22.38 PROBABILITY AND ITS APPLICATIONS TO RELIABILITY, QUALITY CONTROL AND RISK ASSESSMENT

Fall 2005, Lecture 1

RISK-INFORMED OPERATIONAL DECISION MANAGEMENT (RIODM): RISK, EVENT TREES AND FAULT TREES

Michael W. Golay
Professor of Nuclear Engineering
Massachusetts Institute of Technology

RISK AND THE MASSACHUSETTS LOTTERY

Most Tickets Cost \$1.00

Each Ticket Type Has a Unique

- Payoff Amount
- PSuccess

For a Single Lottery Ticket of Type i, the Expected Payoff, $\langle \$ \rangle_i$, is

$$\langle \$ \rangle_i = \text{Prob.-Success}_i * \text{Payoff}_i = P_i \cdot \$_i$$

For a Portfolio of N Lottery Tickets, the Expected Payoff, $\langle \$ \rangle$, is

$$\langle \$ \rangle = \sum_{\substack{i=1 \\ \text{Portfolio}}}^{N} \langle \$ \rangle_i = \sum_{\substack{i=1 \\ \text{Portfolio}}}^{N} P_i \$_i$$

DEFINITION OF RISK

Event Risk ≡ Vector (Set) of Expected Consequences From an Event

For an Event of Type i, the Associated Risk Vector, $\vec{R}_i$,

$\vec{R}_i = \langle \vec{C}_i \rangle$ = (Probability of Event, i) * (Set of Consequences of Event, i)

= [(Frequency of Event, i) * (Time Interval of Interest)] * (Set of Consequences of Event, i)

CORE DAMAGE RISK DUE TO N DIFFERENT CORE DAMAGE EVENTS

$$\vec{R}_{total} = \sum_{i=1}^{N} \vec{R}_i = \sum_{i=1}^{N} p_i \begin{bmatrix} \text{Consequence}_{1,\,i} \\ \Downarrow \\ \text{Consequence}_{M,\,i} \end{bmatrix}$$

Total Risk is the Sum Over All Possible Events of the Risks Associated with Each Event, Respectively

RISK CALCULATION

$$\overrightarrow{\overline{\text{Risk}}} = \sum_{\substack{i,\ \text{All Event} \\ \text{Sequences}}} \overline{C}_i p_i = \langle \overline{C} \rangle = \begin{bmatrix} \langle C_a \rangle \\ \langle C_b \rangle \\ \downarrow \\ \langle C_n \rangle \end{bmatrix}$$

$\overline{C}_i$ = Vector of consequences associated with the i^{th} event sequence

p_i = Probability of the i^{th} event sequence

$\langle \overline{C} \rangle$ = Mean, or expected, consequence vector

$\langle C_a \rangle$ = Mean, or expected, consequence of type a, summed over all event sequences

EXAMPLE

$$\overline{C}_i = \begin{bmatrix} \text{Offsite acute fatalities due to event i} \\ \text{Offsite latent fatalities due to event i} \\ \text{Onsite acture fatalities due to event i} \\ \text{Onsite latent fatalities due to event i} \\ \text{Offsite property loss due to event i} \\ \text{Onsite property loss due to event i} \\ \text{Costs to other NPPs due to event i} \end{bmatrix}$$

MAJOR LOGIC TOOLS USED IN PRA

<u>Event Tree</u> (ET)

