Engineering Risk Benefit Analysis

1.155, 2.943, 3.577, 6.938, 10.816, 13.621, 16.862, 22.82

ESD.72J, ESD.721

RPRA 1. The Logic of Certainty

George E. Apostolakis

Massachusetts Institute of Technology

Spring 2007

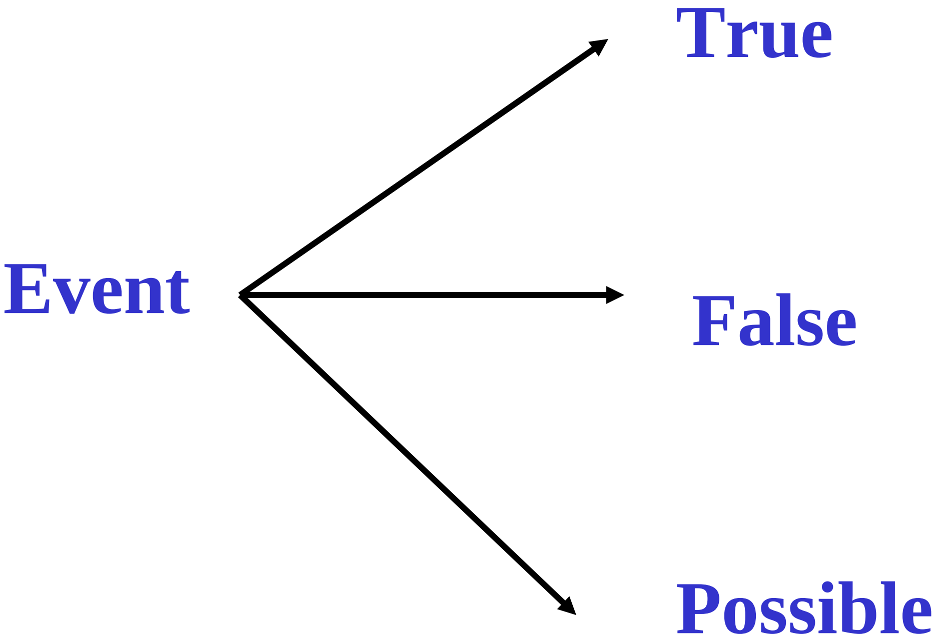
Event Definition

- ***Event:*** **A statement that can be true or false.**

- **"It may rain tonight" is not an event.**

- **According to our current state of knowledge, we may say that an event E is TRUE, FALSE, or POSSIBLE (UNCERTAIN).**

- **Eventually, E will be either TRUE or FALSE.**



Event

True

False

Possible

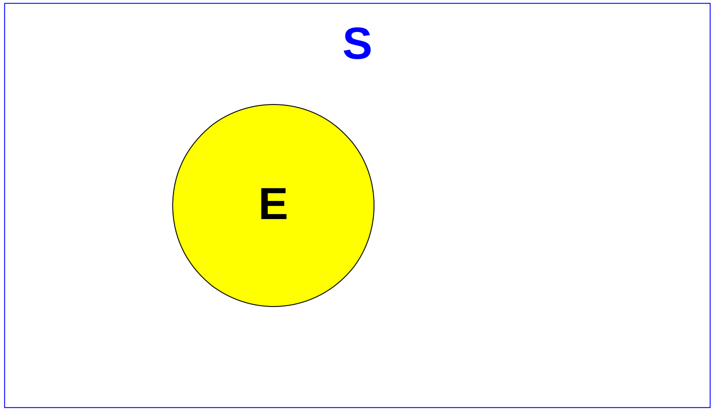
Venn Diagrams

- ***Sample Space:*** **The set of all possible outcomes of an experiment. Each elementary outcome is represented by a *sample point.***

- ***Examples*: Die {1,2,3,4,5,6}   Failure Time {0, ∞}**

- **A collection of *sample points* is an event.**

Venn Diagram

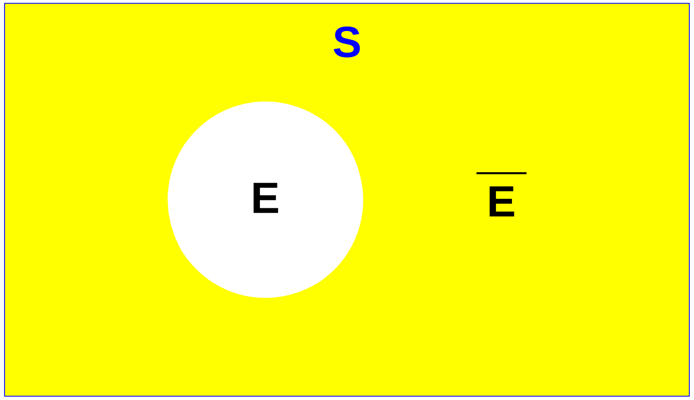


Indicator Variables

$$X_j = \begin{cases} 1, \text{ If } E_j \text{ is } T \\ 0, \text{ If } E_j \text{ is } F \end{cases}$$

Important Note: **$X^k = X$,   k: 1, 2, …**

Venn Diagram

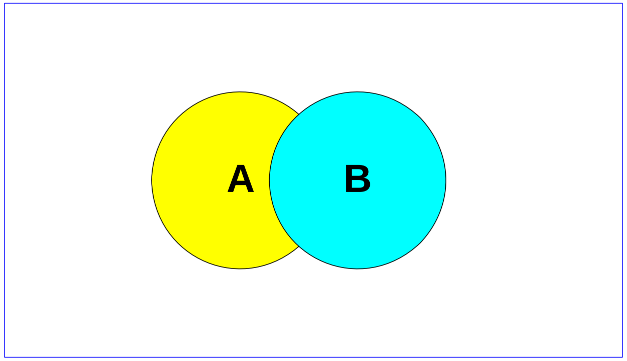


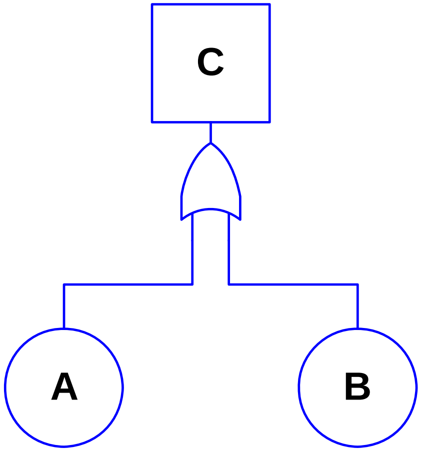
Union (OR operation)

