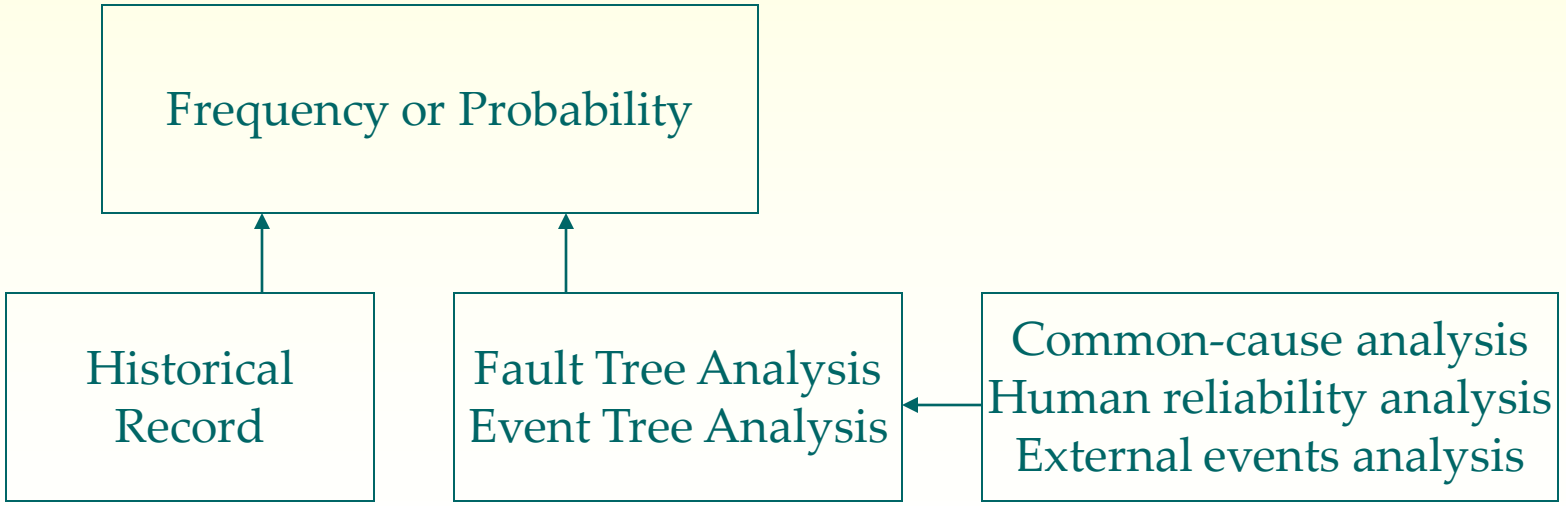
Event Probability and Failure Frequency Analysis

2009_2nd semester

En Sup Yoon

Incident Frequencies from the Historical Record

- Frequency estimation technique
  - Incident frequency can be obtained directly from the historical record



- Historical approach
  - Based on records and incident frequencies
  - Five-step methodology
    - Define context
    - Review source data
    - Check data applicability
    - Calculate incident frequency
    - Validate frequency

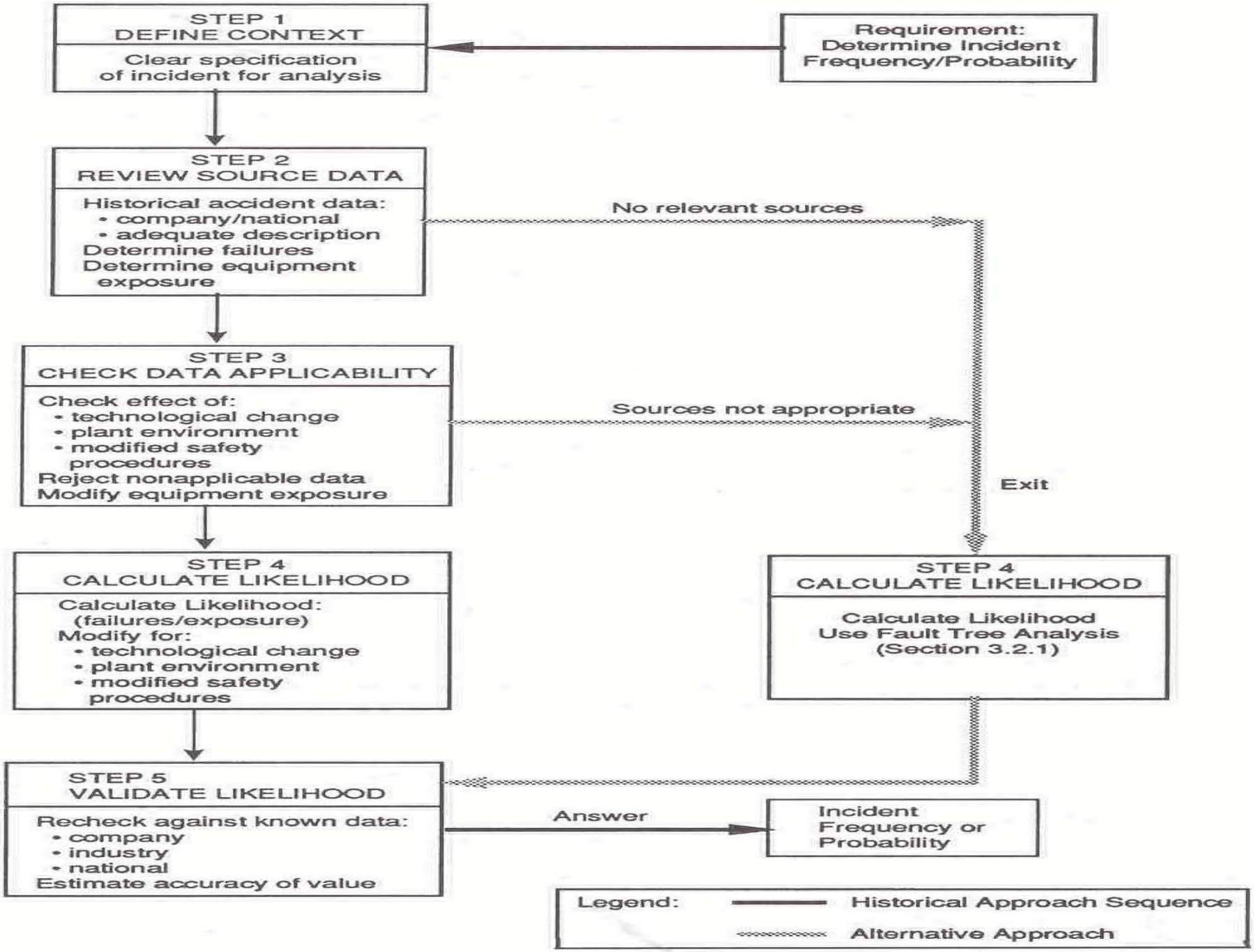


FIGURE 3.2. Procedure for predicting incident likelihood from the historical record.

- Step 1. Define context
  - Clear specification of the incidents for which frequency estimates are sought
- Step 2. Review source data
  - All relevant historical data should be reviewed for completeness and independence
  - Determine failure and equipment exposure
- Step 3. Check data applicability
  - Careful review of the source data to confirm applicability

- Step 4. Calculate event likelihood
  - Historical frequency can be obtained by dividing the number of incidents by the exposed population
- Step 5. Validate frequency

Sample Problem

- Estimation of leakage frequencies from a gas pipeline
  - Step 1. Define Context
    - Objective : determine the leakage frequency of proposed 8-in-diameter, 10 mile long, high pressure ethane pipe to be laid in a semiurban area. The proposed pipeline will be seamless, coated and cathodically protected
  - Step 2. Review source data
    - Applicable data is the gas transmission leak report data collected by the U.S. Department of Transportation for the years 1970-1980

- Step 3. Check data applicability
  - Incorporated pipeline and certain nonrelevant incidents must be rejected among all data base
  - Examples are
    - Pipelines that are not steel
    - Pipelines that are installed before 1950
    - Incident arising at a longitudinal weld
- Step 4. Calculate likelihood
  - The pipeline leakage frequencies are derived from the remaining DOT data using following procedure
    - Estimate the base failure for each failure mode
    - Modify the base failure rate, where necessary to allow for other condition specific this pipeline

TABLE 3.1. Contribution of Failure Mechanisms to Pipeline Example

Failure mode	Failure frequency (per 1000 pipe mile-years)			
	Raw DOT data	Modified data (inappropriate data removed)	Modification factor (judgment)	Final values
Material defect	0.21	0.07	1.0	0.07
Corrosion	0.32	0.05	1.0	0.05
External impact	0.50	0.24[a]	2.0	0.48
Natural hazard	0.35	0.02	0.5	0.01
Other causes	0.06	0.05	1.0	0.05
Total failure frequency	1.44	0.43	—	0.66

[a] This value is appropriate for an 8-in. pipe

Frequency Modeling Techniques

- Fault tree analysis
  - First developed at Bell Telephone Laboratories in 1961 for missile launch control reliability
  - Permits the hazardous incident(top event) frequency to be estimates from a logic model of the failure mechanisms of a system
  - Based on the combinations of failures of more basic system component, safety systems and human reliability
  - The use of a combination of relatively simple logic gate(usually AND and OR gate)

Fault tree analysis

- Usual objective of applying FTA
  - Estimation of the frequency of occurrence of the incident (or of the reliability of the equipment)
  - Determination of the combination of equipment failures, operating conditions, environmental conditions and human errors that contribute to the incident
  - Identification of remedial measures for the improvement of reliability or safety and the determination of their impact and to identify which measures have the greatest impact for the lowest cost