To Determine the Probability of a Particular Event

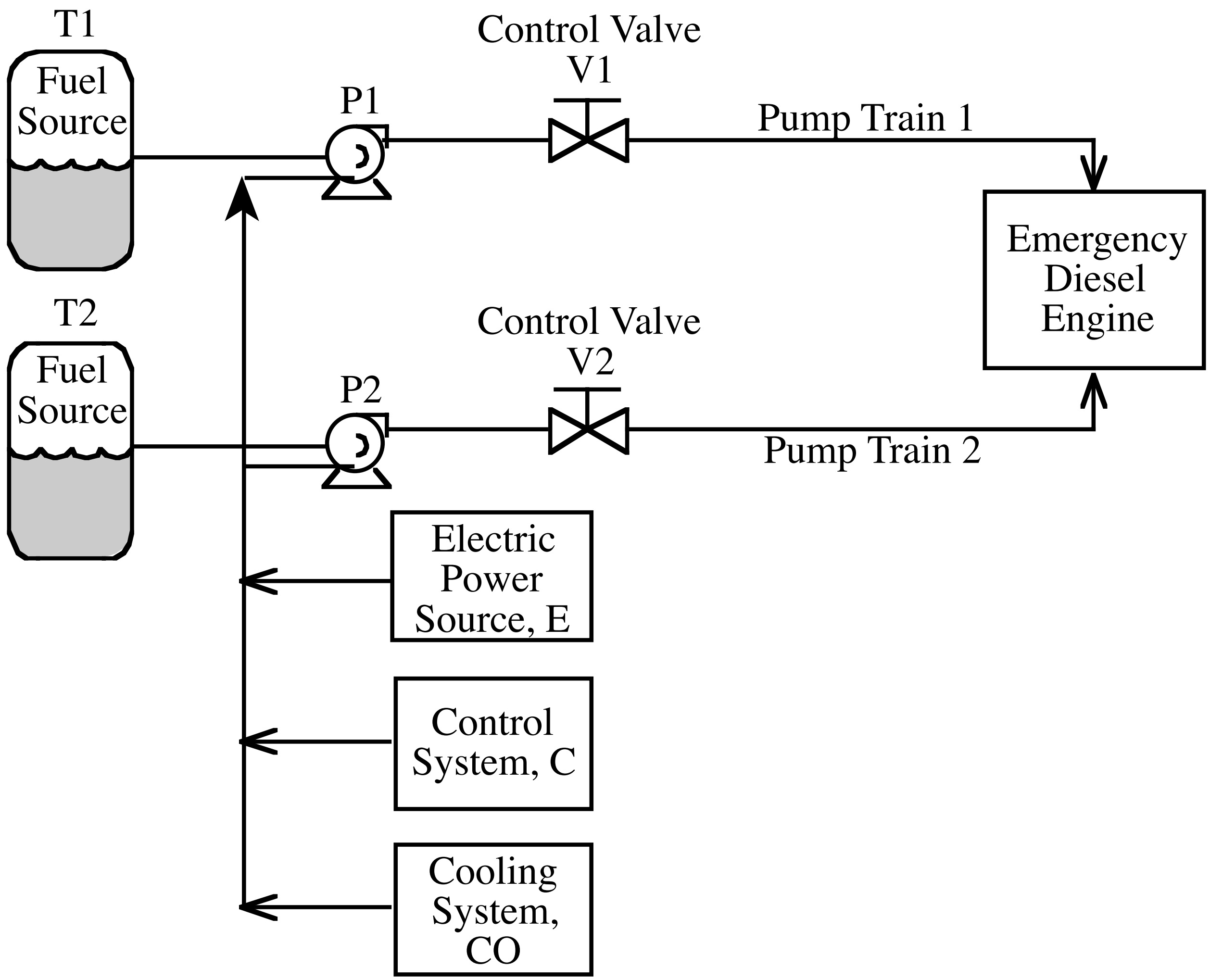
or

To Explicitly Determine Risk Contributors

<u>Fault Tree</u> (FT)

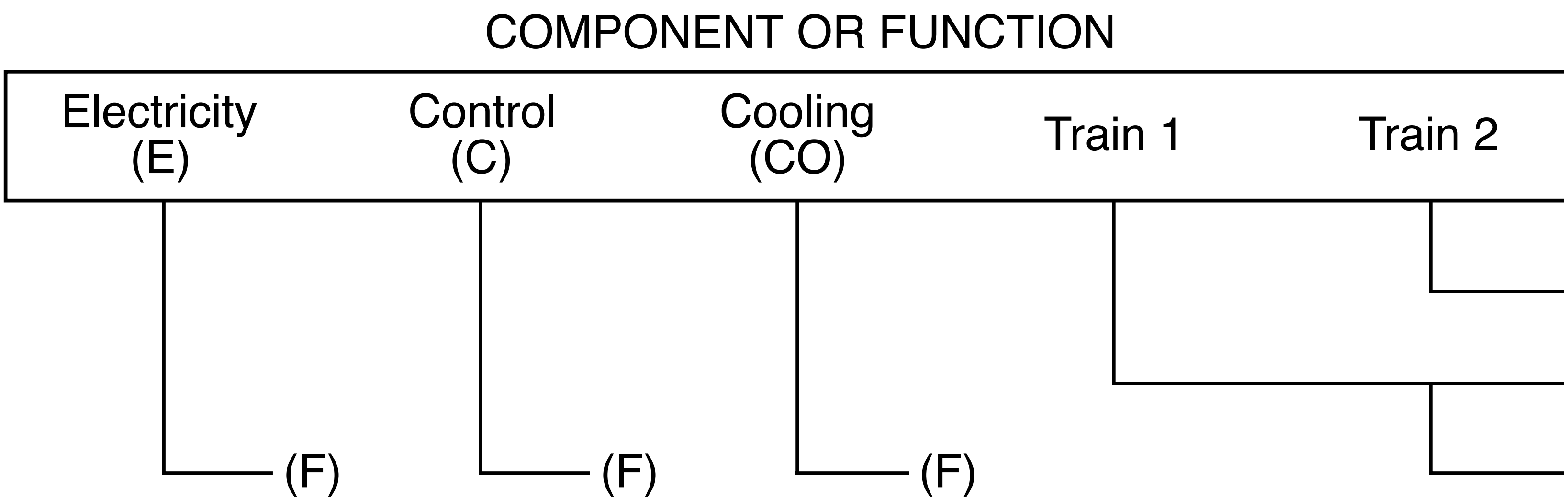
To Determine Failure Probabilities
For Use in Event Trees