$$A \cup B = C$$

$$X_C = 1 - (1 - X_A)(1 - X_B)$$

$$X_C \equiv \coprod X_j$$



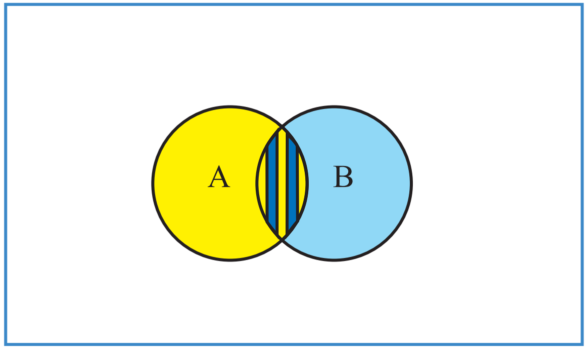


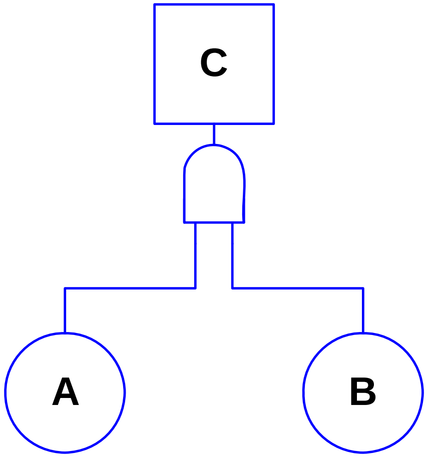
Intersection (AND operation)

$$A \cap B = C$$

$$X_C = X_A X_B$$

$$X_C \equiv \prod X_j$$

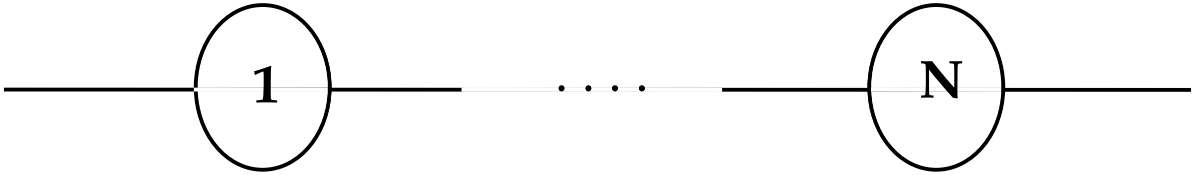


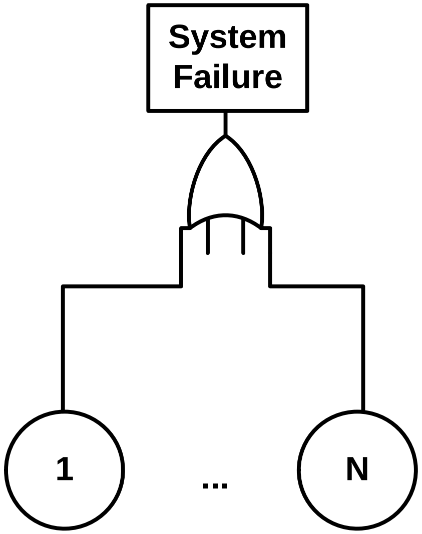


Mutually Exclusive Events: $A \cap B = \varnothing$

Simple Systems

Reliability Block Diagram for the Series System

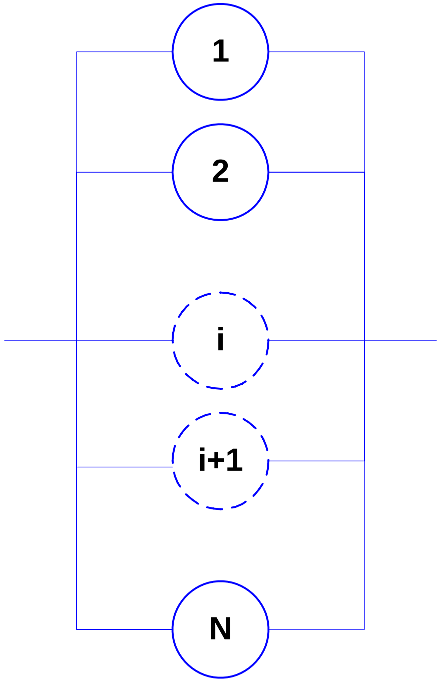




failure: $$X = 1 - \prod_{1}^{N} (1 - X_j) \equiv \coprod_{1}^{N} X_j$$

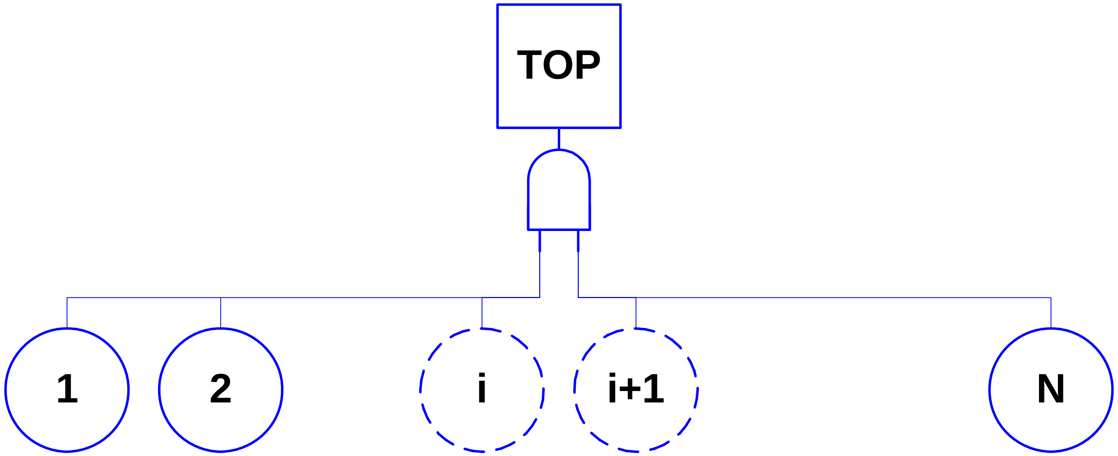
success : $$\mathbf{Y = \prod_{1}^{N} Y_j}$$