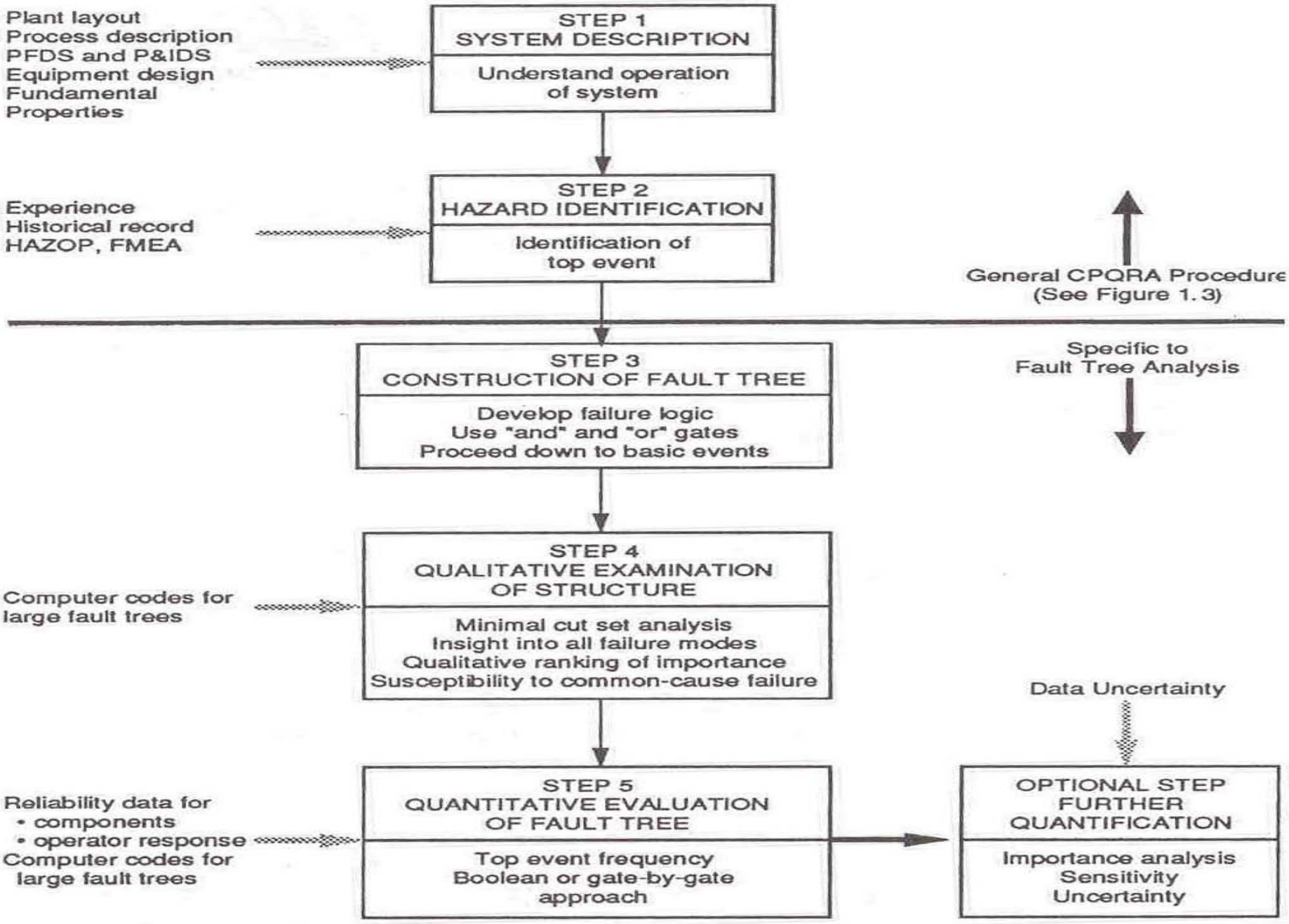


FIGURE 3.3. Logic diagram for application of fault tree analysis.

TABLE 3.2. Terms Used in Fault Tree Analysis

Term	Definition
Event	An unwanted deviation from the normal or expected state of a system component
Top event	The unwanted event or incident at the "top" of the fault tee that is traced downward to more basic failures using logic gates to determine its causes and likelihood
Intermediate event	An event that propagates or mitigates an initiating (basic) event during the accident sequence (e.g., improper operator action, failure to stop an ammonia leak, but an emergency plan mitigates the consequences)
Basic event	A fault event that is sufficiently basic that no further development is judged necessary (e.g., equipment item failure, human failure, external event)
Undeveloped event	A base event that is not developed because information is unavailable or historical data are adequate.
Logic gate	A logical relationship between input (lower) events and a single output (Higher) event. These logical relationships are normally represented as AND or OR gates. AND gates combine input events, all of which must exist simultaneously for the output to occur. OR gates also combine input events, but any one is sufficient to cause the output. Other gate types, which are variants of these and are occasionally used, include inhibit gate, priority AND, exclusive OR, and majority voting gate. Details of these are given in the introductory texts noted elsewhere.
Likelihood	A measure of the expected occurrence of an event, This may be expressed as a frequency (e.g., events/years), a probability of occurrence during some time interval, or a conditional probability (e.g., probability of occurrence given that a precursor event has occurred)
Boolean algebra	That branch of mathematics describing the behavior of linear functions of variables that are binary in nature: on or off, open or closed, true or false. All coherent fault trees can be converted into an equivalent set of Boolean equations.
Minimal cut set	The smallest combination of component and human failures that, if they all occur, will cause the top event to occur. The failures all correspond to basic or undeveloped events. A top event can have many minimal cut sets, and each minimal cut set may have a different number of basic or undeveloped events. Each event in the minimal cut set is *necessary* for the top event to occur, and all events in the minimal cut set are *sufficient* for the top event to occur.

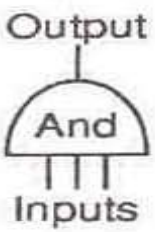
- Procedure for undertaking FTA
  - System description and choice of system boundary
  - Hazard identification and selection of the top event
  - Construction of the fault tree
  - Qualitative examination of structure
  - Quantitative evaluation of the fault tree

- Step 1. System description
  - Required information
    - Chemical and physical processes involved in the plant/system
    - Specific information on the whole process and every stream
    - Hazardous properties of materials
    - Plant and site layout drawings
    - PFD, P&ID
    - Equipment specification
    - Operation of the plant(operating, maintenance, emergency, start-up)
    - Human factor(man-machine interface)
    - Environmental factor

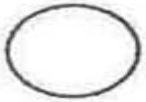
- Step 2. Hazard identification
  - To identify top event, use qualitative hazard analysis technique, such as PHA, What-If analysis, HAZOP
  - Generally 10-20 top events are often adequate to characterize the risk from a single process plant of moderate complexity

- Step 3. Construction of fault tree
  - Three approaches to fault tree construction are manual, algorithmic and automatic
  - Manual fault tree construction
  - Algorithm fault tree construction
    - More systematic methods for the development of fault trees using algorithm such as digraph
  - Automatic fault tree synthesis
    - Enter process flow diagram in to the computer and obtain fault tree for all conceivable top event

OR Gate: The output occurs if one or more of the inputs to the gate exists.

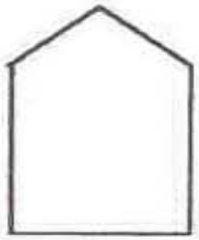


AND Gate: The output occurs if all of the inputs to the gate exist simultaneously.

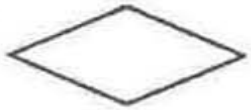


BASIC EVENT: The basic event represents a basic fault that requires no further development into more basic events.

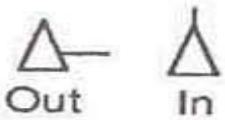
INTERMEDIATE EVENT: The rectangle is often used to present descriptions of events that occur because of one or more other fault events.



HOUSE EVENT: The house event represents a condition that is assumed to exist as a boundary condition (probability of occurrence = 1).



UNDERDEVELOPED EVENT: The underdeveloped event represents a fault event that is not examined further because information is unavailable, its consequences are insignificant, or because a system boundary has been reached.



TRANSFER SYMBOLS: The transfer in symbol indicates that the fault tree is developed further at the occurrence of the corresponding transfer out symbol (on another page). The symbols are labeled to ensure that they can be differentiated.

FIGURE 3.4. Standard fault tree symbols.