AN EXAMPLE OF A FUEL PUMPING SYSTEM

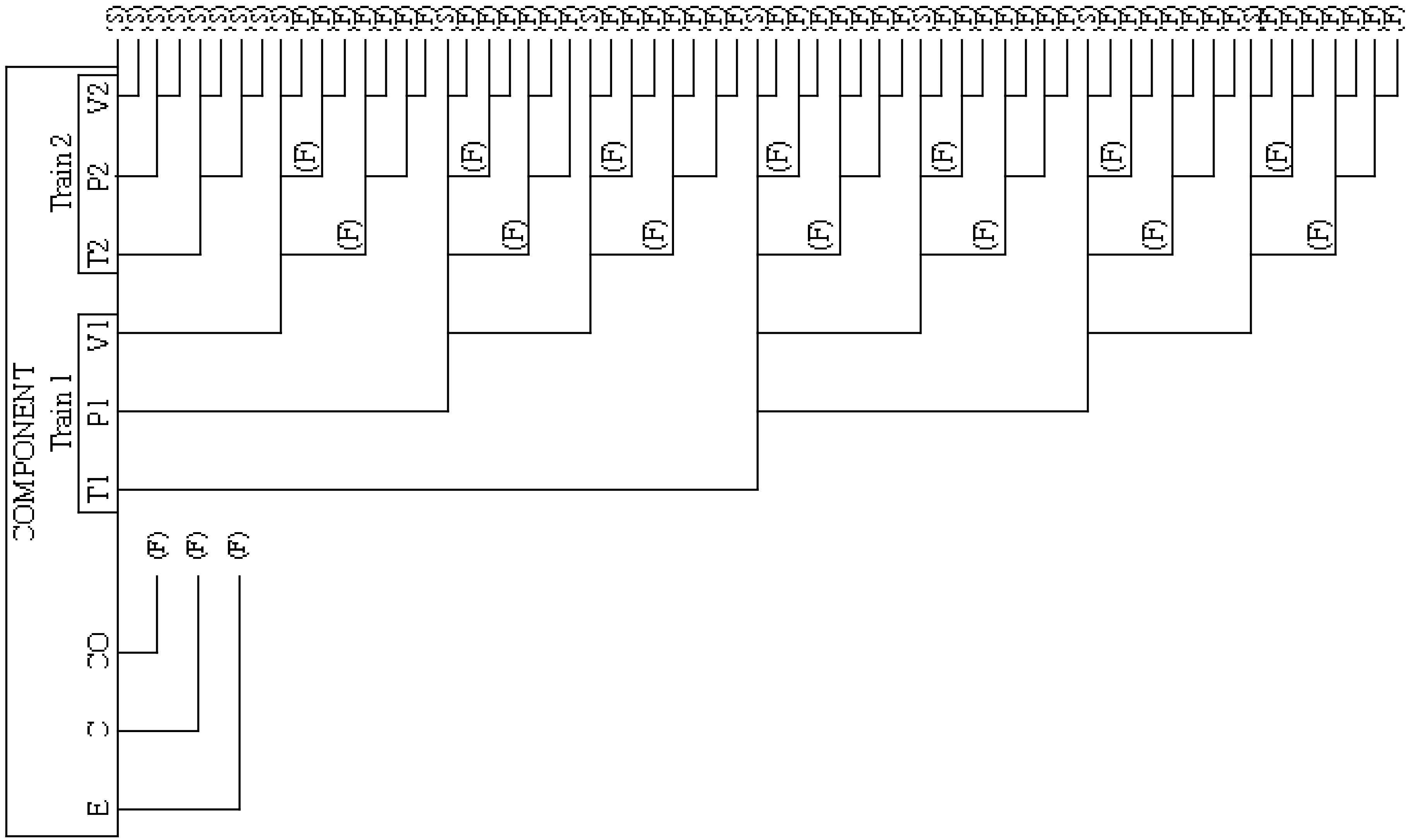


The System Succeeds if Fuel is Provided by Either Train 1 or 2.

FUEL INJECTION SYSTEM EVENT TREE

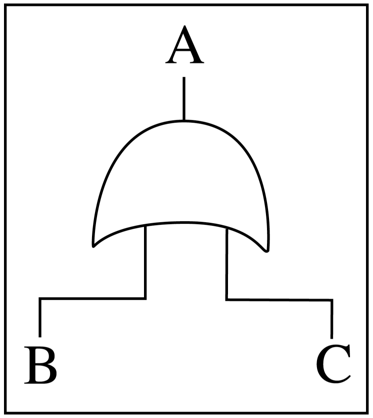


FUEL INJECTION SYSTEM EVENT TREE



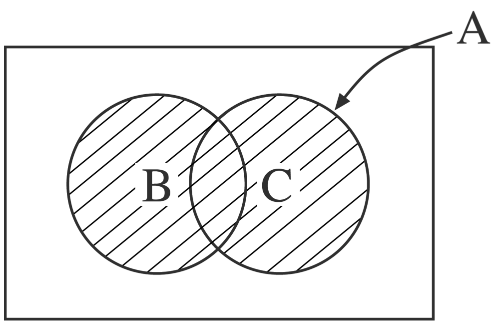
FAULT TREE LOGIC SYMBOLS ("GATES")

Operation, OR

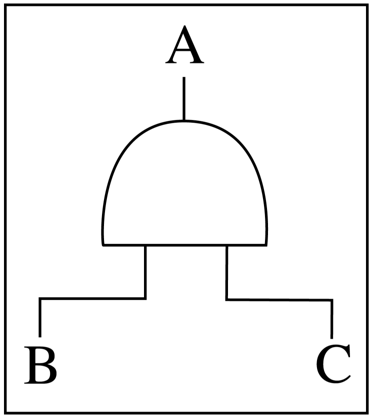


Meaning:

Event A occurs when either event B or C occurs



Operation, AND



Meaning:

Event A occurs when both event B and C occur

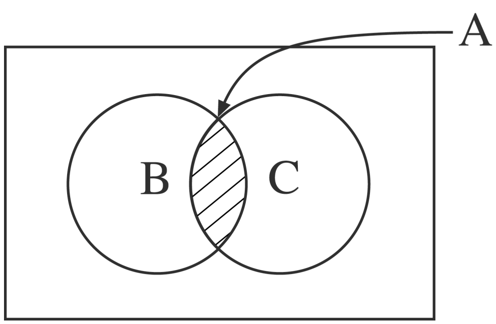
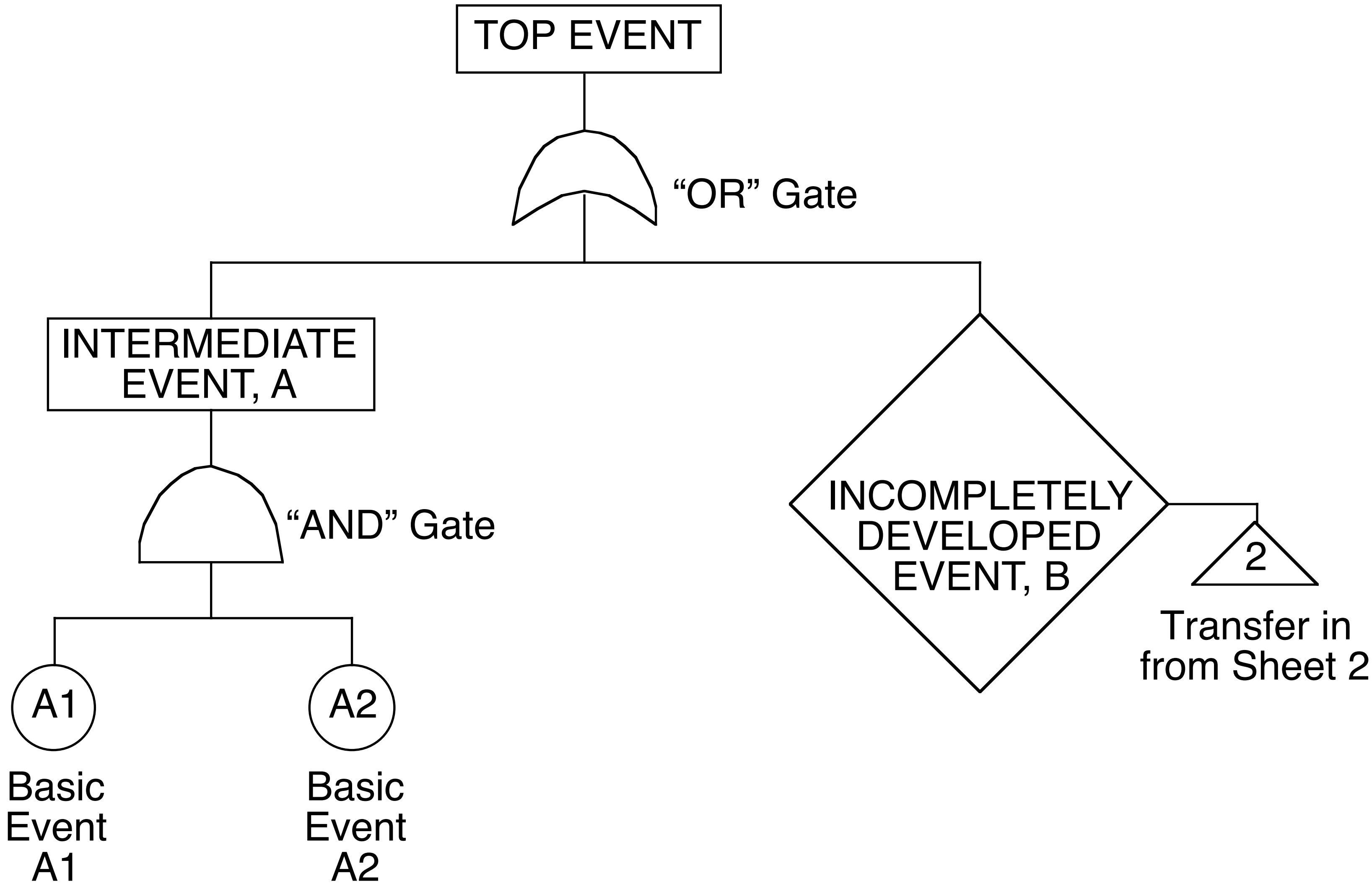
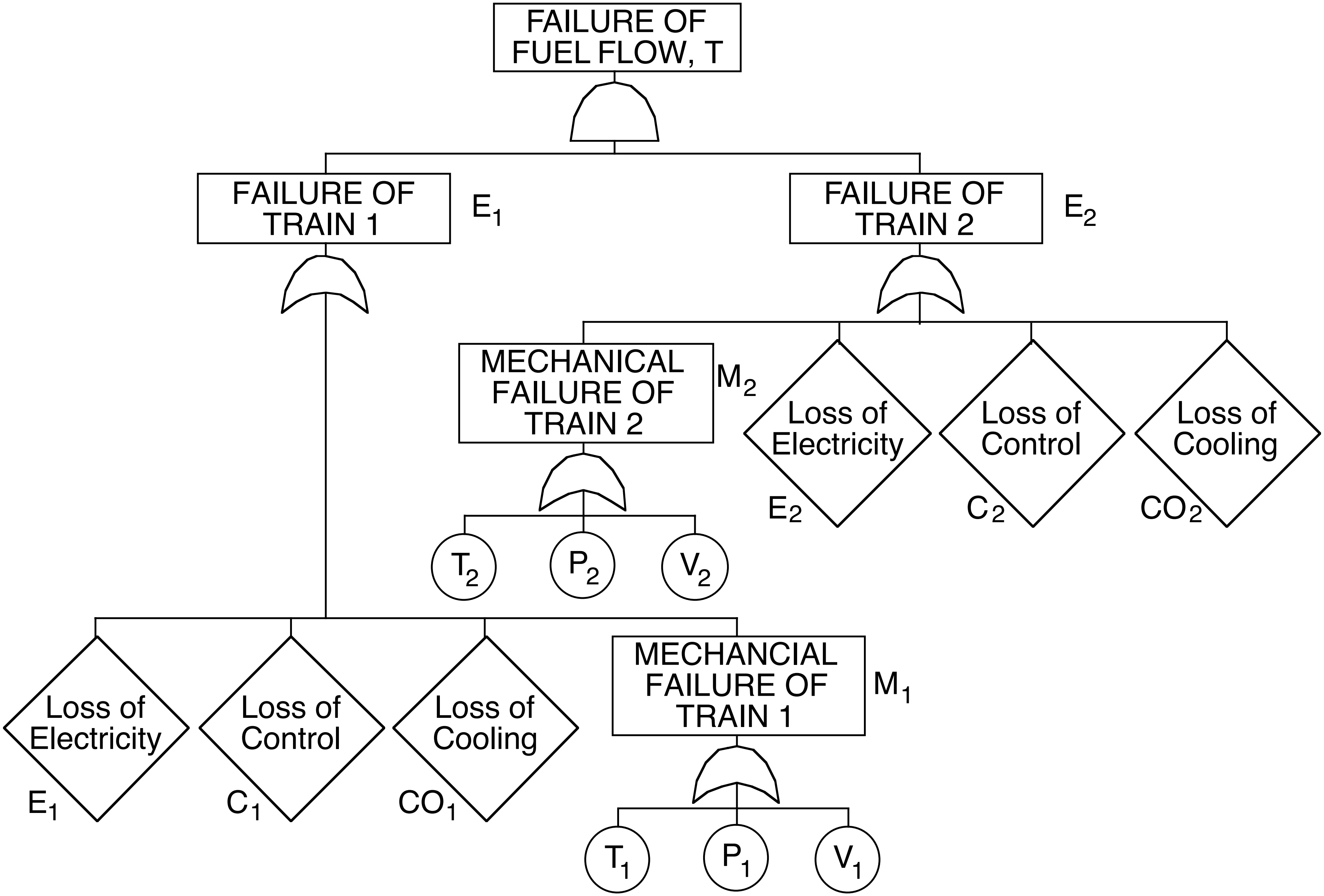