Reliability Block Diagram for the Parallel System

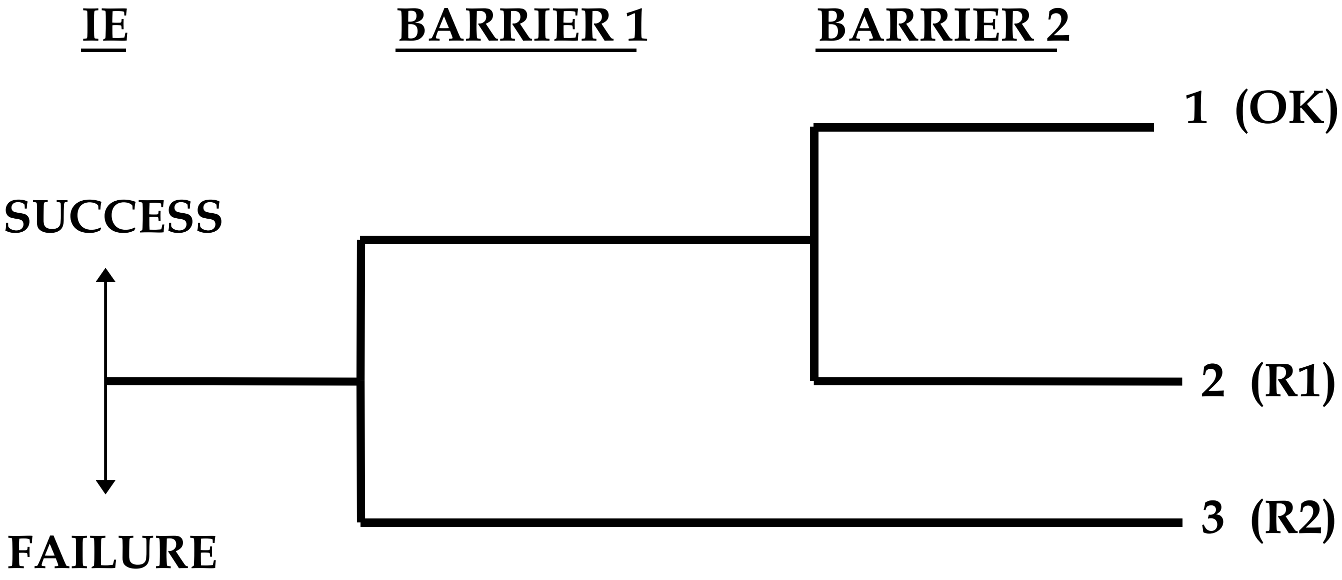


$$X = \prod_{1}^{N} X_j$$

$$Y = \coprod_{1}^{N} Y_j$$

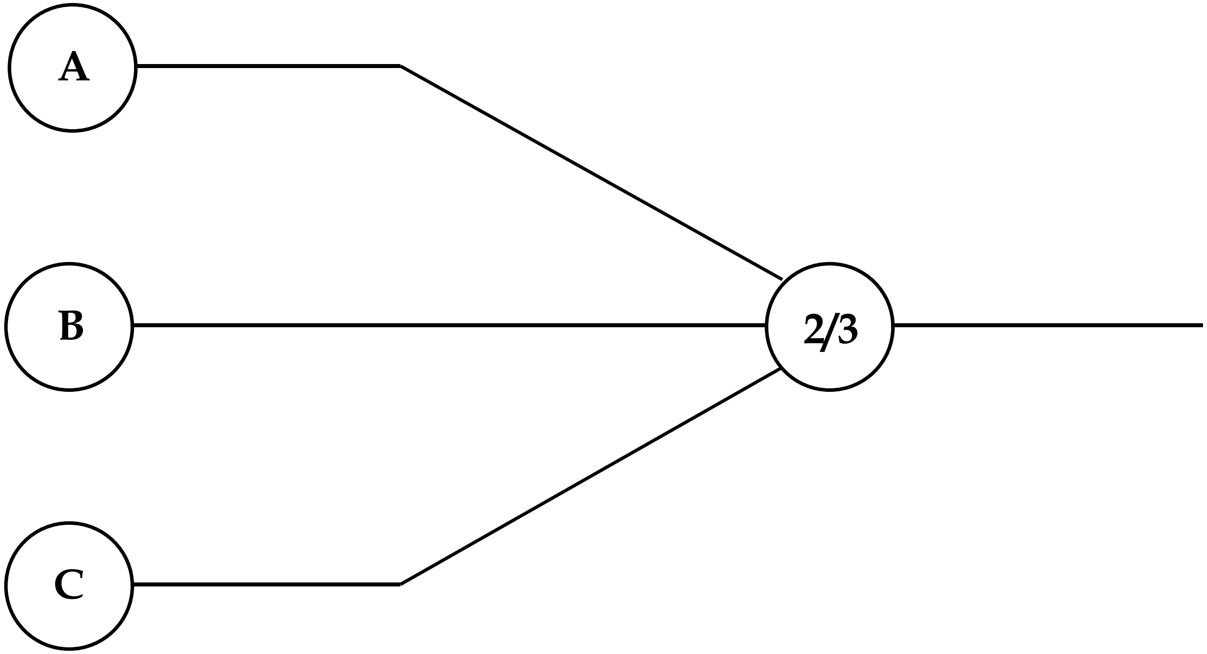


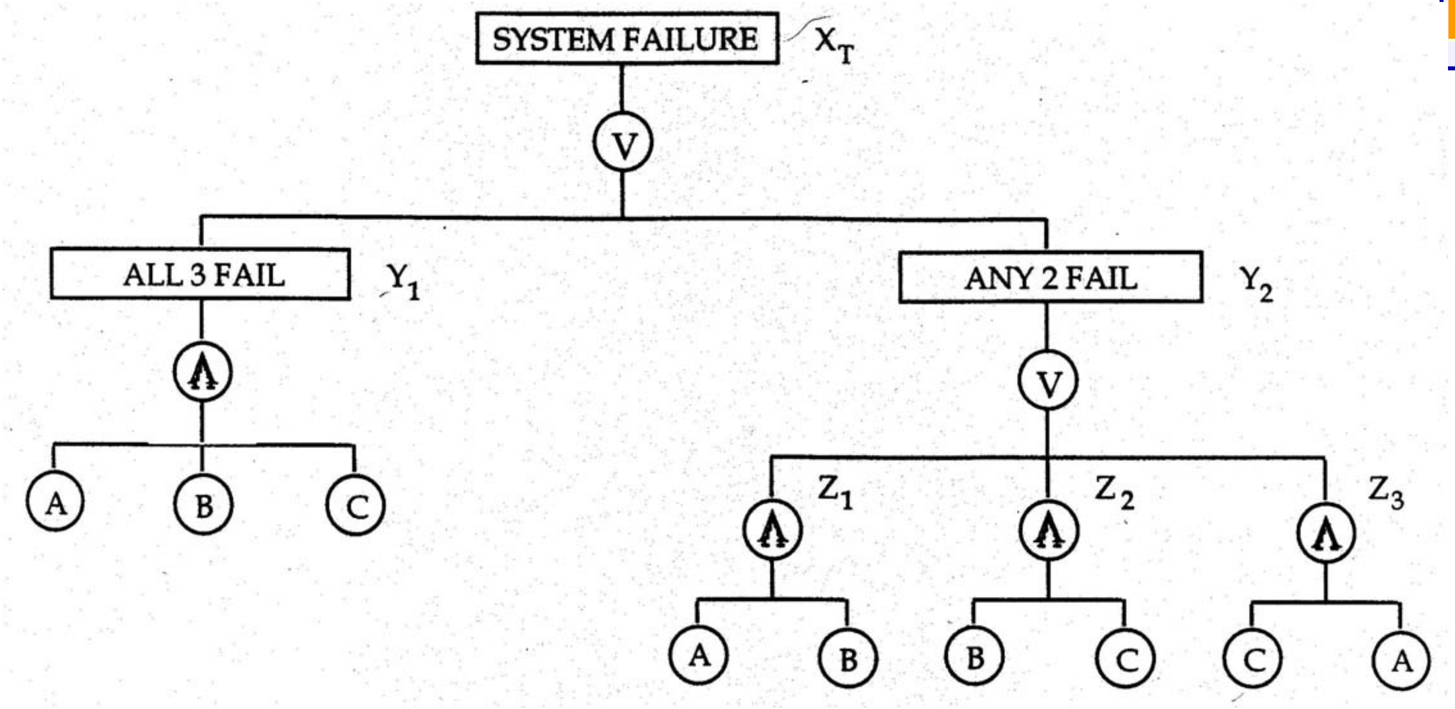
Event-Tree Analysis



Fault-Tree Analysis

Reliability Block Diagram for the 2-out-of-3 System





$$X_T = 1-(1-Y_1)(1-Y_2)$$
$$= 1-(1-X_A X_B X_C)\{1-[1-(1-Z_1)(1-Z_2)(1-Z_3)]\}$$
$$= 1-(1-X_A X_B X_C)\{1-[1-(1-X_A X_B)(1-X_B X_C)(1-X_C X_A)]\}$$

Expanding and using $\mathbf{X^k = X}$ we get

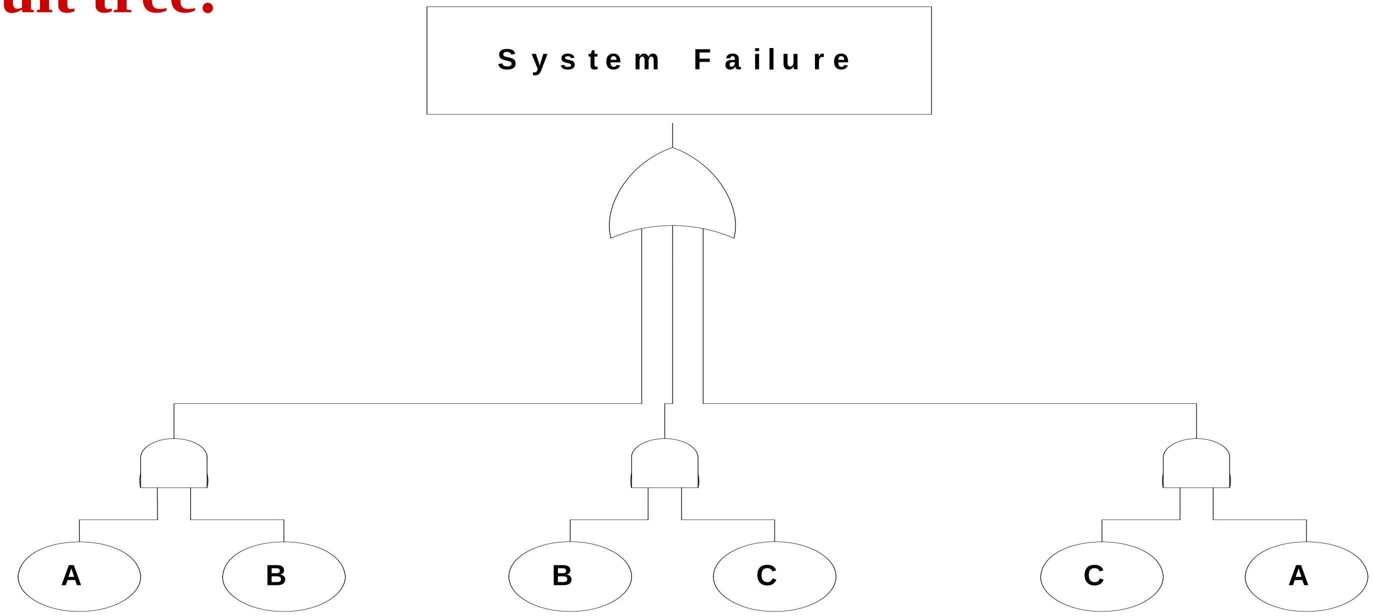
$$X_T = 1-(1-X_A X_B)(1-X_B X_C)(1-X_C X_A)$$

Cut sets and minimal cut sets

- ***CUT SET*: Any set of events (failures of components and human actions) that cause system failure.**

- ***MINIMAL CUT SET*: A cut set that does not contain another cut set as a subset.**

New fault tree:



Minimal cut sets:

$$M_1 = X_A X_{B,} \qquad M_2 = X_B X_C,, \qquad M_3 = X_C X_A$$

$$X_T = \coprod_{1}^{3} M_j \equiv 1-\left(1-M_1\right)\left(1-M_2\right)\left(1-M_3\right)=$$

$$=1-(1-X_A X_B)(1-X_B X_C)(1-X_C X_A)$$

$$X_T = \phi(X_1, X_2, \ldots X_n) \equiv \phi(\underline{X})$$

$\phi(\underline{X})$ is the <u>structure or switching function</u>.

It maps an n-dimensional vector of 0s and 1s onto 0 or 1.

