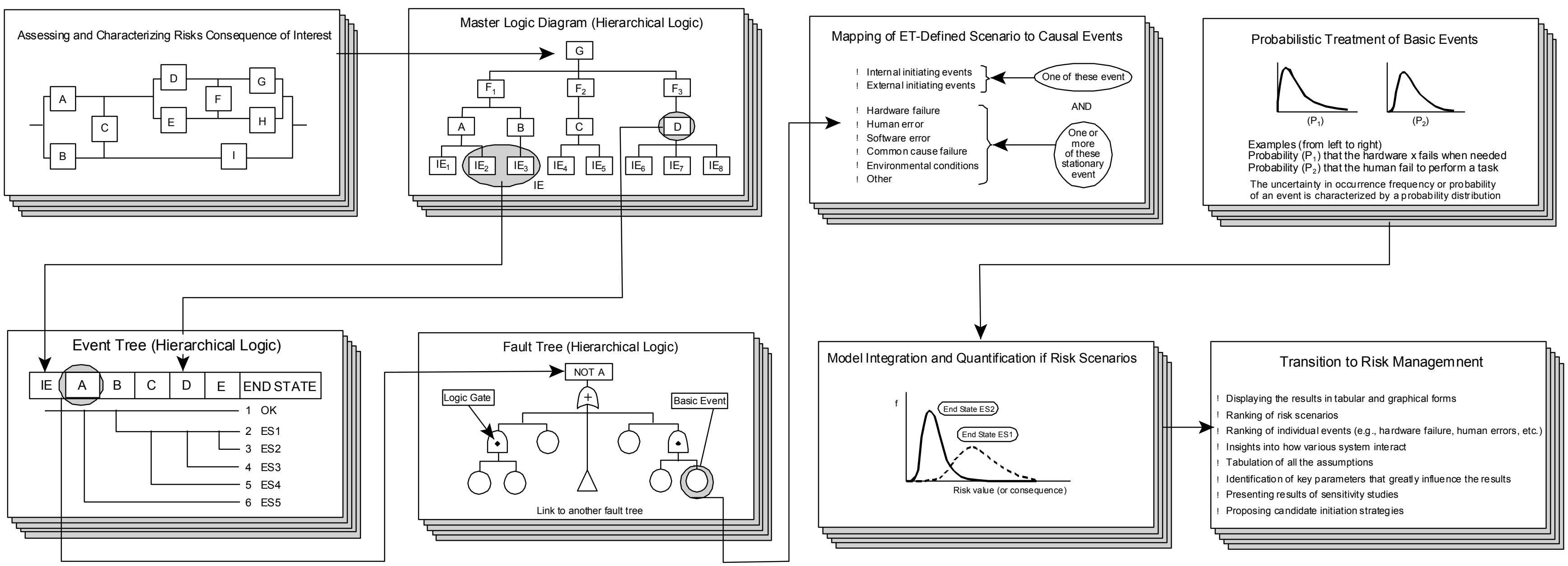
RISK MATRIX SHOWING THE NUMBER OF SCENARIOS FALLING INTO THE VARIOUS RISK CATEGORIES

	Catastrophic	Critical	Marginal	Minor
Likely	0	0	0	4
Probable	1	8	6	15
Unlikely	3	7	12	19
Remote	4	3	2	3

COMPONENTS OF THE OVERALL PRA PROCESS



GRAPHICAL DEPICTION OF THE RELATIONSHIP BETWEEN THE PRA STEPS



EXAMPLE: QUANTITATIVE RISK ASSESSMENT

Consider failure of the CNG tank as a possible initial cause of a failure leading to a gas release and fire scenario. Figure (two slides later) depicts the scenarios, frequencies and consequences. Also, marginal risk contribution due to each scenario is calculated along with the risk contributors due to all scenarios. Clearly the risk is calculated as