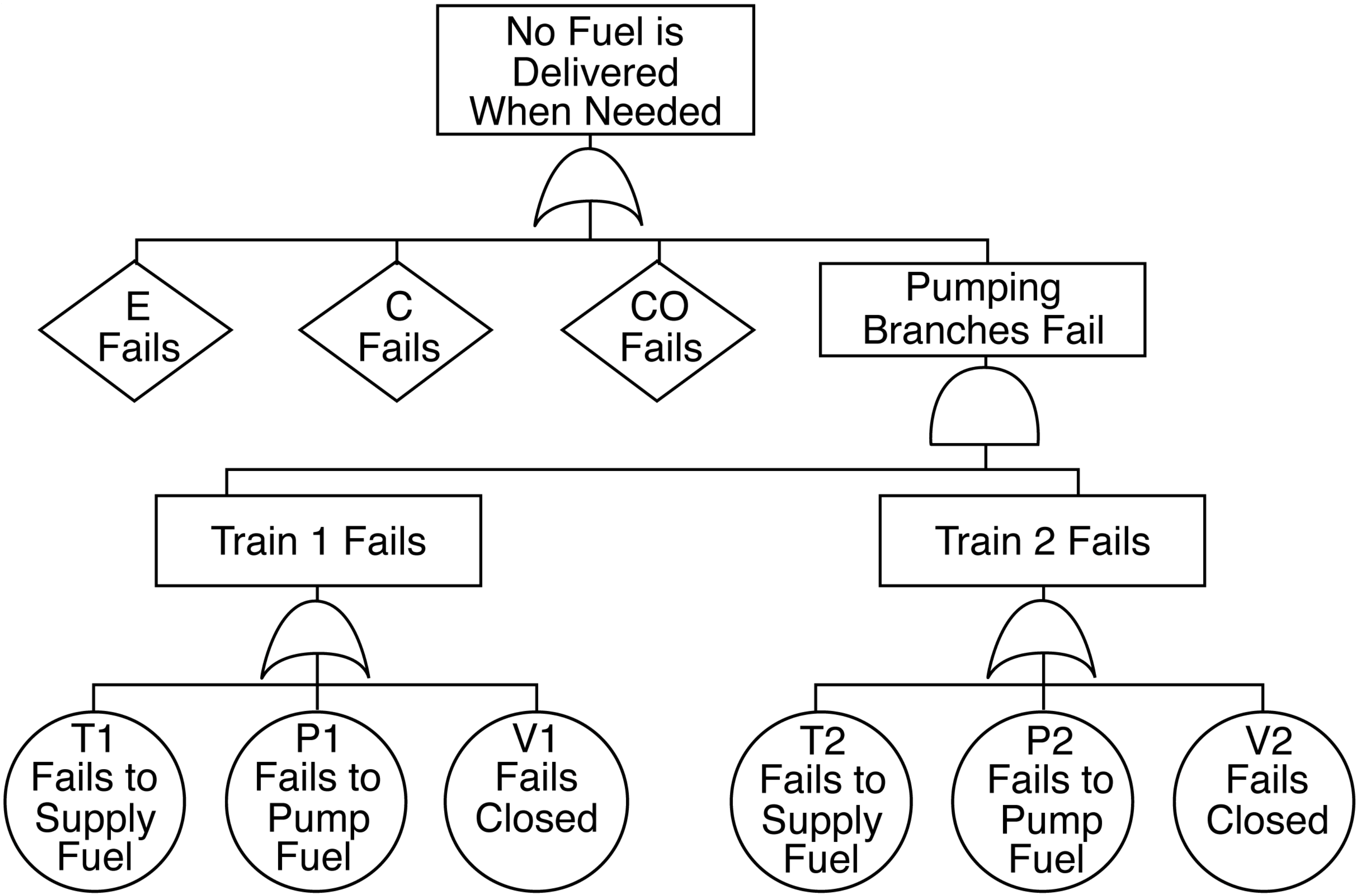
ILLUSTRATION OF ELEMENTS OF A FAULT TREE