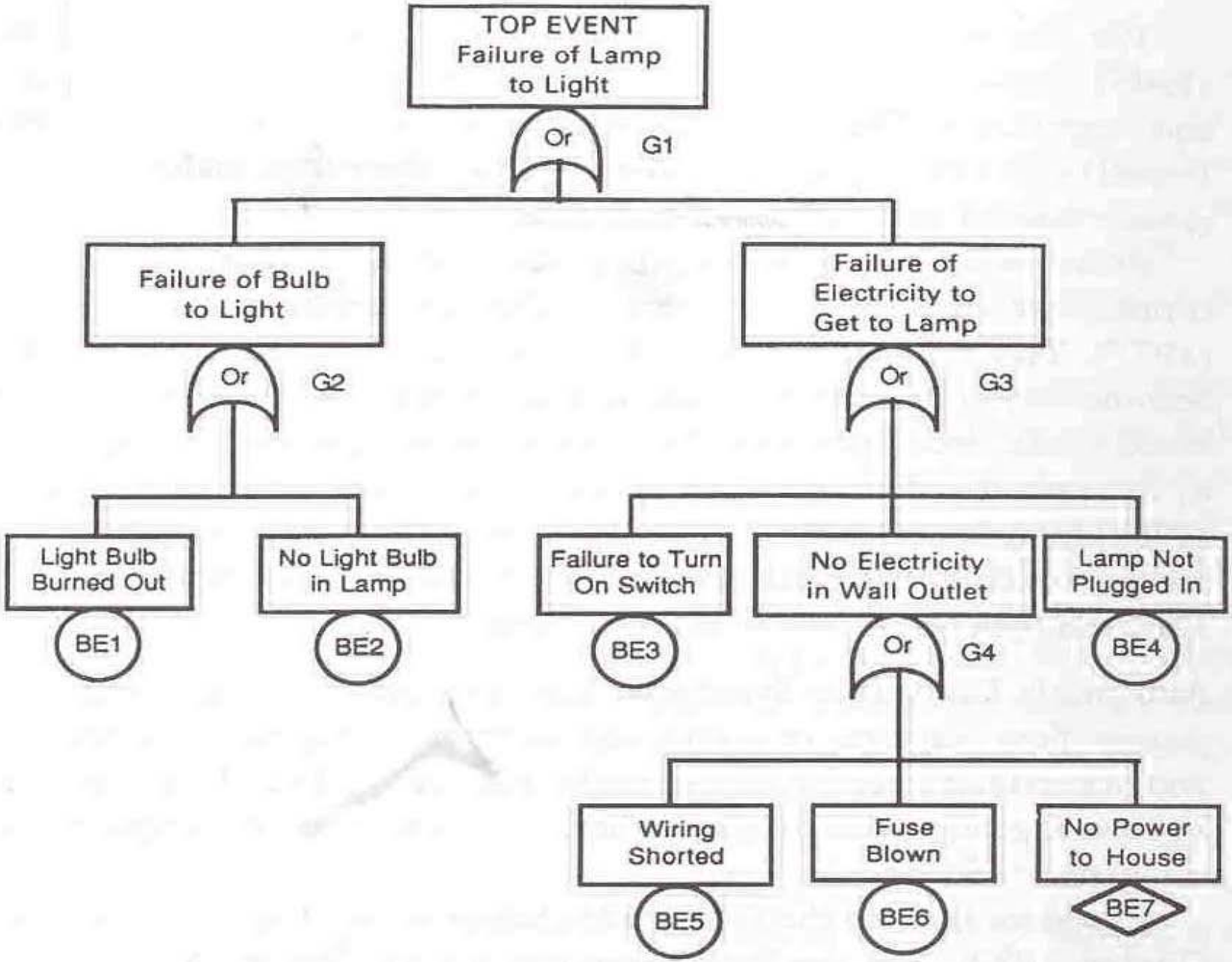


FIGURE 3.5. Fault tree for failure of lamp to light.

- Step 4. Qualitative examination of structure
  - Examine qualitatively to understand the mechanisms of failure
  - The qualitative importance can be determined from the minimal cut set
  - Minimal cut set
    - Mathematical technique for manipulating the logic structure of a fault tree to identify all combinations of basic events that result in the occurrence of the top event

- Step 5. Quantitative evaluation of fault tree
  - Calculate the top event frequency or probability
  - Use minimal cut set approach in the Boolean expression or gate-by-gate approach
  - Gate-by-gate approach
    - Start with the basic event of the fault tree and proceeds upward toward the top event
    - All inputs to a gate must be defined before calculating the gate output
    - All the bottom gates must be computed before proveeding to the higher level

TABLE 3.3. Rules for Gate-by-Gate Fault Tree Calculation[a]

Gate	Input pairing	Calculation for output	Units
OR	P_A OR P_B	$P(\text{A OR B}) = 1-(1-P_A)(1-P_B)$ $= P_A + P_B - P_A P_B$ $\cong P_A + P_B$	
	F_A OR F_B	$F(\text{A OR B}) = F_A + F_B$	t^{-1}
	P_A OR F_B	Not permitted	
AND	P_A AND P_B	$P(\text{A AND B}) = P_A P_B$	
	F_A AND F_B	Unusual pairing, reform to F_A AND P_B[b]	t^{-1}
	F_A AND P_B	$F(\text{A AND B}) = F_A P_B$	

[a] P, probability; F, frequency (time^{-1}); t, time (usually year).

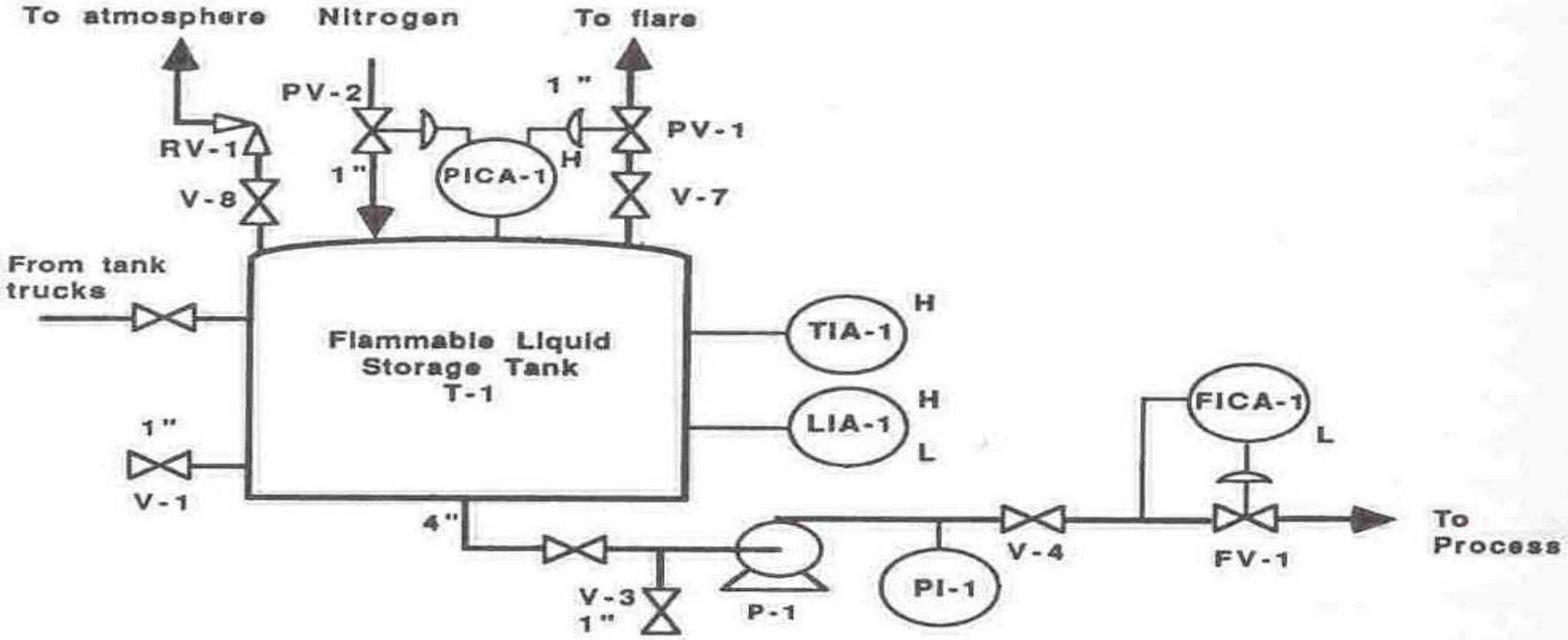
[b] For an example, see sample problem.

- Strength and weaknesses
  - Advantage of the FTA is the complementary information provided from the qualitative and quantitative analysis of the fault tree
  - Weakness
    - Required much effort to develop the tree
    - Potential for error if failure paths are omitted or manual calculation methods are incorrectly employed

TABLE 3.4. Sample Computer Codes Available for Fault Tree Analysis

Step	Activity	Computer Codes	Availability
3	Construction of fault tree	Rikke	R. Taylor, Denmark
		CAT	G. Apostolakis et al. (1978)
		Fault Propagation	FP Lees, UK
		Diagraph	S. Lapp and G. Powers (1977)
		IRRAS-PC (plotting)	EG & G, Idaho
		TREDRA	JBF Associates
		GRAFTER	Westinghouse
		BRAVO	JBF Associates
4	Qualitative examination	IRRAS-PC	EG & G, Idaho
		CAFTA + PC	Science Applications Int. Corp.
		SAICUT	Science Applications Int. Corp.
		MOCUS	JBF Associates
		GRAFTER	Westinghouse
		BRAVO	JBF Associates
5	Quantitative evaluation	IRRAS-PC	EG & G, Idaho
		CAFTA + PC	Science Applications Int. Corp.
		SUPERPOCUS	JBF Associates
		GRAFTER	Westinghouse
		BRAVO	JBF Associates
		RISKMAN	Pickard, Lowe, and Garrick

[a] R. Taylor, Advanced Risk Analysis, Egern Vej 16, 2000 Copenhagen, Denmark; EG & G Services Inc., P.O. Box 2266, Idaho Falls, ID 83401; FP Lees, Dept. Chemical Engineering, Loughborough University, Loughborough, Leics, UK; Science Applications Int. Corp., 5150 El Camino Real, Los Altos, CA 94022; JBF Associates, 1000 Technology Drive, Knoxville, TN; Westinghouse Risk Management, P.O. Box 355, Pittsburgh, PA 15230; Pickard, Lowe, and Garrick, 2260 University Dr., Newport Beach, CA 92660.



P & I D Legend	
EQUIPMENT AND VALVES	**INSTRUMENTS**
FV - Flow Control Valve T - Tank P - Pump PV - Pressure Control Valve RV - Relief Valve V - Valve 1" - 1 inch size	P - Pressure T - Temperature L - Level F - Flow I - Indicator C - Controller A - Alarm H - High, L - Low

FIGURE 3.6. Flammables liquid storage tank P&ID.