<u>Disjunctive Normal Form</u>:

$$\mathbf{X_T = 1 - \prod_{1}^{N}(1 - M_i) \equiv \coprod_{1}^{N} M_i}$$

<u>Sum-of-Products Form</u>:

$$X_T = \sum_{i=1}^{N} M_i - \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} M_i M_j + \ldots + (-1)^{N+1} \prod_{i=1}^{N} M_i$$

For the 2-out-of-3 System:

$$X_T = 1-(1-X_A X_B)\,(1-X_B X_C)\,(1-X_C X_A)$$

$$X_T \;=\; (M_1+M_2+M_3) \;-\; (M_1M_2+M_2M_3+M_3M_1) \;+\; M_1M_2M_3$$

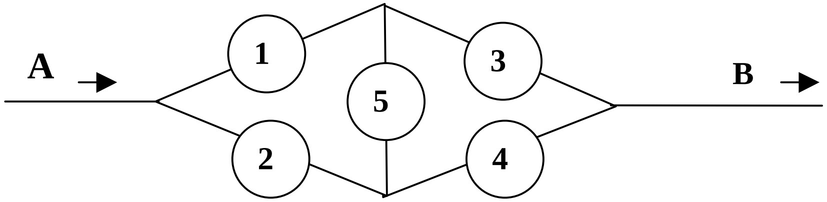
But,

$$M_1M_2 \;=\; X_A X_B^2 X_C \;=\; X_A X_B X_C$$

Therefore, the sum-of-products expression is:

$$X_T \;=\; (X_A X_B+X_B X_C+X_C X_A) - 2X_A X_B X_C$$

The Bridge Network



$$\{X_1X_2\}, \{X_3X_4\}, \{X_2X_3X_5\}, \{X_1X_4X_5\}$$

Disjunctive Normal Form:

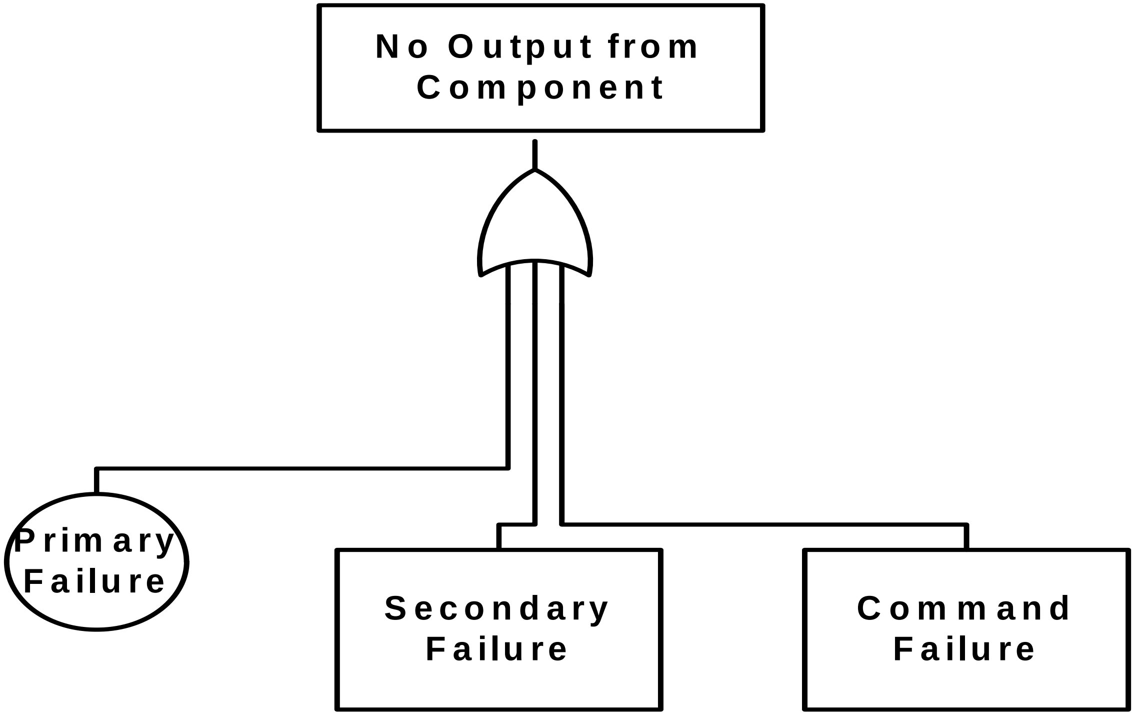
$$X_T=1-(1-X_1X_2)(1-X_3X_4)(1-X_2X_3X_5)(1-X_1X_4X_5)$$

Sum-of-Products Form:

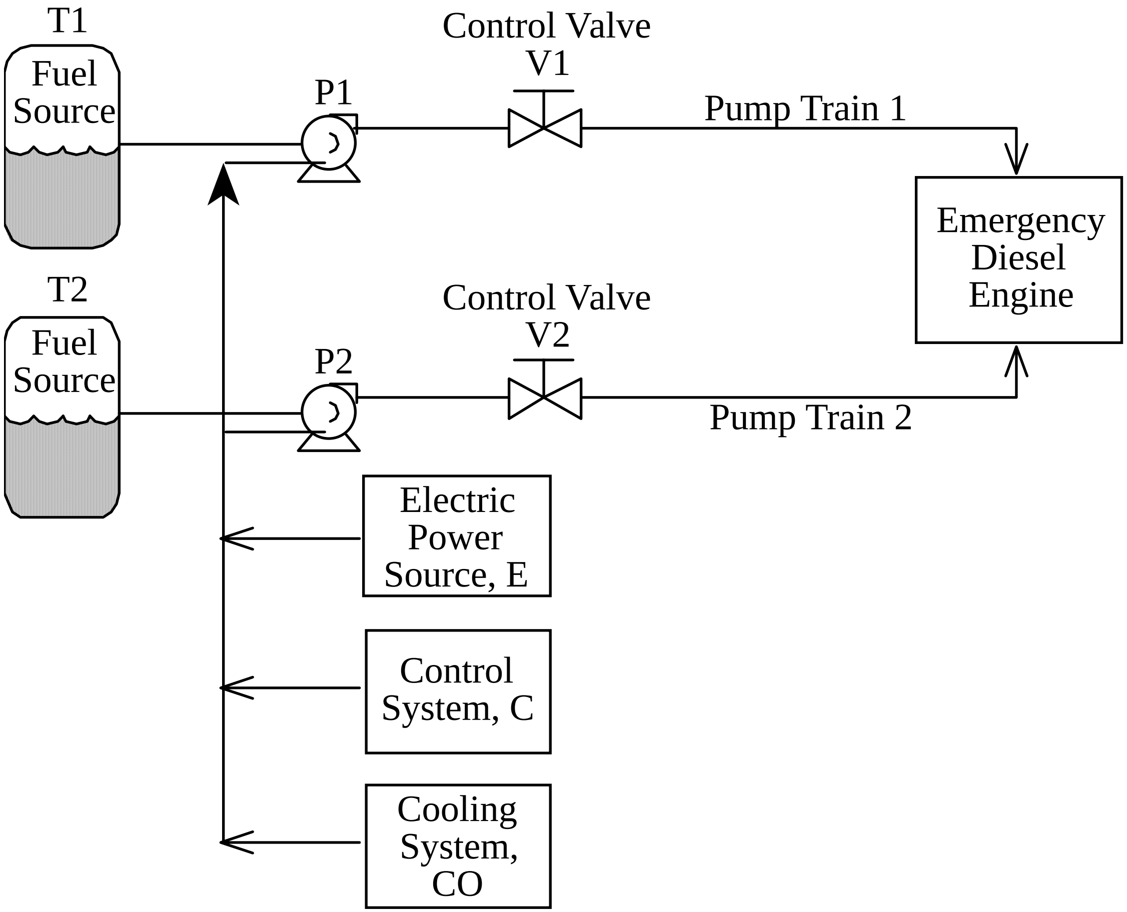
$$X_T = X_1X_2+ X_3X_4+ X_2X_3X_5+ X_1X_4X_5-$$
$$- X_1X_2\, X_3X_4- X_1X_2X_3X_5- X_1X_2X_4X_5 -$$
$$-X_2X_3X_4X_5 - X_1X_3X_4X_5 + 2X_1X_2X_3X_4X_5$$