FUEL PUMPING SYSTEM FAULT TREE

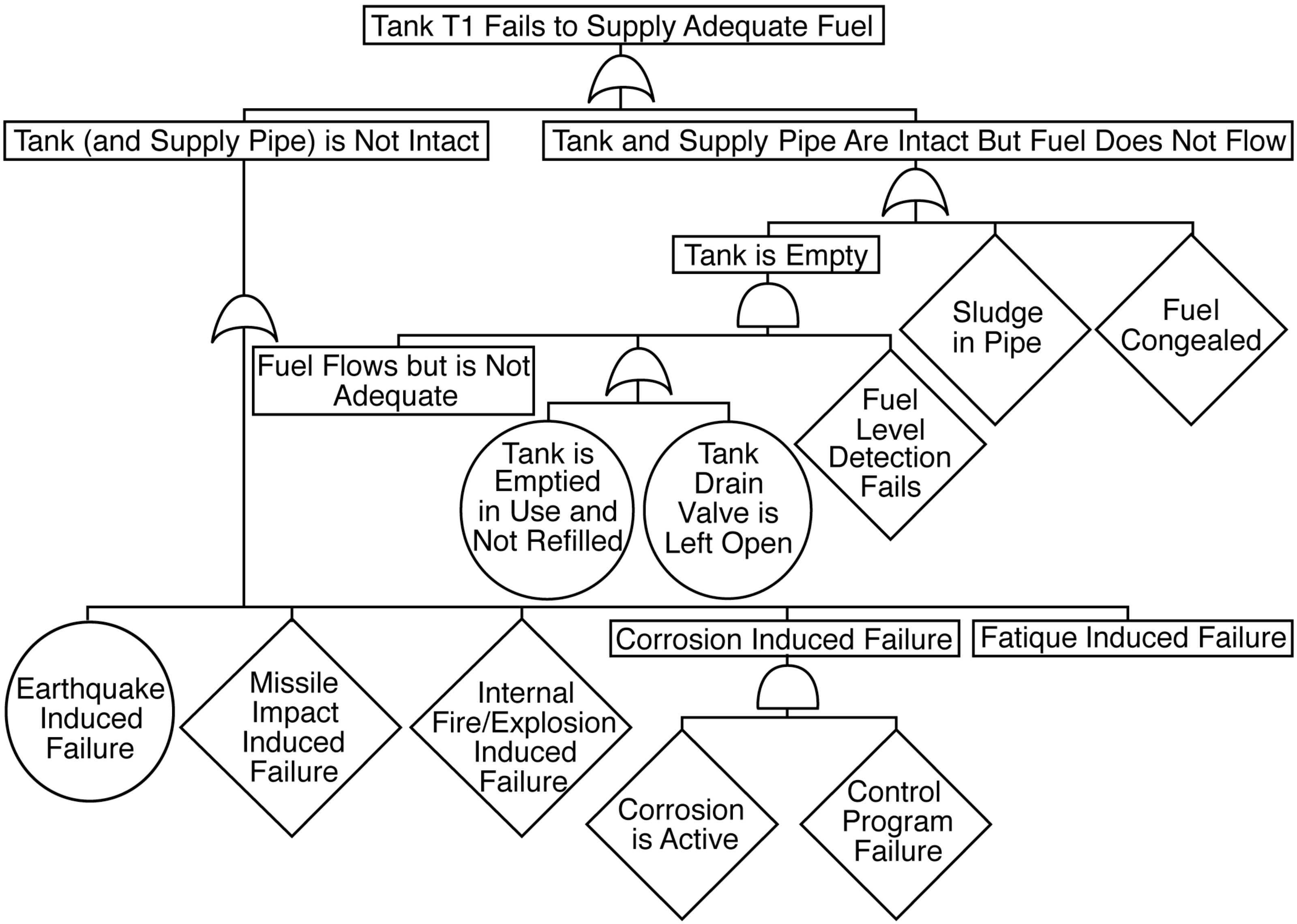


SIMPLIFIED FAULT TREE FOR THE FUEL PUMPING SYSTEM



NOTE: Prob.(E1·E2) = Prob.(E2|E1·Prob.(E1) = Prob. (E1)

FAULT TREE FOR TOP EVENT: TANK T1 FAILURE



CUT SETS AND MINIMAL CUT SETS

CUT SET: A cut set is any set of failures of components and actions that will cause system failure.

MINIMAL CUT SET (MCS): A minimal cut set is one where failure of <u>every</u> set element is necessary to cause system failure. A minimal cut set does not contain more than one cut set.

$$\text{Top Event, } T = \bigcup_{i-1}^{N} \left(MCS_i\right)$$

PUMPING SYSTEM EXAMPLE
MINIMAL CUT SETS

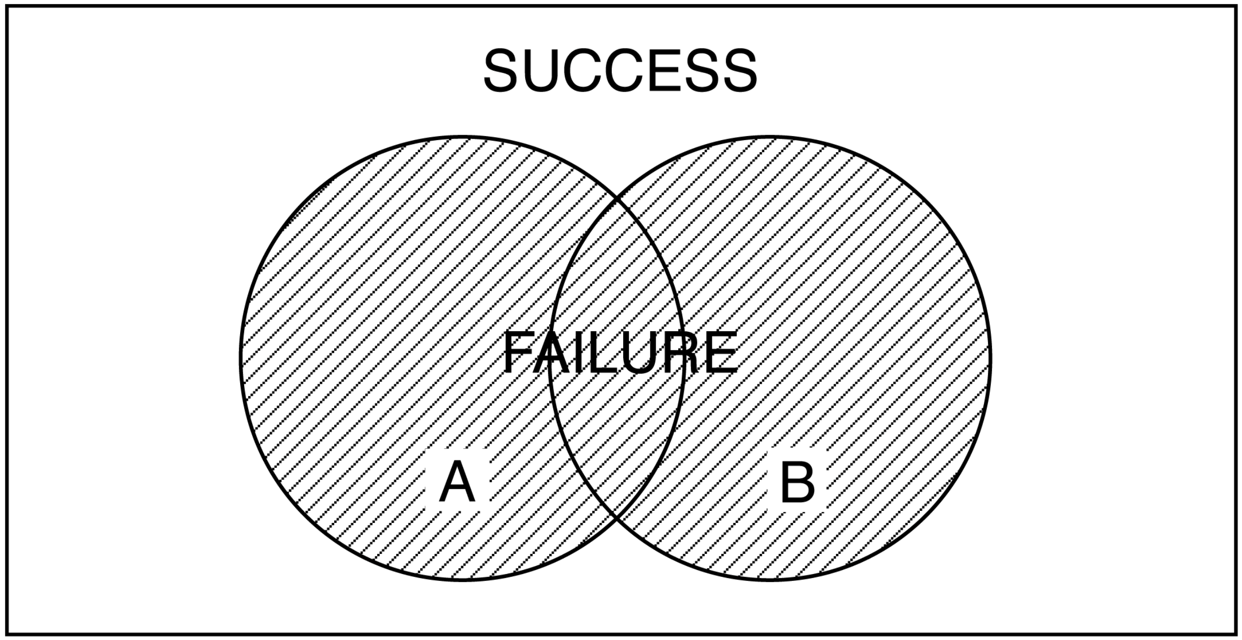
$$\text{Any Binary Combination of an Element of } \underbrace{\begin{bmatrix} \text{T1, Tank} \\ \text{P1, Pump} \\ \text{V1, Valve} \end{bmatrix}}_{\text{Train 1}} \text{ and of } \underbrace{\begin{bmatrix} \text{T2, Tank} \\ \text{P2, Pump} \\ \text{V2, Valve} \end{bmatrix}}_{\text{Train 2}}$$

$$\left.\begin{array}{ll} \text{C} & \text{Control System} \\ \text{E} & \text{Electric Power Source} \\ \text{CO} & \text{Cooling System} \end{array}\right\} \text{Dependent Failure of Pumping Train 1 and 2}$$