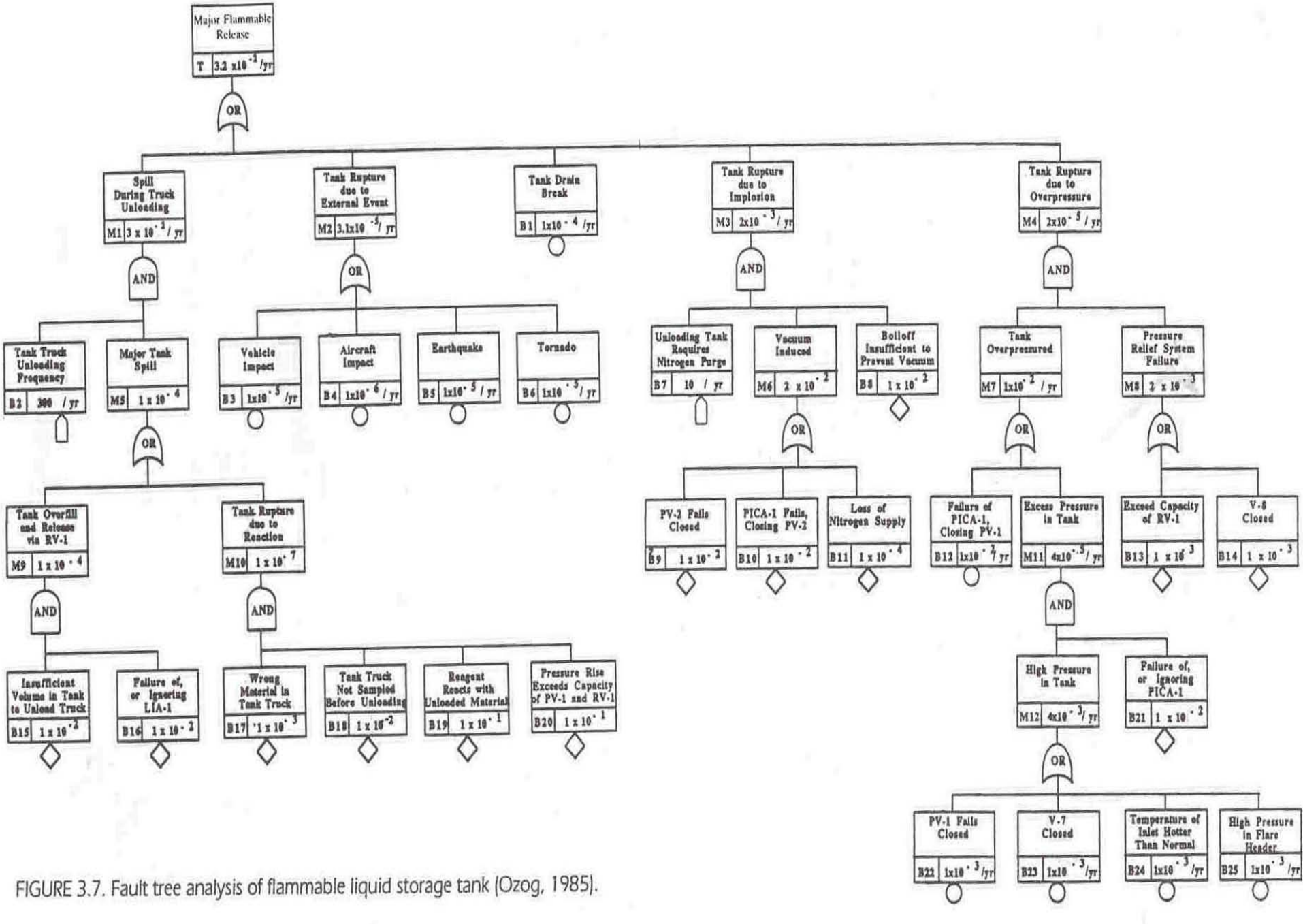


FIGURE 3.7. Fault tree analysis of flammable liquid storage tank (Ozog, 1985).

Event Tree Analysis

- A graphical logic model that identified and quantified possible outcome following an initiating event
- Provide systematic coverage of the time sequence of event propagation
- Consequences can be direct (e.g., fire, explosion) or indirect (e.g., domino incidents on adjacent plants)

- Event tree analysis
  - Preincident event tree
    - Can be used to evaluate the effectiveness of a multielement protective system
  - Postincident event tree
    - Can be used to identify and evaluate quantitatively the various incident outcome(e.g., flash fire, UVCE, BLEVE) that might arise from a single release of hazardous material

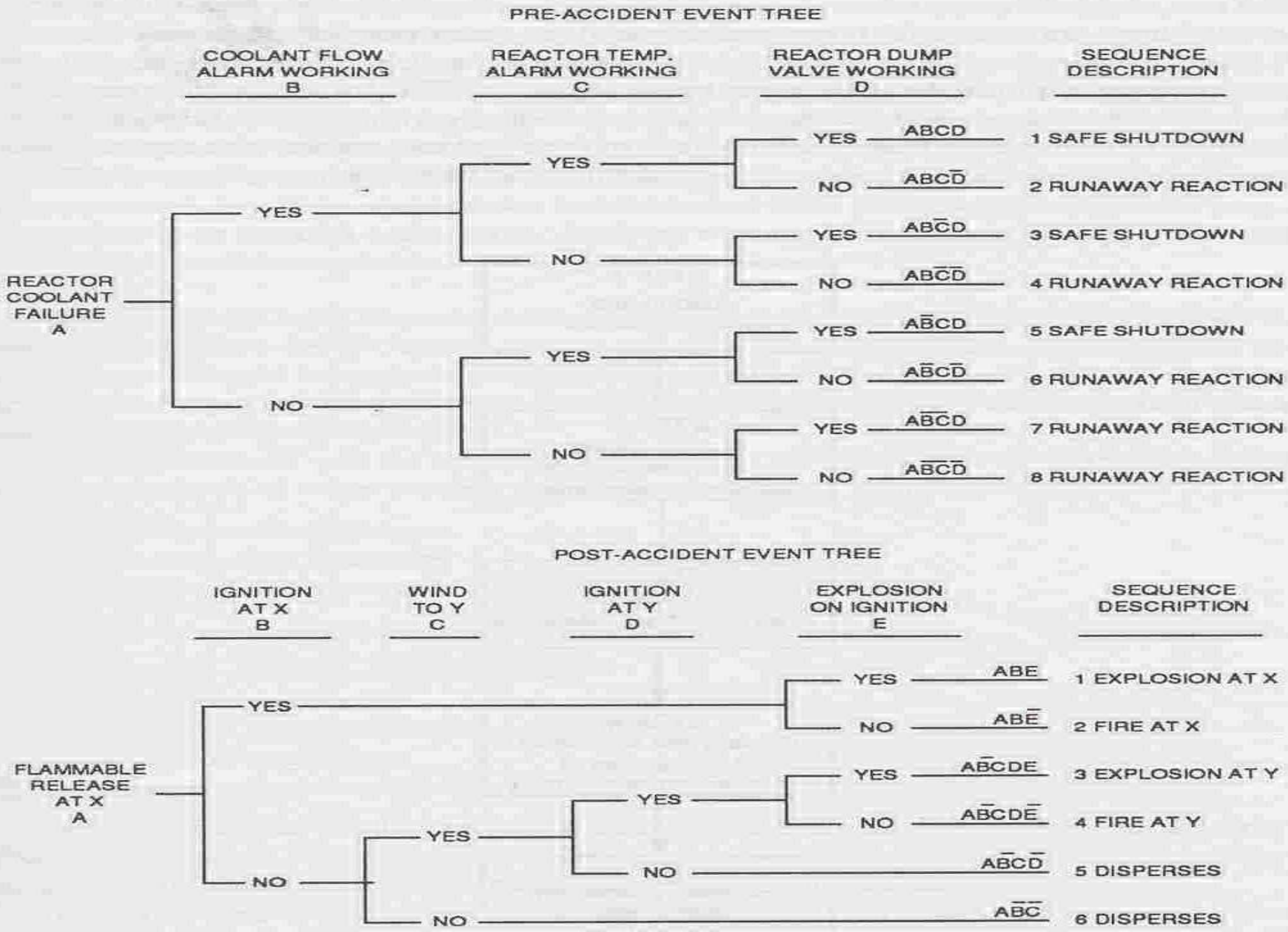


FIGURE 3.8. Examples of preincident and postincident event trees. From EFCE (1985).