Causes of Failure

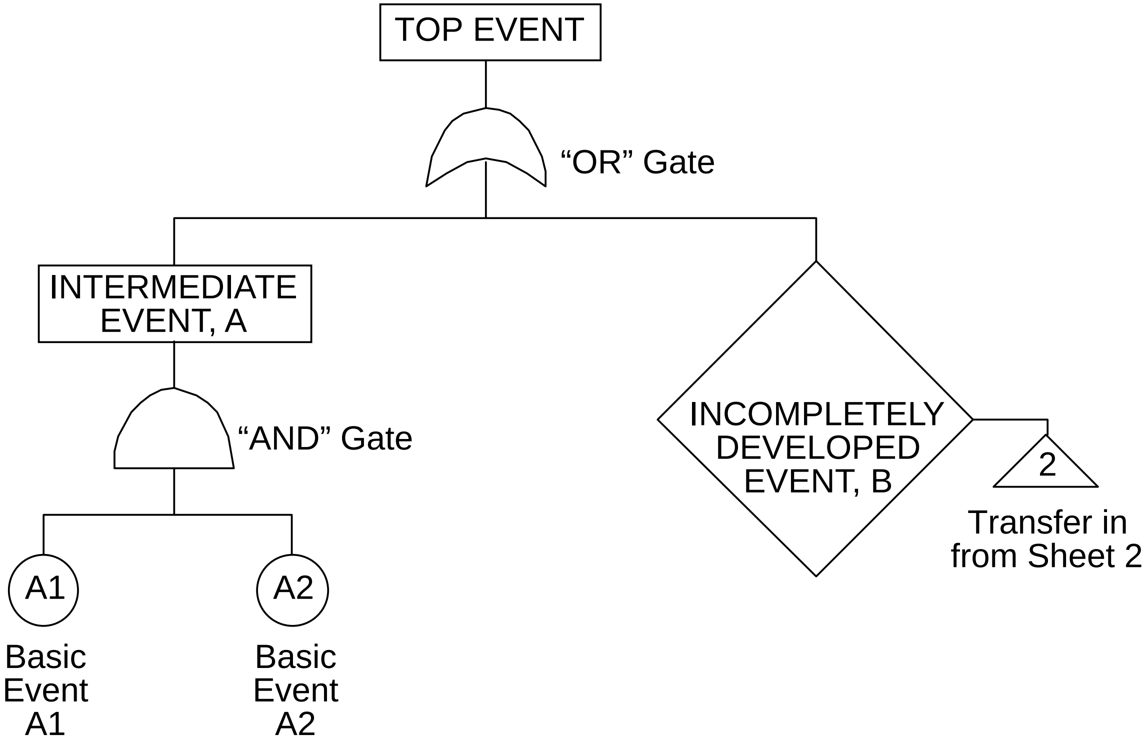
1. Primary failure ("hardware" failure)
2. Secondary failure (external, environmental)
3. "Command" failure (no input; no power)



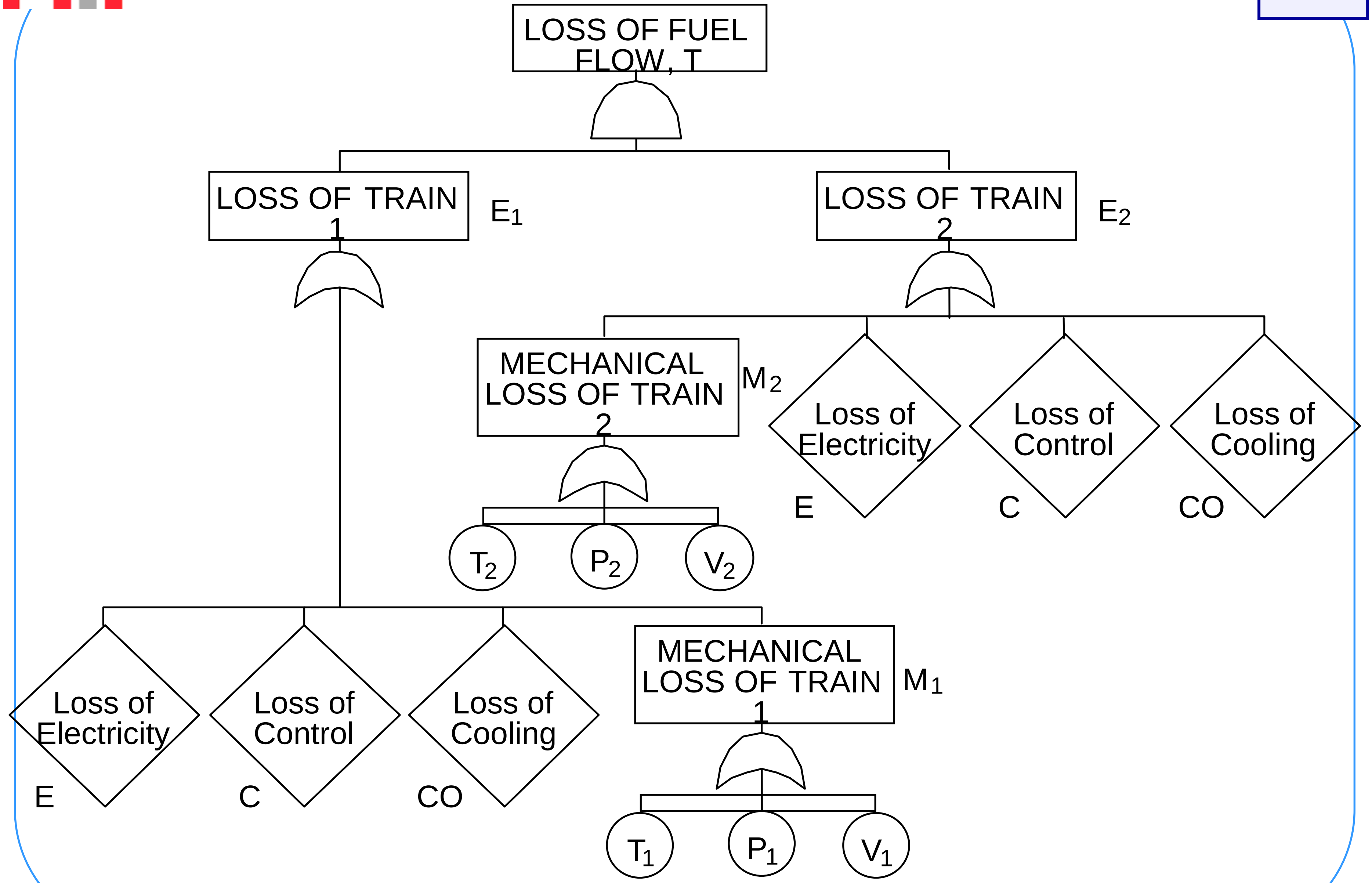
Reliability Block Diagram for the Fuel-Supply System