Failure of Any Minimal Cut Set Will Result in System Failure

MINIMAL CUT SETS OF THE HUMAN BODY

CONSIDER SYSTEM MINIMAL CUTS SETS A & B



$$\text{Prob.}(\text{Failure}) = \text{Prob.}_A + \text{Prob.}_B - \text{Prob.}(A \cdot B)$$
$$= \text{Prob.}_A + \text{Prob.}_B - \left[\text{Prob.}\ (B/A)\ \text{Prob.}_A\right]$$
$$= \text{Prob.}_A + \text{Prob.}_B - \left(\text{Prob.}_A \cdot \text{Prob.}_B\right)$$

if A & B are independent

For a good system : Prob._A, $\text{Prob.}_B << 1$, and $\text{Prob.}_A \cdot \text{Prob.}_B << \text{Prob.}_A$ or Prob._B, and

$\text{Prob.}(\text{Failure}) \leq \text{Prob.}_A + \text{Prob.}_B$, (rate event approximation)

SYSTEM MINIMAL CUT SETS

E

C

CO

Train 1 • Train 2

SYSTEM CUT SETS

All possible combinations of the minimal cut sets, from

E, C, CO, (Train 1 • Train 2) to

[E • C • CO • Train 1 • Train 2]

The top event, T, is the union of the minimal cut sets. The top event probability is the probability of the union of the minimal cut sets, (mcs_i)

$$\text{Prob.}(T) = \text{Prob.}\left(mcs_1 + mcs_2 + \cdots + mcs_N\right)$$

ILLUSTRATION OF DECOMPOSITION OF TOP EVENT INTO THE UNION OF THE MINIMAL CUT SETS

$$T = E_1 \cdot E_2 \tag{1}$$

$$E_1 = E + C + CO + M_1 \tag{2}$$

$$E_2 = E + C + CO + M_2 \tag{3}$$

$$M_1 = T_1 + P_1 + V_1 \tag{4}$$

$$M_2 = T_2 + P_2 + V_2 \tag{5}$$

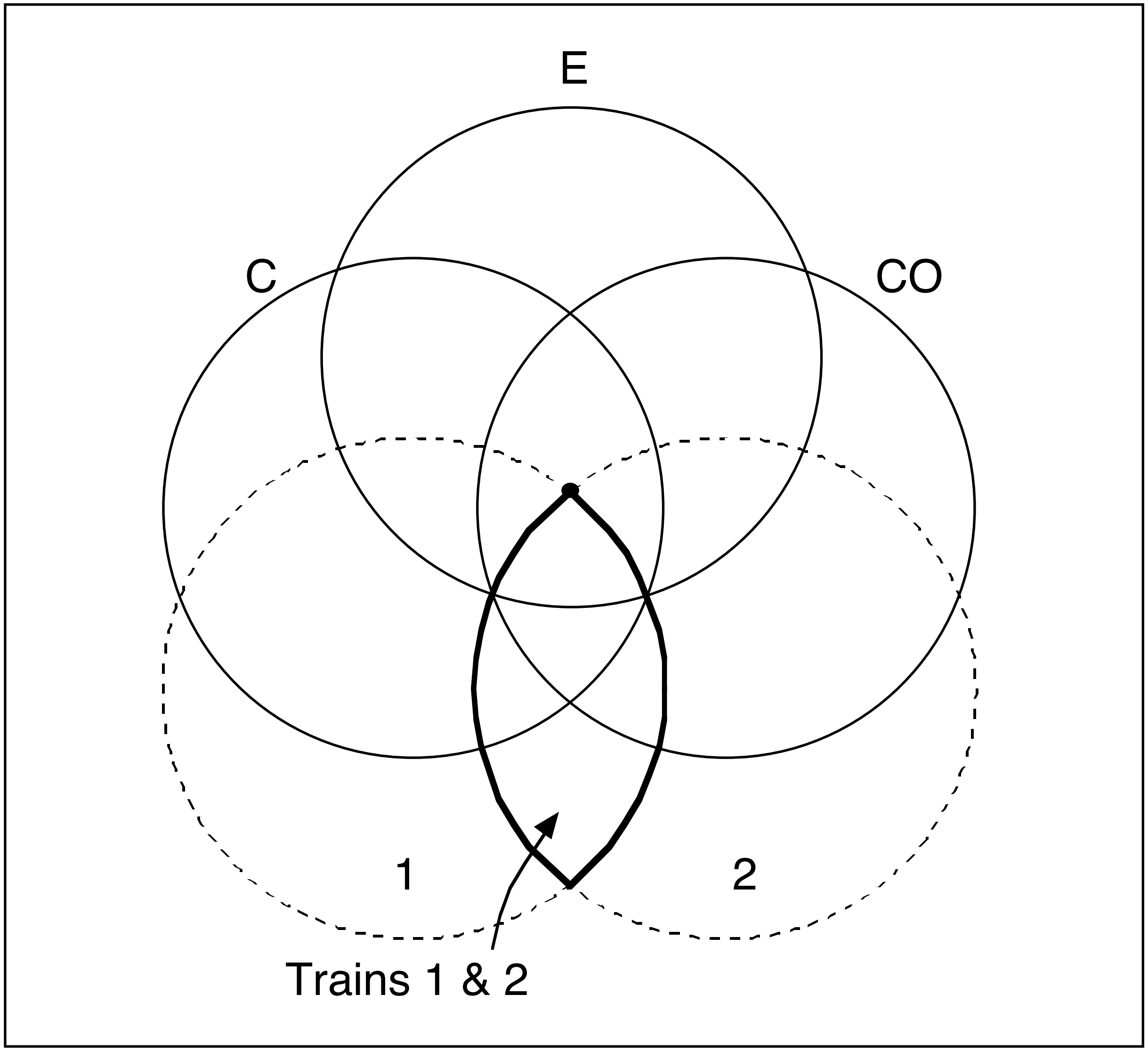
$$E_1 = E + C + CO + \left(T_1 + P_1 + V_1\right) \tag{6}$$

