XI. Fault Tree/ Reliability Analysis

PROBLEM XI.1: Diagnosing Computer Malfunction

A student wants to avoid losing an important term paper due to a computer shutdown.

DESCRIPTION

Before the student starts the term paper, the probability that the student's computer would shut down needs to be determined, as well as the expected cost to prevent loss of data.

METHODOLOGY

By applying Fault Tree Analysis, the student can derive a minimal cut set and recalculate the computer's reliability by imposing different failure probabilities on each component.

SOLUTION

Given:

A = Operating System
B = Keyboard
C = Mouse
D = Motherboard
E = CPU
F = Hard Disc
G = Floppy Drive
H = CD Rom
I = Video Card
J = Monitor

Let:

Z1 = Software
Z2 = Hardware
Z3 = I/O
Z4 = Storage
Z5 = Input
Z6 = Outputs
Z7 = Processing
Z8 = Video

Note: Denote Z for subgroups to avoid confusion with E representing the CPU.
Let:

T = Z1 + Z2
Z1 = A
Z2 = Z3 + Z4
Z3 = Z5 + Z6
Z4 = F + (G · H)
Z5 = (B · C)
Z6 = Z7 + Z8
Z7 = D + E
Z8 = I + J

Therefore:

Z6 = Z7 + Z8
Z6 = D + E + I + J

Z5 = (B · C)

Z3 = Z5 + Z6
Z3 = [(B · C)] + (D + E + I + J)

Z4 = F + (G · H)

Z2 = Z3 + Z4
Z2 = [(B · C) + D + E + I + J] + [F + (G · H)]

Z1 = A

T = Z1 + Z2

Answer:

T = A + (B · C) + D + E + I + J + F + (G · H)

Figure XI.1.1 shows 8 minimal cut sets:

- 6 "one-component" cut sets
- 2 "two-component" cut sets

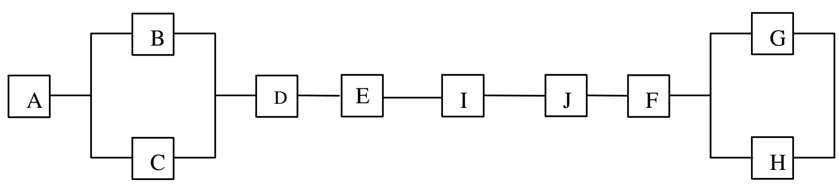

Figure XI.1.1. Minimal cut sets

Table XI.1.1. Component Reliability and Cost Data

Reliability	Unreliability	Cost
$R_A = 0.90$	$Q_A = 0.10$	C_A = \$300
$R_B = 0.95$	$Q_B = 0.05$	C_B = \$ 30
$R_C = 0.95$	$Q_C = 0.05$	C_C = \$ 30
$R_D = 0.98$	$Q_D = 0.02$	C_D = \$200
$R_E = 0.97$	$Q_E = 0.03$	C_E = \$500
$R_F = 0.96$	$Q_F = 0.04$	C_F = \$200
$R_G = 0.96$	$Q_G = 0.04$	C_G = \$ 40
$R_H = 0.97$	$Q_H = 0.03$	C_H = \$150
$R_I = 0.96$	$Q_I = 0.04$	C_I = \$150
$R_J = 0.94$	$Q_J = 0.06$	C_J = \$200

For Z7 (Processing):

$R_{DE} = (R_D)(R_E)$
$R_{DE} = (0.98)(0.97)$
$R_{DE} = 0.9506$

For Z8 (Video):

$R_{IJ} = (R_I)(R_J)$
$R_{IJ} = (0.96)(0.94)$
$R_{IJ} = 0.9024$

For Z6 (Outputs):

$R_{DEIJ} = (R_{DE})(R_{IJ})$
$R_{DEIJ} = (0.9506)(0.9024)$
$R_{DEIJ} = 0.85782144$

For Z5 (Inputs):

$R_{BC} = 1 - (Q_B)(Q_C)$
$R_{BC} = 1 - (0.05)(0.05)$
$R_{BC} = 1 - (0.0025)$
$R_{BC} = 0.9975$

For Z3 (I/O):

$R_{BCDEIJ} = (R_{BC})(R_{DEIJ})$
$R_{BCDEIJ} = (0.9975)(0.85782144)$
$R_{BCDEIJ} = 0.855676886$

For Z4 (Storage):

$R_{GH} = 1 - (Q_G)(Q_H)$
$R_{GH} = 1 - (0.04)(0.03)$
$R_{GH} = 1 - 0.0012$
$R_{GH} = 0.9988$

$R_{FGH} = (R_F)(R_{GH})$
$R_{FGH} = (0.96)(0.9988)$
$R_{FGH} = 0.958848$

For Z2 (Hardware):

