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.
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, \infty\}

- A collection of sample points is an event.
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: \( X^k = X, \ k: 1, 2, \ldots \)
Union (OR operation)

\[ A \cup B = C \]

\[ X_C = 1 - (1 - X_A)(1 - X_B) \]

\[ X_C \equiv \bigcup X_j \]
Intersection (AND operation)

\[ A \cap B = C \]

\[ X_C = X_A X_B \]

\[ X_C \equiv \prod X_j \]

Mutually Exclusive Events:

\[ A \cap B = \emptyset \]
Simple Systems

Reliability Block Diagram for the Series System

\[
X = 1 - \prod_{j=1}^{N} (1 - X_j) = \bigwedge_{j=1}^{N} X_j
\]

\[
Y = \prod_{j=1}^{N} Y_j
\]
Reliability Block Diagram for the Parallel System

\[ X = \prod_{j=1}^{N} X_j \]

\[ Y = \bigcup_{j=1}^{N} Y_j \]
Event-Tree Analysis

IE

SUCCESS

FAILURE

BARRIER 1

1 (OK)

2 (R1)

3 (R2)

BARRIER 2
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 \( X^k = X \) 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:

\[ M_1 = X_A X_B, \quad M_2 = X_B X_C, \quad M_3 = X_C X_A \]

\[ X_T = \bigcap_{1}^{3} M_j \equiv 1 - (1 - M_1)(1 - M_2)(1 - M_3) = \]

\[ = 1 - (1 - X_A X_B)(1 - X_B X_C)(1 - X_C X_A) \]
\[ X_T = \phi(X_1, X_2, \ldots X_n) \equiv \phi(X) \]

\( \phi(X) \) is the **structure or switching function**.

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

**Disjunctive Normal Form:**

\[
X_T = 1 - \prod_{1}^{N} (1 - M_i) \equiv \bigcup_{1}^{N} M_i
\]

**Sum-of-Products Form:**

\[
X_T = \sum_{i=1}^{N} M_i - \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} M_i M_j + \ldots + (-1)^{N+1} \prod_{i=1}^{N} M_i
\]
For the 2-out-of-3 System:

\[ X_T = 1 - (1 - X_A X_B) (1 - X_B X_C) (1 - X_C X_A) \]

\[ X_T = (M_1 + M_2 + M_3) - (M_1 M_2 + M_2 M_3 + M_3 M_1) + M_1 M_2 M_3 \]

But,

\[ M_1 M_2 = X_A X_B X_C = X_A X_B X_C \]

Therefore, the sum-of-products expression is:

\[ X_T = (X_A X_B + X_B X_C + X_C X_A) - 2 X_A X_B X_C \]
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:**

\[ X_T = X_1X_2 + X_3X_4 + X_2X_3X_5 + X_1X_4X_5 - \]
\[ - X_1X_2X_3X_4 - X_1X_2X_3X_5 - X_1X_2X_4X_5 - \]
\[ - X_2X_3X_4X_5 - X_1X_3X_4X_5 + 2X_1X_2X_3X_4X_5 \]
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

T1 Fuel Source

P1

Control Valve V1

Pump Train 1

Emergency Diesel Engine

T2 Fuel Source

P2

Control Valve V2

Pump Train 2

Electric Power Source, E

Control System, C

Cooling System, CO
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.
RPRA 1. The Logic of Certainty

LOSS OF FUEL FLOW, T

LOSS OF TRAIN E₁

MECHANICAL LOSS OF TRAIN M₂

MECHANICAL LOSS OF TRAIN M₁

Loss of Electricity E₁
Loss of Control C₁
Loss of Cooling CO₁

Loss of Electricity E₂
Loss of Control C₂
Loss of Cooling CO₂

T₁ P₁ V₁
T₂ P₂ V₂
A simpler fault tree

No Fuel is Delivered When Needed

- E Fails
- C Fails
- CO Fails

Pumping Branches Fail

Train 1 Fails
- T1 Fails to Supply Fuel
- P1 Fails to Pump Fuel
- V1 Fails Closed

Train 2 Fails
- T2 Fails to Supply Fuel
- P2 Fails to Pump Fuel
- V2 Fails Closed
Development of T1

Tank T1 Failure to Supply Fuel

Tank is Intact But Empty and Undetected

Tank is Empty

Tank is Emptied Inadvertantly (human error)

Tank is Emptied in Use and Not Refilled

Tank Drain Valve is Left Open

Fuel Level Detection Fails

Supply Pipe is Plugged

Human Action

Sludge Buildup

Corrosion Induced Failure

Earthquake Induced Failure

Missile Impact Induced Failure

Internal Fire/Explosion Induced Failure

Fatigue Induced Failure

Faulty Manufacture & Control Program

Corrosion

Faulty Manufacture & Control Program
System min cut sets

Any combination of an element of

C Control System

or

E Electric Power Source

or

CO Cooling System

and of

T1, Tank
P1, Pump
V1, Valve

T2, Tank
P2, Pump
V2, Valve
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