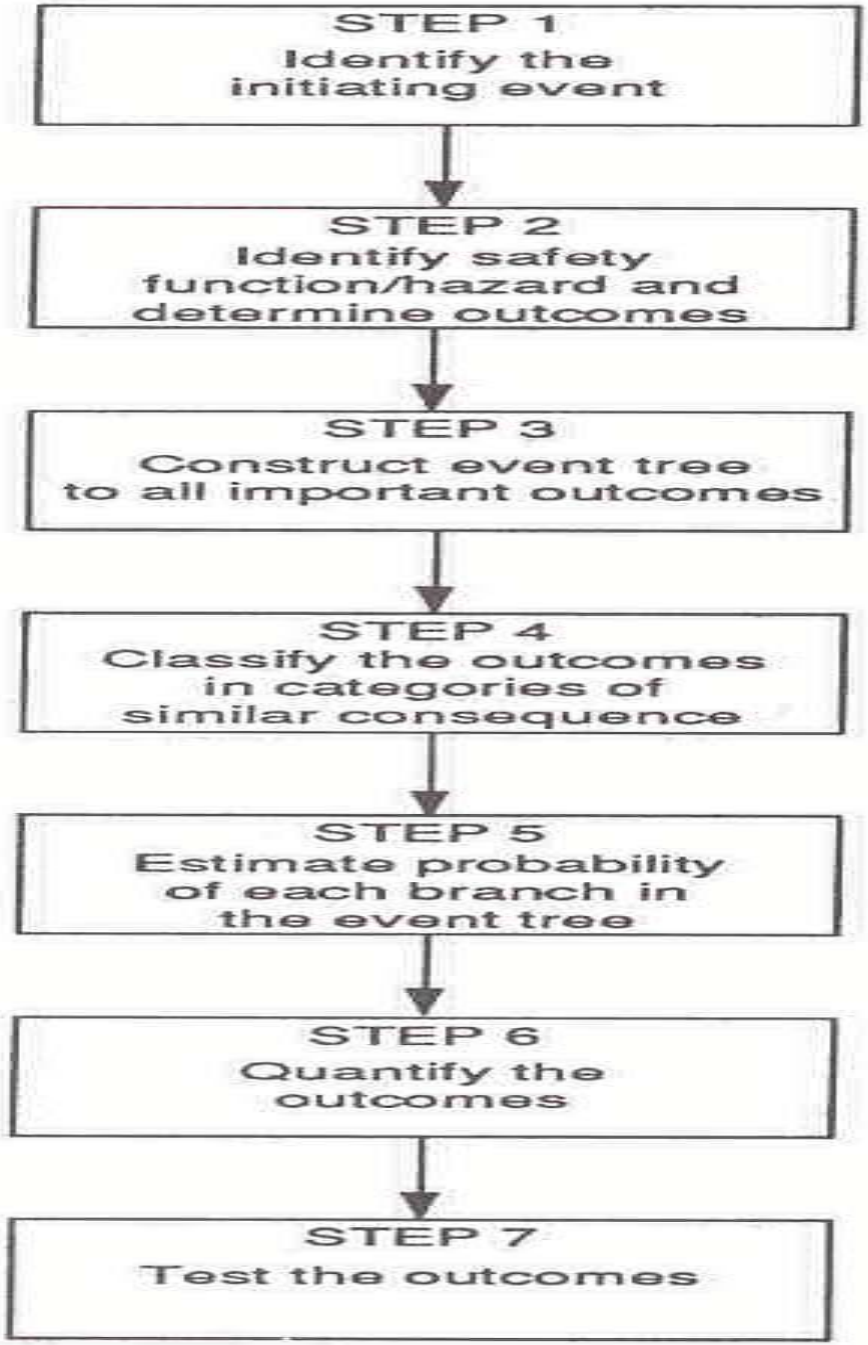


FIGURE 3.9. Logic diagram for event tree analysis.

- Procedure of ETA
  - Step 1. Identifying the initiating event
    - Identify the failure event corresponding to a release of hazardous material
  - Step 2. Identify safety function/hazard promoting factor and determine outcomes
    - Safety function is a device, action or barrier that can interrupt the sequence from an initiating event
    - Safety function
      - Automatic safety system
      - Alarm to alert operators
      - Barriers or containment to limit the effect of an accident

- Hazard promoting factor
  - Ignition or no ignition or release
  - Explosion or flash fire
  - Liquid spill contained in dike or not
  - Daytime or nighttime
  - Meteorological condition
- Step 3. Construction the event tree
  - Graphically display the chronological progression of an incident
  - At each heading or node, two or more alternatives are analyzed until a final outcome is obtained for each node

- Step 4. Classify the outcome
  - Final outcome can be classified according to type of consequence model that must be employed to complete the analysis
- Step 5. Estimate the probability of each branch in the event tree
  - Source of conditional probability data may be the historical record, plant and process data, chemical data, environmental data, equipment data, human reliability data and use of expert opinion
  - The probabilities associated with each branch must sum to 1.0 for each heading

- Step 6. Quantify the outcomes
  - Determined by multiplying the initiating event frequency with the conditional probabilities along each path leading to that outcome
- Test the outcome
  - Test the results with common sense and against the historical record
  - Bone by independent reviewer

Sample Problem

- Postincident analysis of a large leakage of pressurized flammable material from an isolated LPG storage tank
- Initiating event is LPG leakage
- Table 3.5 provide a sample event tree data
- Figure 3.10 provide the event tree for LPG leakage

TABLE 3.5. Sample Event Tree Input Data

Event	Frequency or probability[a] ($\times 10^{-4}$/yr.)	Source of data[a]
A. Large leakage of pressurized LPG	1.0	Fault tree analysis
B. Immediate ignition at tank	0.1	Expert opinion
C. Wind blowing toward populated area	0.15	Wind rose data
D. Delayed ignition near populated area	0.9	Expert opinion
E. VCE rather than flash fire	0.5	Historical data
F. Jet flame strikes the LPG tank	0.2	Tank layout geometry

[a] These data are for illustrative purposes only.

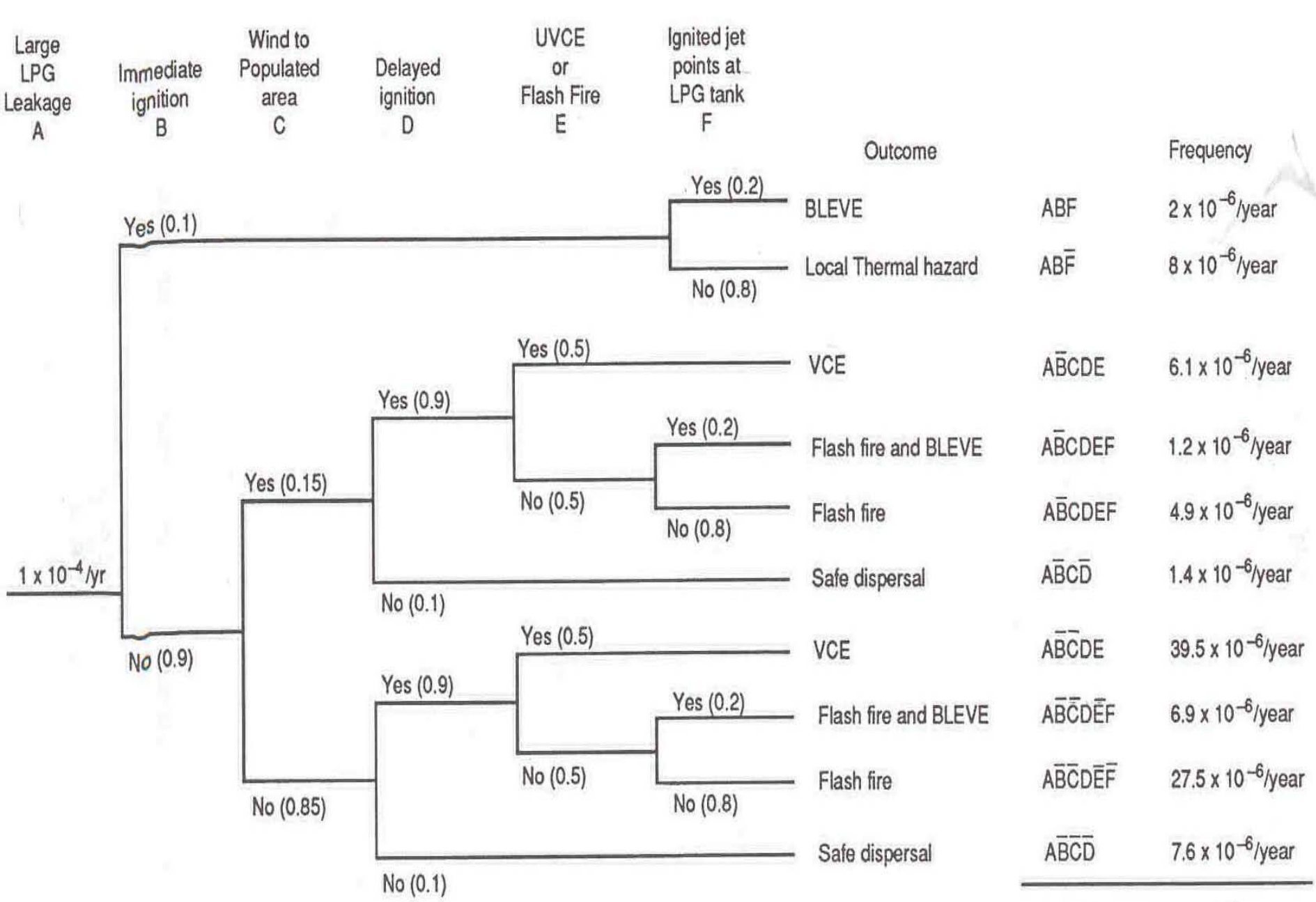


FIGURE 3.10. Event tree outcomes for sample problem.