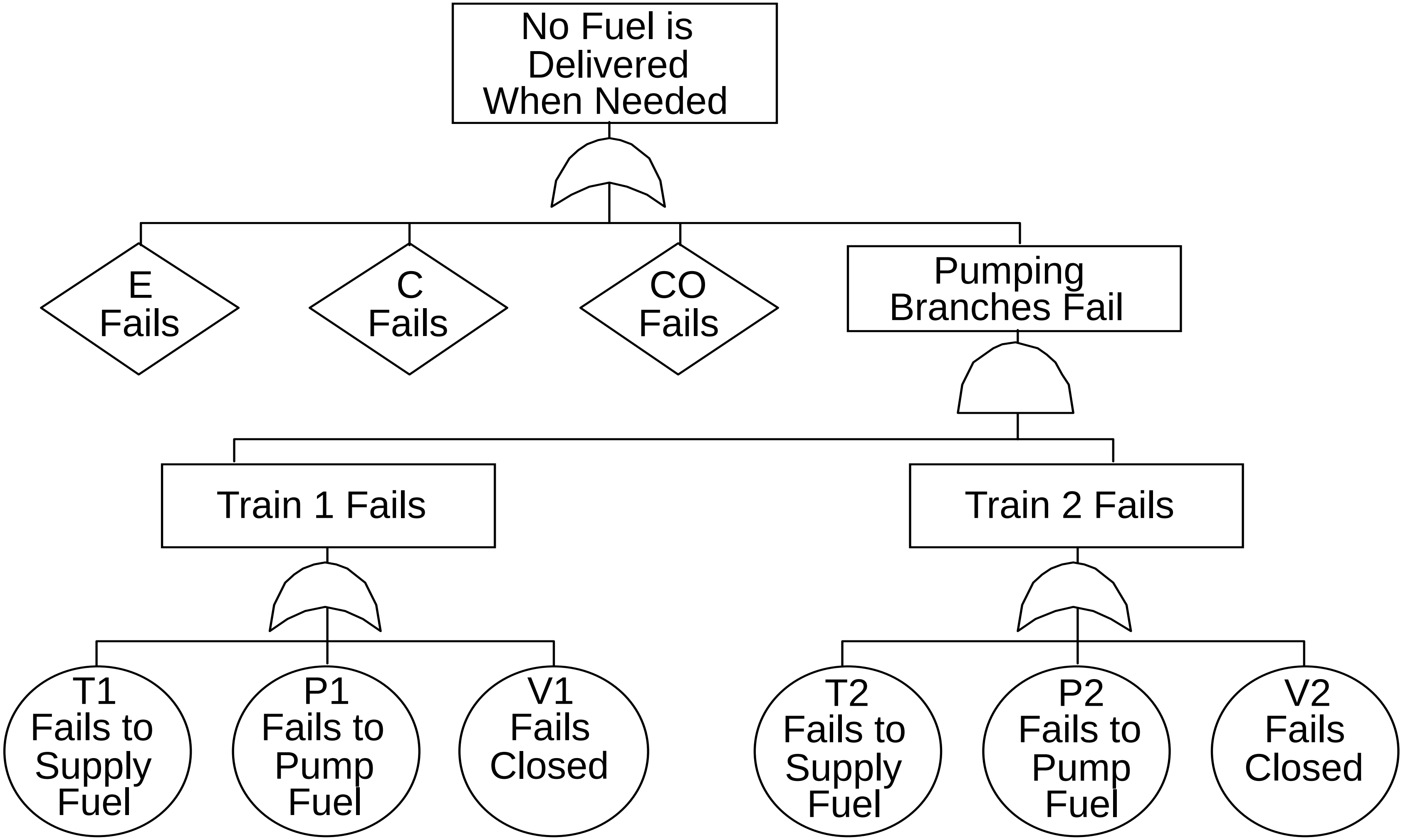
Fault tree elements



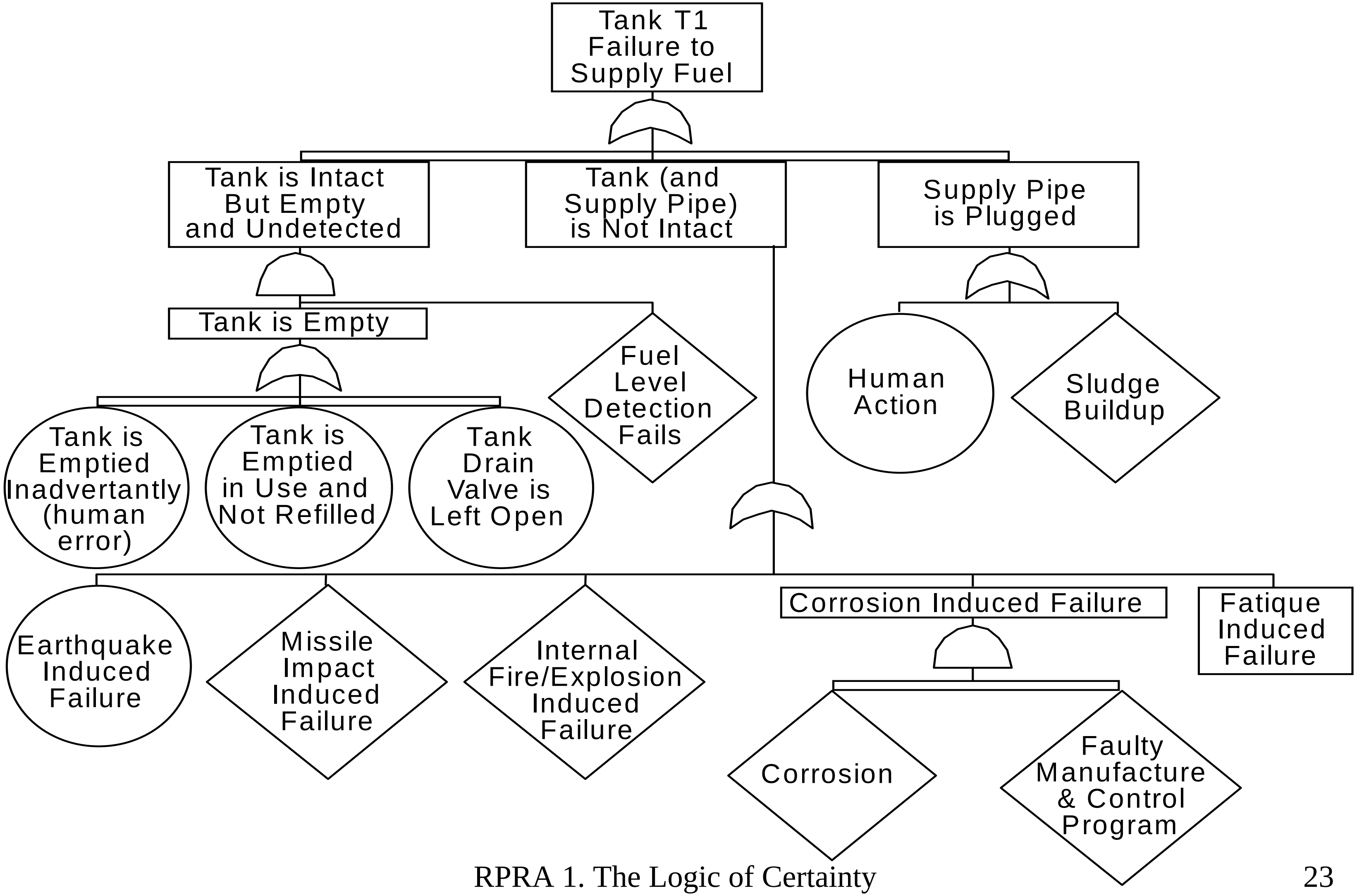
Note: It's helpful to start the fault-tree development from the output of the system (the top event) and work backwards.


LOSS OF FUEL FLOW, T
LOSS OF TRAIN 1
E_1
LOSS OF TRAIN 2
E_2
MECHANICAL LOSS OF TRAIN 2
M_2
Loss of Electricity
E
Loss of Control
C
Loss of Cooling
CO
T_2
P_2
V_2
Loss of Electricity
E
Loss of Control
C
Loss of Cooling
CO
MECHANICAL LOSS OF TRAIN 1
M_1
T_1
P_1
V_1

A simpler fault tree



Development of T1


Tank T1 Failure to Supply Fuel
Tank is Intact But Empty and Undetected
Tank (and Supply Pipe) is Not Intact
Supply Pipe is Plugged
Tank is Empty
Fuel Level Detection Fails
Human Action
Sludge Buildup
Tank is Emptied Inadvertantly (human error)
Tank is Emptied in Use and Not Refilled