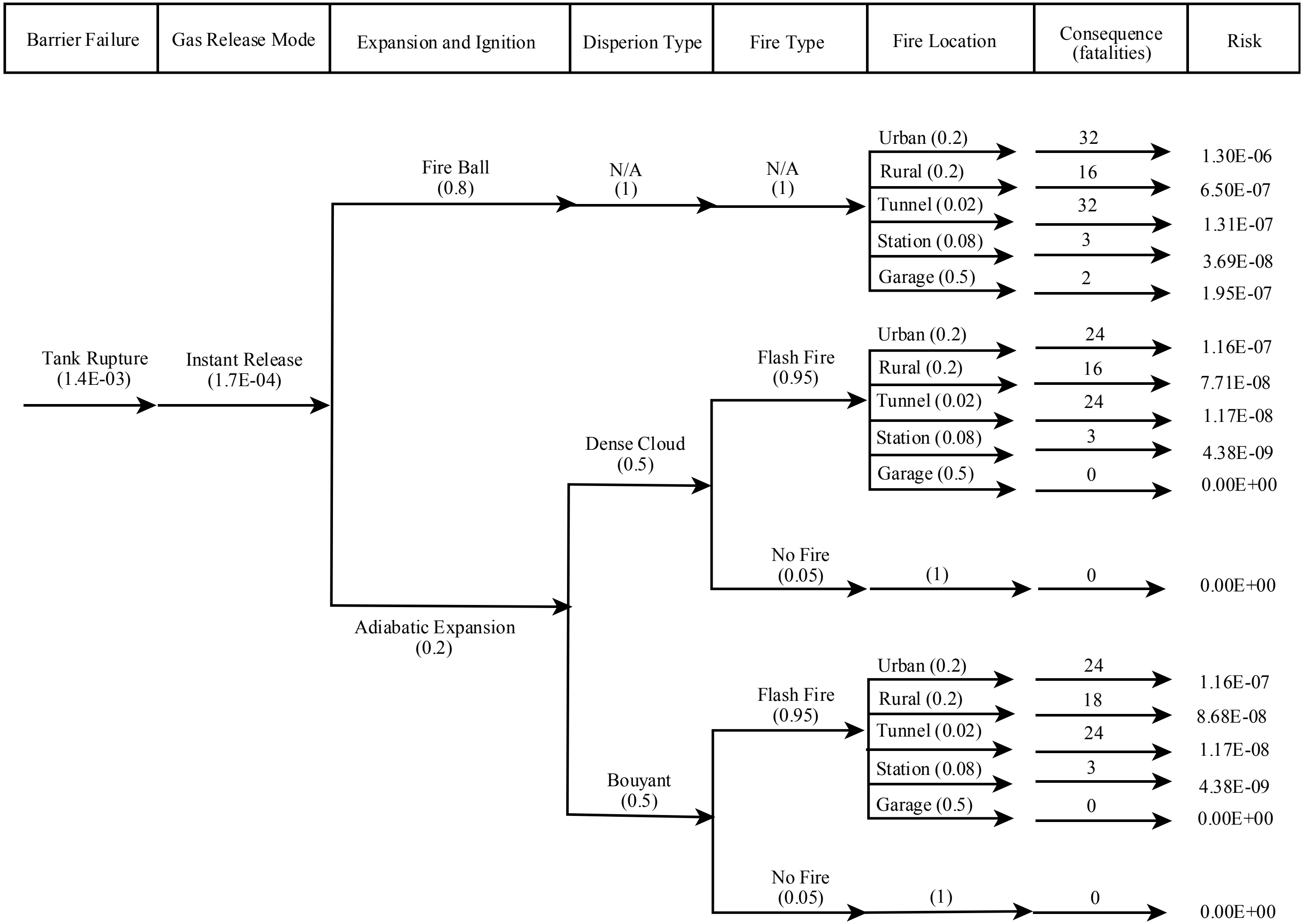
Risk = (Frequency of a barrier failure) ×
(Probability of gas release given barrier failure) ×
(Probability of expansion and ignition given gas release) ×
(Probability of a particular fire dispersion type given ignition of the gas) ×
(Probability of a particular fire type given a specific dispersion) ×
(Probability that fire occurs in a specific location) × (Consequence).

FAILURE DATA COLLECTION, ANALYSIS, AND PERFORMANCE ASSESSMENT

The following procedures should be followed in this step of the PRA:

1. Determine generic values of material strength or endurance, load or damage agents, failure times, failure occurrence rate and failures on demand for each item (hardware, human action, or software) identified in the PRA models. This can be obtained either from facility-specific or system-specific experiences, from generic sources of data, or both
2. Gather data on hazard barrier tests, repair, and maintenance data primarily from experience, if available. Otherwise use generic performance data.
3. Assess the frequency of initiating events and other probability of failure events from experience, expert judgment, or generic sources.
4. Determine the dependent or common cause failure probability for similar items, primarily from generic values. However, when significant specific data are available, they should be primarily used