TABLE 3.6. Sample Event Tree Outcomes and Frequencies

Outcome	Sequences leading to outcome	Frequency (per year)
BLEVE	$AB\overline{F}$	$2.0 \times 10^{-6} = 2.0 \times 10^{-6}$
Flash Fire	$A\overline{B}CD\overline{E}\overline{F} + A\overline{B}\overline{C}D\overline{E}\overline{F}$	$4.9 \times 10^{-6} + 27.5 \times 10^{-6} = 32.4 \times 10^{-6}$
Flash fire and BLEVE	$A\overline{B}CD\overline{E}F + A\overline{B}\overline{C}D\overline{E}F$	$1.2 \times 10^{-6} + 6.9 \times 10^{-6} = 8.1 \times 10^{-6}$
UVCE	$A\overline{B}CDE + A\overline{B}\overline{C}DE$	$6.1 \times 10^{-6} + 34.5 \times 10^{-6} = 40.5 \times 10^{-6}$
Local thermal hazard	$AB\overline{F}$	$8.0 \times 10^{-6} = 8.0 \times 10^{-6}$
Safe dispersal	$A\overline{B}C\overline{D} + A\overline{B}\overline{C}\overline{D}$	$1.4 \times 10^{-6} + 7.6 \times 10^{-6} = 9.0 \times 10^{-6}$
Total all outcomes		$= 100 \times 10^{-6}$

- Strength and weakness
  - Strength of the event tree is that it portrays the event outcomes in a systematic, logical, self-documenting form that is easily audited by others
  - Logical and arithmetic computations are simple and the format is usually compact
  - Indicating outcomes that lead directly to failures with no interventing protective measures

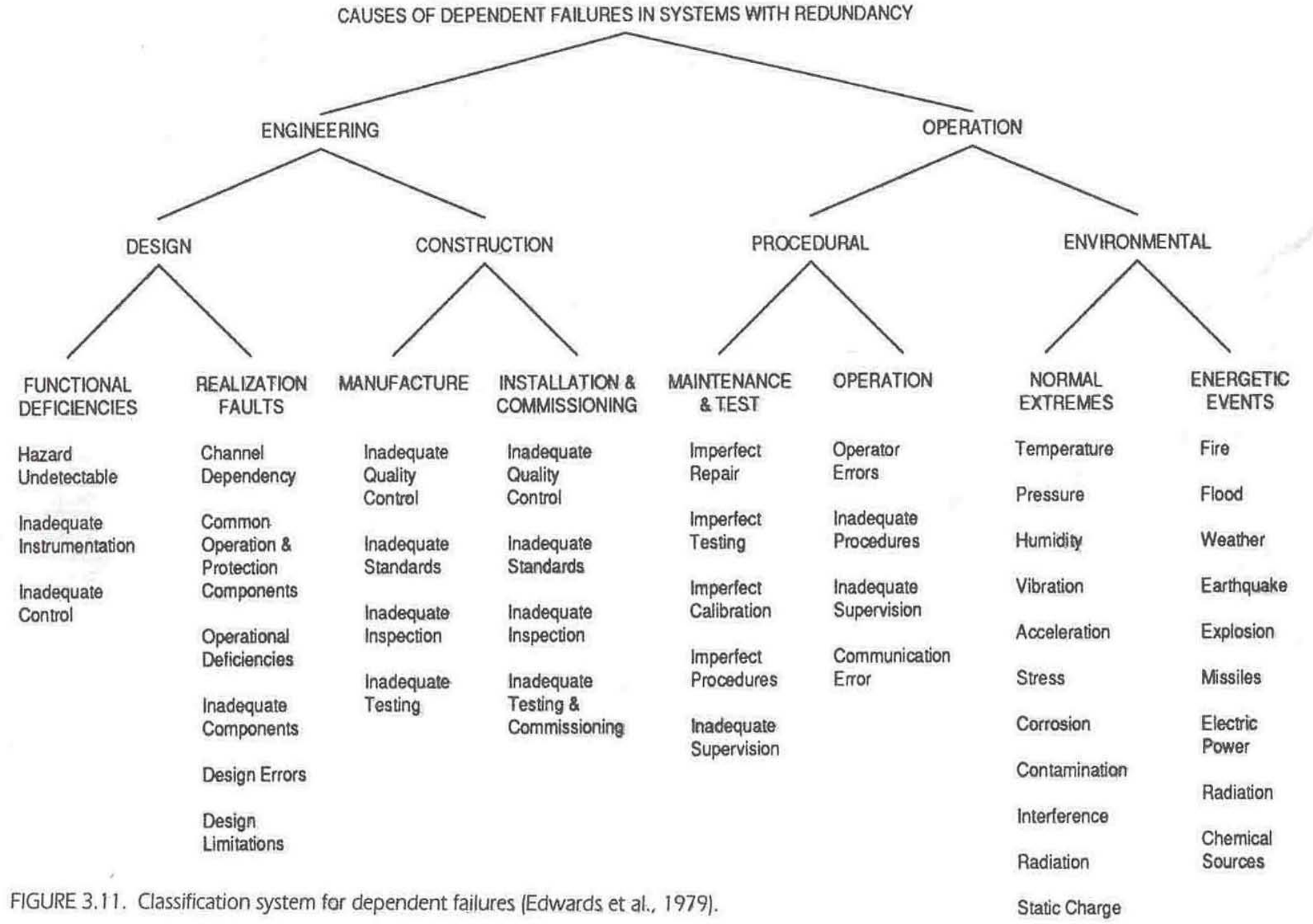


FIGURE 3.11. Classification system for dependent failures (Edwards et al., 1979).

Complementary Plant-modeling Technique

- Common cause failure analysis
  - Objective
    - Identification of relevant CCF events
    - Quantification of CCF contributors
    - Formulation of defense alternatives and stipulation of recommendation to prevent CCF

- Human reliability analysis
  - To provide quantitative values of human error for inclusion in fault tree analysis and event tree analysis
  - Valuable in identifying potential recommendations for error reduction
  - Characteristics
    - Identification of relevant tasks performed or to be performed
    - Representation of each task by some method, such as decomposition of the task into its principle component to identify
      - Opportunities for error
      - Points of interaction with the plant
    - Use of data derived from historical or judgment

Measurement, Calculation and Presentation of Risk Estimates

- Risk measure
  - Defines risks as a measure of economic loss, human injuries or environmental damage in terms of both the likelihood and magnitude of the loss, injury or damage
  - Three commonly ways of combining incident frequency and consequence data to produce risk estimates
    - Risk indices
    - Individual risk measures
    - Societal risk measures

TABLE 4.1. Presentation of Measures of Risk

Risk measure	Presentation format
	Indices
Equivalent social cost index	A single number index value representation
Fatal accident rate	A point estimate of fatalities/10^8 exposure hours
Individual hazard index	An estimate of peak individual risk or FAR
Average rate of death	A number representing the estimated average number of fatalities per unit time
Mortality index	A single value representation of consequence
	Individual risk
Individual risk contour	Contour lines connecting points of equal risk superimposed over a local map
Individual risk profile or risk transect	A graph of individual risk as a function of distance from the plant in a specified direction
Maximum individual risk	A single numerical value of individual risk corresponding to the person at highest risk
Average individual risk (exposed population)	A single numerical value estimating the average risk to a person in the exposed population
Average individual risk (total population)	A single numerical value estimating the average risk to a person in a predetermined population, whether or not all members of that population are exposed to the hazard
	Societal risk
Societal risk curve (F-N curve)	A graph of the cumulative probability or frequency of events causing N or more fatalities, injuries or exposures versus N, the number of fatalities, injuries, or exposures
Average societal risk	Another term for average rate of death
Aggregate Risk	A term for societal risk to personnel in a building or facility introduced in API 750 (API, 1995)

- Risk indices
  - Single number or tabulations of numbers which are correlated to the magnitude of risk
  - Represent simplifications of more complex risk measures and have unit which have real physical meaning(fatal accident rate, individual hazard index, average rate of) death
  - Limitation
    - There may not be absolute criteria for accepting or rejecting the risk
    - Indices risk resolution and do not communicate the same information as individual or societal risk measure

- Types of Risk indices-1
  - FAR(fatal accident rate)
    - Estimated number of fatalities per 10^8 exposure hours
  - IHI(individual hazard index
    - Actual time that a person is exposed to the hazard of concern
  - Average rate of death
    - Average number of fatalities that might be expected per unit time from all possible incident
  - Mortality index or number
    - Characterized the potential hazards of toxic material storage

- Types of Risk indices-2
  - Dow fire and explosion index
    - Estimate relative risk from fire and explosion
    - Estimate the magnitude of potential plant damage from a fire or explosion
  - Dow chemical exposure index
    - Estimates risk associated with a single toxic chemical release

- Individual risk
  - Risk to a person in the vicinity of a hazard
  - Include the nature of the injury to the individual, likelihood of the injury occurring and the time period over which the injury might occur
  - Can be estimated for the most exposed individual, for group of individual at particular places or for an average individual in an effect zone

- Definition of some individual risk measures
  - Individual risk contours
    - The geographical distribution of individual risk
  - Maximum individual risk
    - The individual risk to the person exposed to the highest risk in an exposed population
  - Average individual risk
    - The individual risk averaged over the population that is exposed to risk from the facility
    - Calculated for the duration of the activity or may be averaged over the working day

- Societal risk
  - A measure of risk to a group of people
  - Expressed in terms of the frequency distribution of multiple casualty event(the F-N curve)
  - Societal risk estimation requires a definition of the population at risk around the facility

Risk Presentation

- Risk presentation
  - Provide a simple quantitative risk description useful for decision making
  - Reduces this large volume of information to a manageable form
  - End result may be a single0number index, a table, a graph and/or a risk map