$$E_2 = E + C + CO + \left(T_2 + P_2 + V_2\right) \tag{7}$$

$$
\begin{aligned}
T &= \left[(E+C+CO)+\left(T_1+P_1+V_1\right)\right]\cdot\left[(E+C+CO)+\left(T_2+P_2+V_2\right)\right] \\
&= \underbrace{\underbrace{(E+C+CO)\cdot(E+C+CO)}_{(E+C+CO)}+(E+C+CO)\cdot\left[\left(T_1+P_1+V_1\right)+\left(T_2+P_2+V_2\right)\right]}_{(E+C+CO)\left\{\cancelto{1}{1+\left[\left(T_1+P_1+V_1\right)+\left(T_2+P_2+V_2\right)\right]}\right\}} \qquad (8) \\
&\quad +\underbrace{\left(T_1+P_1+V_1\right)\left(T_2+P_2+V_2\right)}_{\left[\begin{array}{l} T_1\cdot T_2+T_1\cdot P_2+T_1\cdot V_2 \\ +P_1\cdot T_2+P_1\cdot P_2+P_1\cdot V_2 \\ +V_1\cdot T_2+V_1\cdot P_2+V_1\cdot V_2 \end{array}\right]}
\end{aligned}
$$

$$
T=\left(E+C+CO\right)+\left[\begin{array}{l} T_1\cdot T_2+T_1\cdot P_2+T_1\cdot V_2 \\ +P_1\cdot T_2+P_1\cdot P_2+P_1\cdot V_2 \\ +V_1\cdot T_2+V_1\cdot P_2+V_1\cdot V_2 \end{array}\right]=\bigcup_{i=1}^{N}\left(MCS_i\right)
$$

VENN DIAGRAM FOR FUEL SYSTEM FAILURE



$$T = C + E + CO + (\text{Train } 1 \supseteq \text{Train } 2)$$

BOOLEAN ALGEBRA

Boolean algebra is employed in problems involving binary variable. A binary variable has only two values, denoted by "1" and "0," or "A" and "$\overline{A}$," or "true" and "false," or "high" and "low," or "switch closed" and "switch open," among other things. Since the two states can be captured in functional proportions, Boolean algebra is sometimes also called propositional calculus. In algebra involving binary states, the plus sign, "+," is used to denote the "or" function, and the multiplication sign, " $\cdot$," is used to denote the "and" function. These two signs are called *logical sum* and *logical product*, respectively. Naturally, the + and $\cdot$ signs used in this context will not follow conventional arithmetic rules. With this background, the following theorems are assembled here for easy reference: (from *Engineering Reliability*, R. Ramakumar)

$$1 \cdot 1 = 1 \tag{1}$$

$$(\cdot = \text{ intersection, } \cap, \ \wedge, \text{ and})$$

$$1 + 1 = 1 \tag{2}$$

$$1 \cdot 0 = 0 \tag{3}$$

$$1 + 0 = 1 \tag{4}$$

$$(+ = \text{ union, } \cup, \ \vee, \text{ or})$$

Let A, B, and C be Boolean variables. Then

$$A \cdot 1 = A \tag{5}$$

$$A + A = A \tag{6}$$

$$A \cdot 0 = 0 \tag{7}$$

$$A + 0 = A \tag{8}$$

BOOLEAN ALGEBRA (continued)

$$A \cdot A = A \tag{9}$$

$$A + 1 = 1 \tag{10}$$

$$A + \overline{A} = 1 \tag{11}$$

$$A \cdot \overline{A} = 0 \tag{12}$$

$$A + AB = A \tag{13}$$

$$A(A + B) = A \tag{14}$$

Associative law:
$$(A + B) + C = A + (B + C) \tag{15}$$

Associative law:
$$(AB)C = A(BC) \tag{16}$$

Cumulative law:
$$A + B = B + A \tag{17}$$

Cumulative law:
$$A \cdot B = B \cdot A \tag{18}$$

Distributive law:
$$A(B + C) = AB + AC \tag{19}$$

Distributive law:
$$A + BC = (A + B)(A + C) \tag{20}$$

Double complement:
$$\overline{\overline{A}} = A \tag{21}$$

DeMorgan's law:
$$\overline{A + B} = \overline{A}\,\overline{B} \tag{22}$$

DeMorgan's law:
$$\overline{AB} = \overline{A} + \overline{B} \tag{23}$$

$$A + \overline{A}B = A + B \tag{24}$$

$$A\left(\overline{A} + B\right) = A \cdot B \tag{25}$$

$$(A + B)\left(\overline{A} + C\right) = AC + B \tag{26}$$

$$\left(AC + B\overline{C}\right) = \overline{A}C + \overline{B}\,\overline{C} \tag{27}$$

SUMMARY

- Risk is the Expected Consequence Vector of System Operation
- Risk Can Be Modeled via Combined Event and Fault Trees
- System Failure Consists of the Union of the System Minimal Cut Sets
- Prob. $(A \cdot B)$ = Prob.$(B|A)$ Prob.(A)