SCENARIOS INVOLVING A CNG TANK FAILURE



QUANTIFICATION AND INTEGRATION

The following procedures should be followed as part of the quantification and integration step in the PRA:

1. Merge corresponding fault trees associated with each failure or success event modeled in the event tree scenarios (i.e., combine them in a Boolean form). Develop a reduced Boolean function for each scenario (i.e., truncated minimal cut sets).
2. Calculate the total frequency of each sequence, using the frequency of initiating events, the probability of barrier failure including contributions from test and maintenance frequency (outage), common cause failure probability, and human error probability.
3. Use the minimal cut sets of each sequence for the quantification process. If needed, simplify the process by truncating based on the cut sets or probability.
4. Calculate the total frequency of each scenario.
5. Calculate the total frequency of all scenarios of all event trees.

RISK MATRIX FOR CNG FUELED BUSES FOR ALL SCENARIOS

CNG Bus Fire Scenarios Involving Failure of The Following Class of Barriers	Frequency of Occurrence/ Bus/Year)	Risk (Fatalities/ Bus/Year)	Risk (Fatalities/ 100 Million Miles of Travel)
Bus Hardware (Such as the gas tank)	1.4×10^{-3}	2.7×10^{-6}	2.8×10^{-2}
Refueling Station Hardware	3.7×10^{-3}	7.5×10^{-6}	7.8×10^{-2}
Electrostatic Discharge of CNG	1.4×10^{-5}	3.7×10^{-6}	3.9×10^{-2}
Impact Failures due to Collisions	3.6×10^{-2}	4.6×10^{-6}	4.8×10^{-2}
Non-CNG Hardware	3.6×10^{-4}	3.1×10^{-6}	3.2×10^{-2}
Operator Error	4.0×10^{-2}	3.5×10^{-7}	3.5×10^{-3}
Total Fire Fatality Risk	---	2.2×10^{-5}	2.3×10^{-1}

**Assuming ~11,000 miles of travel per bus per year*

UNCERTAINTY ANALYSIS

Steps in uncertainty analysis include:

1. Identify models and parameters that are uncertain and the method of uncertainty estimation to be used for each.
2. Describe the scope of the PRA.
3. Estimate and assign probability distributions depicting model and parameter uncertainties in the PRA.
4. Propagate uncertainties associated with the hazard barrier models and parameters to find the uncertainty associated with the risk value.
5. Present the uncertainties associated with risks and contributors to risk in an easy way to understand and visually straightforward to grasp.

RISK RANKING AND IMPORTANCE ANALYSIS

Applications of importance measures may be categorized into the following areas:

1. (Re)Design: To support decisions of the system design or redesign by adding or removing elements (barriers, subsystems, human interactions, etc.)
2. Test and Maintenance: To Address questions related to the plant performance by changing the test and maintenance strategy for a given design.
3. Configuration and Control: To measure the significance or the effect of failure of a component on risk or safety or temporarily taking a component out of service.
4. Reduce uncertainties in the input variables of the PRAs.

RISK RANKING AND IMPORTANCE ANALYSIS

The following are the major steps of importance ranking:

1. Determine the purpose of the ranking and select appropriate ranking importance measure that has consistent interpretation for the use of the ranked results.
2. Perform risk ranking and uncertainty ranking, as needed.
3. Identify the most critical and important elements of the system with respect to the total risk values and total uncertainty associated with the calculated risk values.

INTERPRETATION OF RESULTS

The basic steps of the PRA results interpretation are:

1. Determine accuracy of the logic models and scenario structures, assumptions, and scope of the PRA.
2. Identify system elements for which better information would be needed to reduce uncertainties in failure probabilities and models used to calculate performance.
3. Revise the PRA and reinterpret the results until attaining stable and accurate results

STRENGTH OF PRA

The most important strengths of the PRA, as the formal engineering approach to risk assessment are:

1. Integrated and systematic examination of a broad set of design and operational features of an engineered system.
2. Incorporates the influence of system interactions and human-system interfaces.
3. Incorporating operating experience with the engineered system and updating risk estimates.
4. A process for the explicit consideration of uncertainties.
5. Analysis of competing risks (e.g., of one system vs. another or of possible modifications to an existing system).
6. Analysis of (assumptions, data) issues via sensitivity studies.
7. Measure of the absolute or relative importance of systems, components to the calculated risk value.
8. Measure of overall level of health and safety for the engineered system.

?