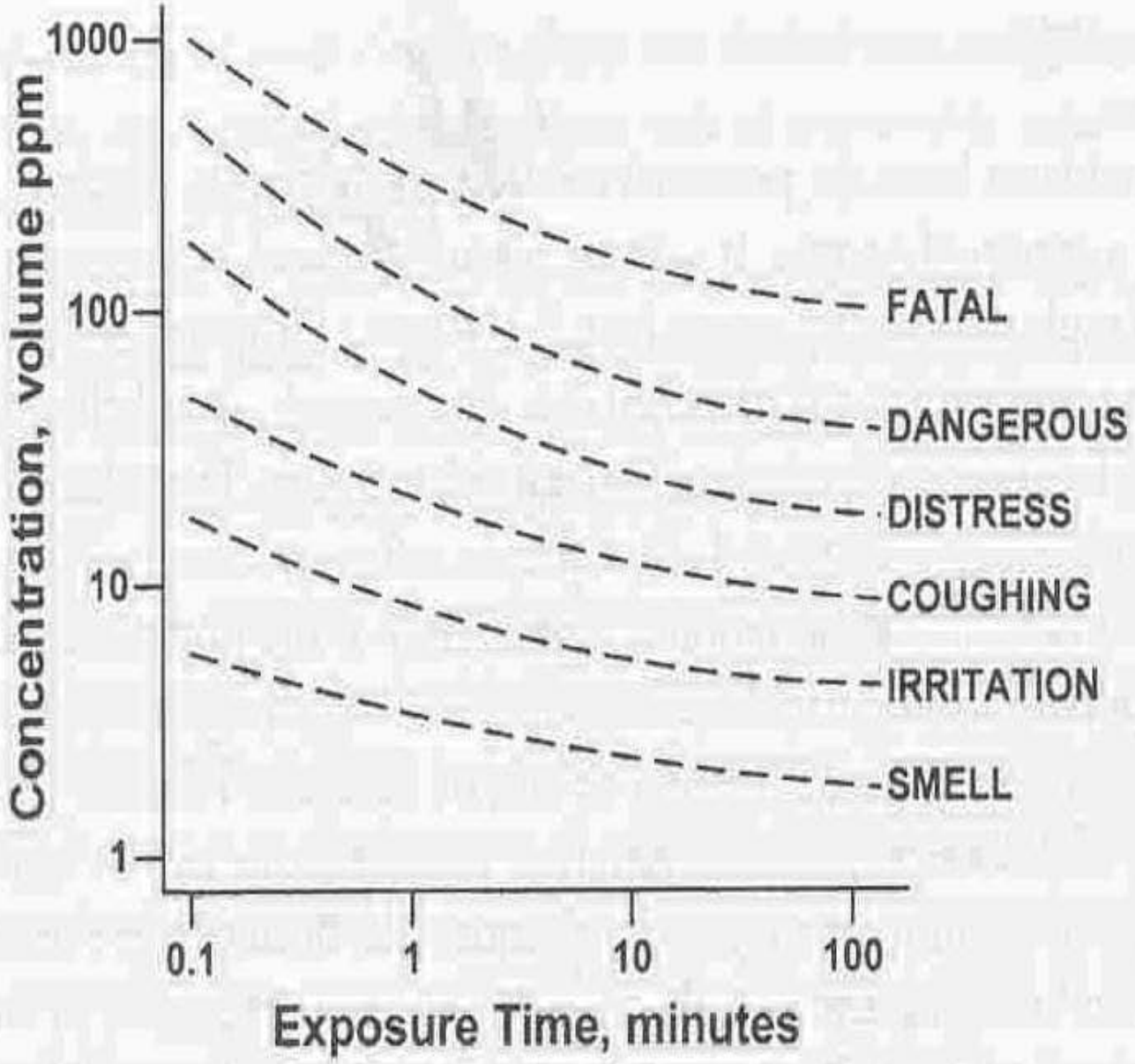


FIGURE 4.1. Typical relationship between injury levels and concentration/exposure for a toxic gas.

- Risk indices
  - Risk indices are single-number measurement, they are normally presented in tables
    - Foe example, Kletz(1977) has tabulated the FAR for various industries in the U.K.

TABLE 4.2. Fatal Accident Rates in Various Industries and Activities[a]

Activity	Fatal accident rate (fatalities/10^8 exposed hr)
British industry (overall)	4
Clothing and footwear manufacture	0–15
Vehicle manufacture	1–3
Timber, furniture, and so on	3
Metal manufacture, ship building	8
Agriculture	10
Coal mining	12
Railway shunters	45
Construction erectors	67
Staying at home (men 16–65)	1
Traveling by train	5
Traveling by car	57

[a] From Kletz (1977).

- Individual risk
  - Common form are risk contour plots(figure 4.2) and individual risk profiles also known as risk transect(figure 4.3)
  - Risk contour shows individual risk estimates at specific point on a map
  - Risk profile is a plot of individual risk as a function of distance from the risk source

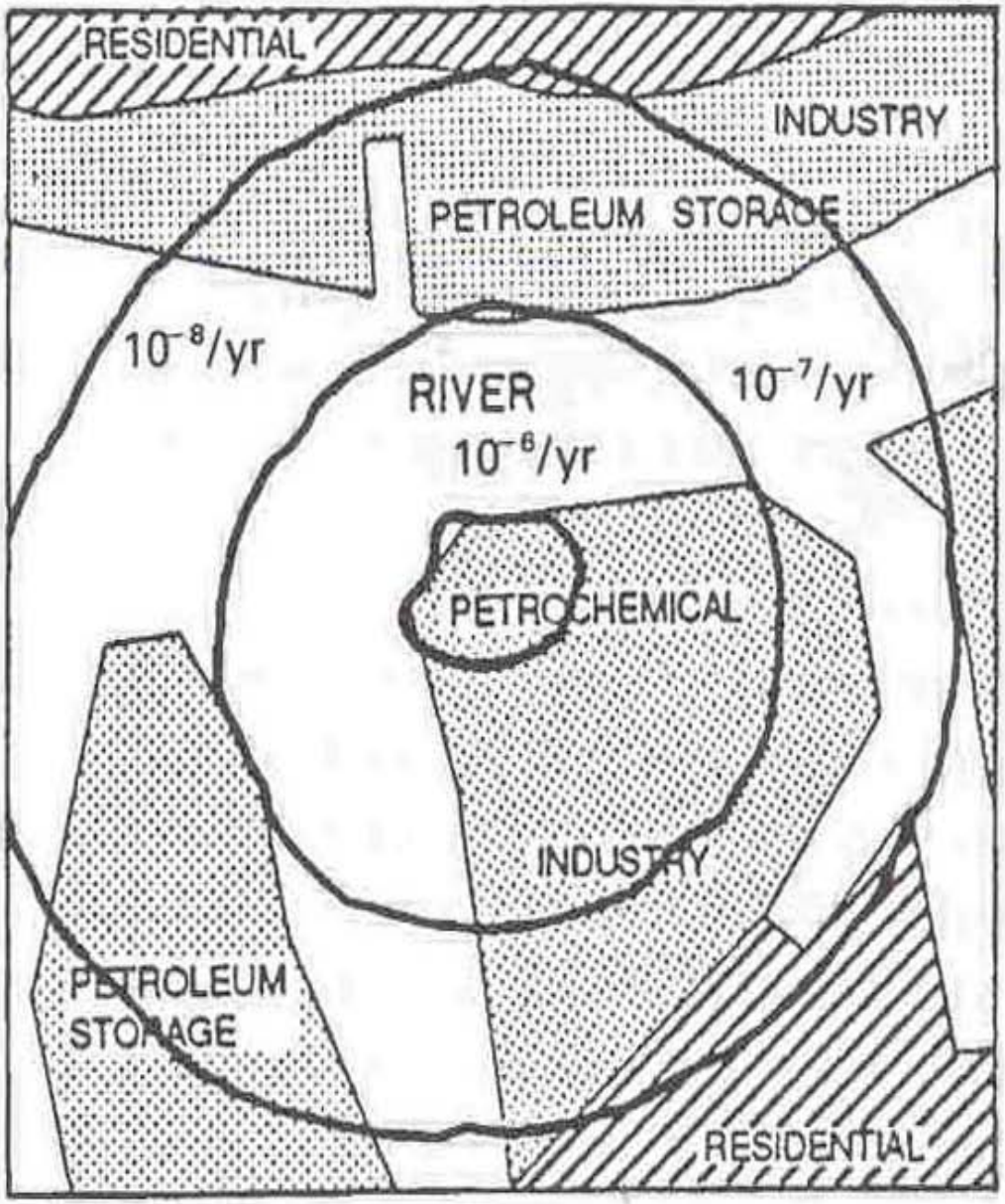


FIGURE 4.2. Example of an individual risk contour plot. Note: The contours connect points of equal individual risk of fatality, per year.