Tank Drain Valve is Left Open
Earthquake Induced Failure
Missile Impact Induced Failure
Internal Fire/Explosion Induced Failure
Corrosion Induced Failure
Fatique Induced Failure
Corrosion
Faulty Manufacture & Control Program

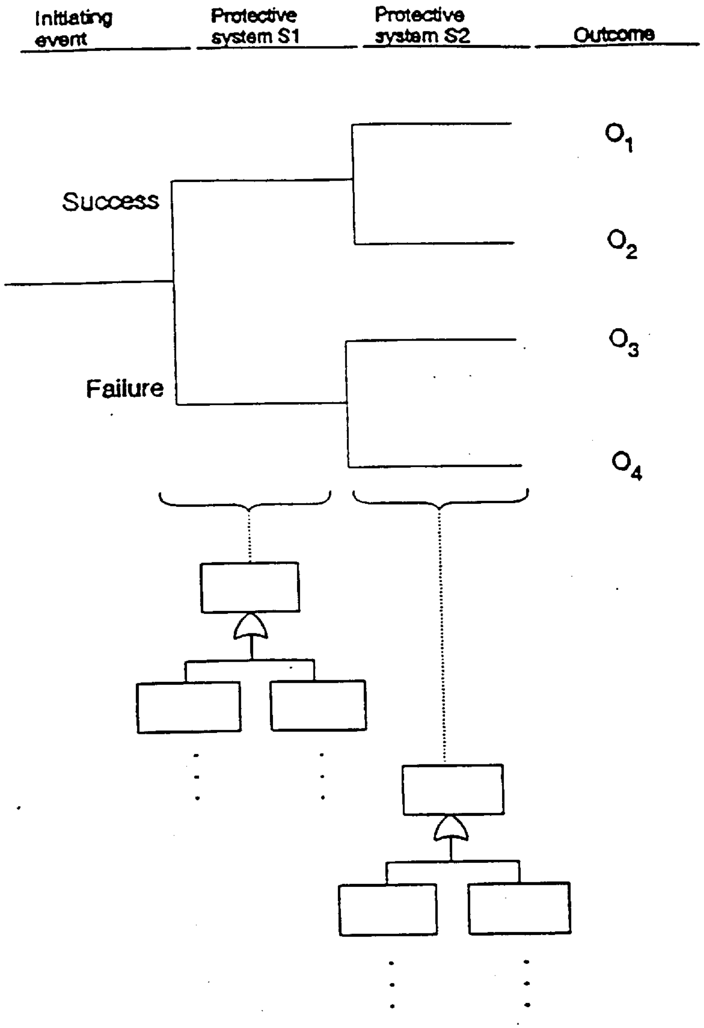
System min cut sets

Any combination of an element of

$$\begin{bmatrix}\textbf{T1, Tank}\\ \textbf{P1, Pump}\\ \textbf{V1. Valve}\end{bmatrix} \text{ and of } \begin{bmatrix}\textbf{T2, Tank}\\ \textbf{P2, Pump}\\ \textbf{V2. Valve}\end{bmatrix}$$

plus

C	**Control System**
	or
E	**Electric Power Source**
	or
CO	**Cooling System**



Example of event tree analysis with fault trees

Examples of Initiating Events

- Loss of Coolant
- Transients
- Human Error
- Loss of Power
- Fires
- Airplane Crashes
- Earthquakes