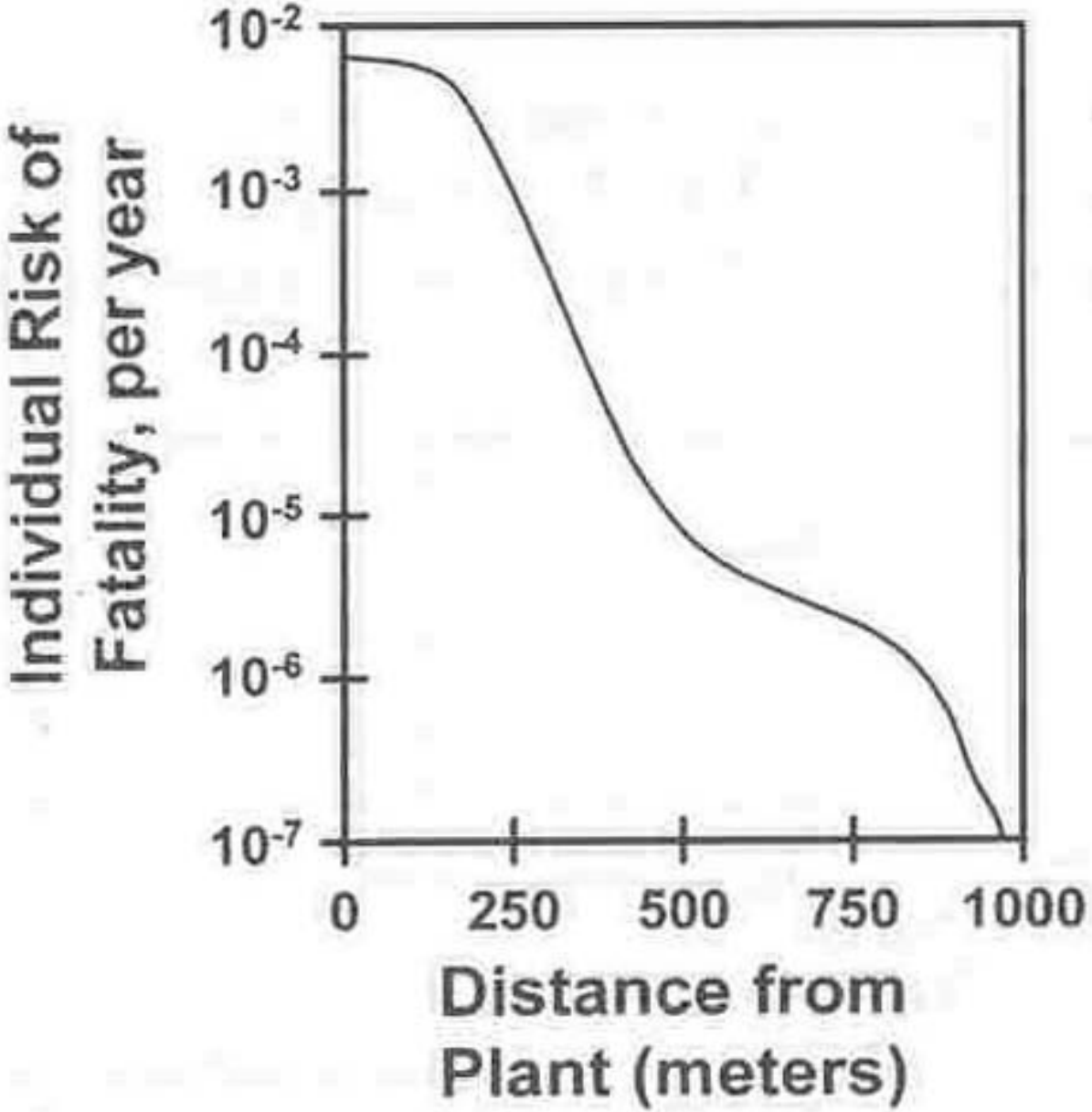


FIGURE 4.3. Example of an individual risk profile, or risk transect.

- Societal risk
  - Addresses the number of people who might be affected by hazardous incidents
  - Common form of societal risk is known as an F-N curve (frequency-number)
  - F-N curve
    - A plot of cumulative frequency versus consequences
  - Figure 4.4
    - Sample F0N curve for a single liquefied flammable gas facility

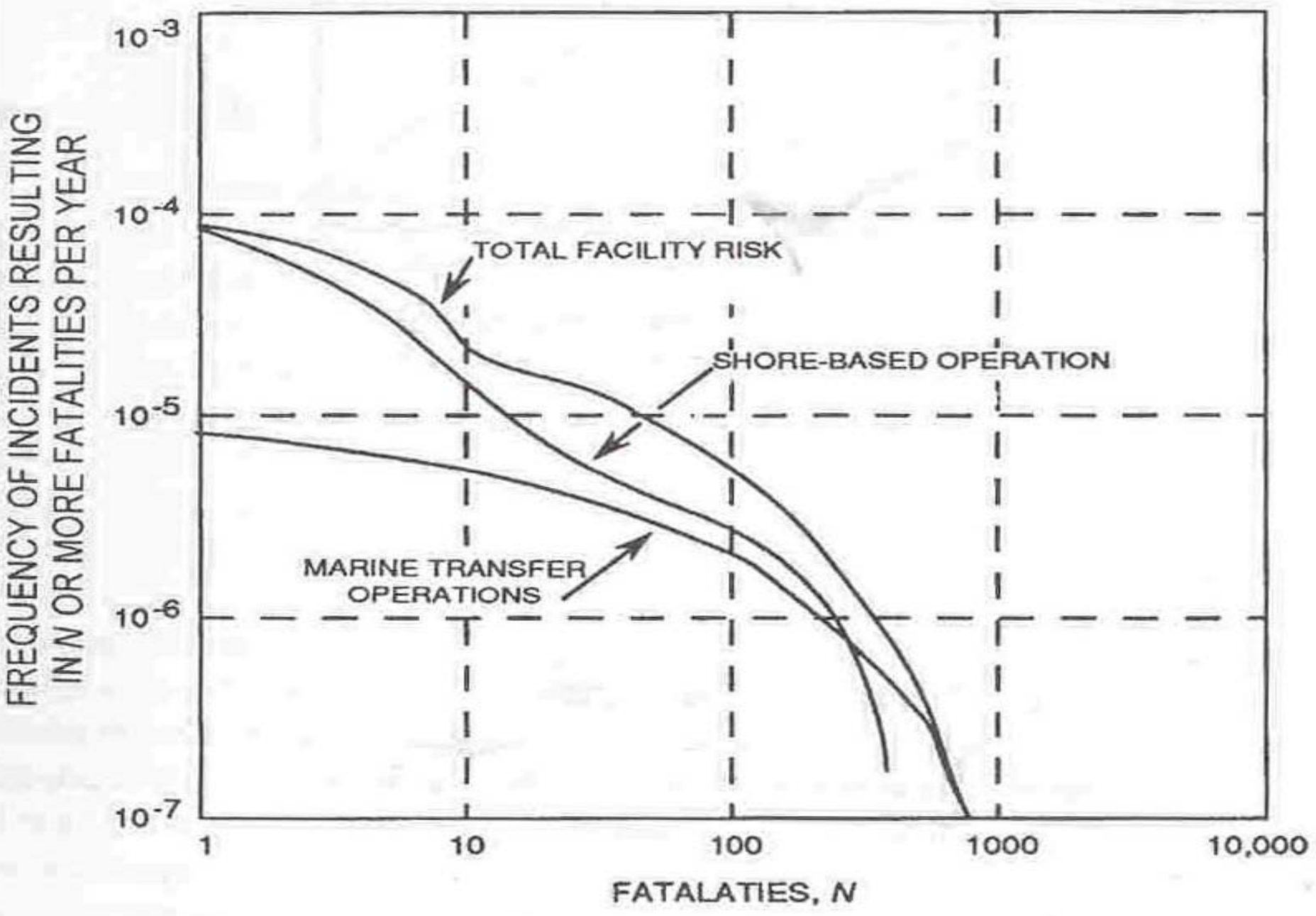


FIGURE 4.4. Example of a societal risk F-N curve.

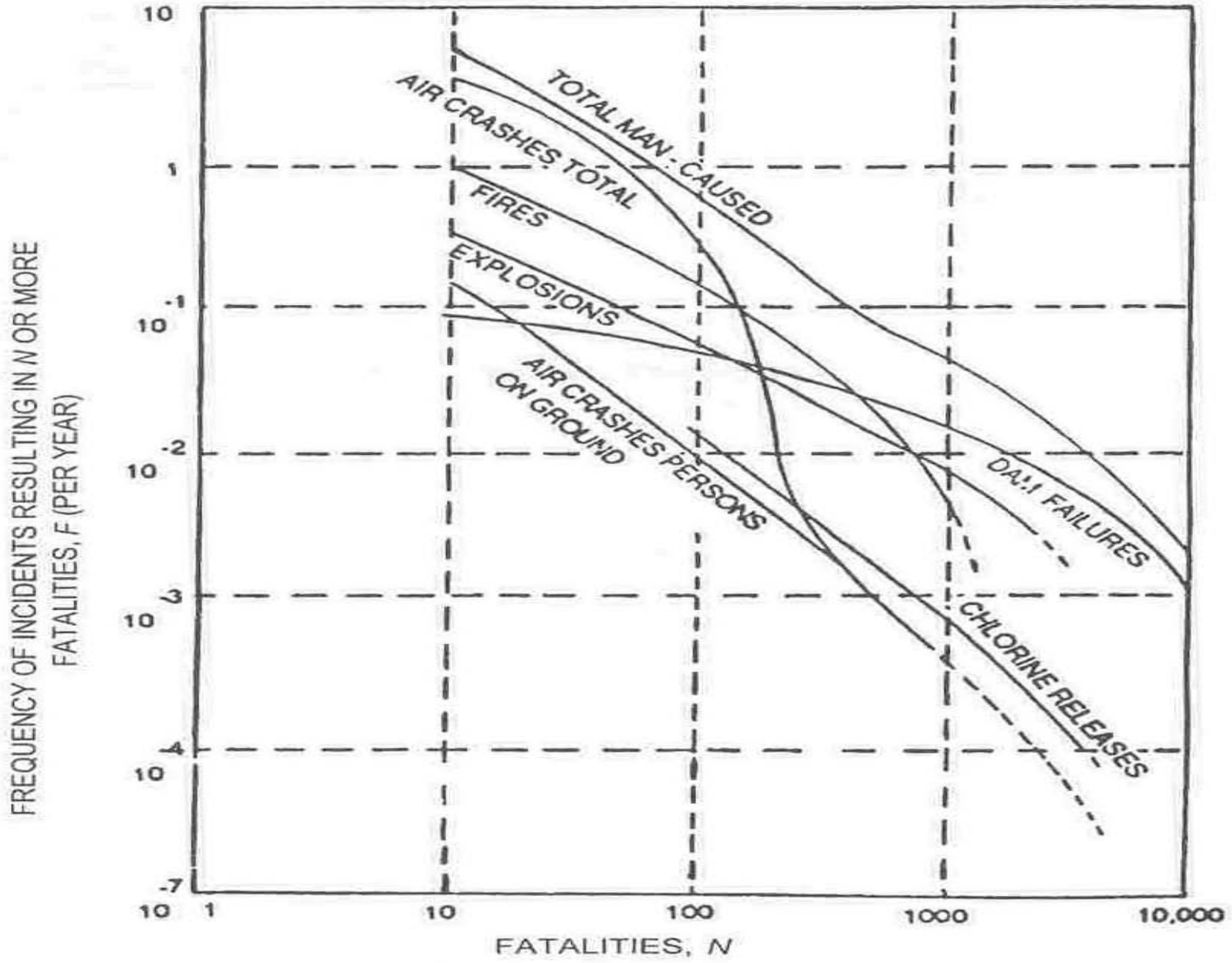


FIGURE 4.5. Some examples of U.S. societal risk estimates. From Rasmussen (1975).