$R_{BCDEIJFGH} = (R_{BCDEIJ})(R_{FGH})$
$R_{BCDEIJFGH} = (0.855676886)(0.958848)$
$R_{BCDEIJFGH} = 0.820464071$

For T (System):

$R_{System} = (R_A)(R_{BCDEIJFGH})$
$R_{System} = (0.9)(0.820464071)$
$\mathbf{R_{System} = 0.738417664 \approx 0.7384}$

$Q_{System} = 1 - R_{System}$
$Q_{System} = 1 – 0.738417664$
$\mathbf{Q_{System} = 0.261582336 \approx 0.2616}$

Base Total System Cost (C_0) = $C_A + C_B + C_C + C_D + C_E + C_F + C_G + C_H + C_I + C_J$
$C_0 = 300 + 30 + 30 + 200 + 500 + 200 + 40 + 150 + 150 + 200 = \$1800$

NOTE: The added components are in parallel *only* with the original component of the same type *and no other components,* and are calculated accordingly. For example, the added monitor (J_2) is in parallel *only* with the original monitor (J_1) (*not* with the video cards); the added hard disc (F_2) is in parallel *only* with the original hard disc (F_1) (*not* with the floppy drive and CD ROM); the added video card (I_2) is in parallel *only* with the original video card (I_1) (*not* with the monitors); and the added CPU (E_2) is in parallel *only* with the original CPU (E_1) (*not* with the motherboard).

Constructing parallel structure

For Z7 (Processing):
$R_{E1E2} = 1- (Q_{E1})(Q_{E2})$
$R_{E1E2} = 1 – (0.03)(0.03)$
$R_{E1E2} = 1 – 0.0009$
$R_{E1E2} = 0.9991$

$R_{DE1E2} = (R_D)(R_{E1E2})$
$R_{DE1E2} = (0.98)(0.9991)$
$R_{DE1E2} = 0.979118$

For Z8 (Video):
$R_{I1I2} = 1 – (Q_{I1})(Q_{I2})$
$R_{I1I2} = 1 – (0.04)(0.04)$
$R_{I1I2} = 1 – 0.0016$
$R_{I1I2} = 0.9984$

$R_{J1J2} = 1 – (Q_{J1})(Q_{J2})$
$R_{J1J2} = 1 – (0.06)(0.06)$
$R_{J1J2} = 1 – 0.0036$
$R_{J1J2} = 0.9964$

$R_{I1I2J1J2} = (R_{I1I2})(R_{J1J2})$
$R_{I1I2J1J2} = (0.9984)(0.9964)$
$R_{I1I2J1J2} = 0.99480576$

For Z6 (Outputs):
$R_{DE1E2I1I2J1J2} = (R_{DE1E2})(R_{I1I2J1J2})$
$R_{DE1E2I1I2J1J2} = (0.979118)(0.99480576)$
$R_{DE1E2I1I2J1J2} = 0.974032226$

For Z5 (Inputs):

From previous calculations:

$R_{BC} = 0.9975$

For Z3 (I/O):

$R_{BCDE1E2I1I2J1J2} = (R_{BC})(R_{DE1E2I1I2J1J2})$

$R_{BCDE1E2I1I2J1J2} = (0.9975)(0.974032226)$

$R_{BCDE1E2I1I2J1J2} = 0.971597145$

For Z4 (Storage):

$R_{F1F2} = 1 – (Q_{F1})(Q_{F2})$

$R_{F1F2} = 1 – (0.04)(0.04)$

$R_{F1F2} = 1 – (0.0016)$

$R_{F1F2} = 0.9984$

From previous calculations:

$R_{GH} = 0.9988$

$R_{F1F2GH} = (R_{F1F1})(R_{GH})$

$R_{F1F2GH} = (0.9984)(0.9988)$

$R_{F1F2GH} = 0.99720192$

For Z2 (Hardware):

$R_{BCDE1E2I1I2J1J2F1F2GH} = (R_{BCDE1E2I1I2J1J2})(R_{F1F2GH})$

$R_{BCDE1E2I1I2J1J2F1F2GH} = (0.971597145)(0.99720192)$

$R_{BCDE1E2I1I2J1J2F1F2GH} = 0.968878539$

For T (System):

$R_{System} = (R_A)(R_{BCDE1E2I1I2J1J2F1F2GH})$

$R_{System} = (0.9)(0.968878539)$

$\mathbf{R_{System} = 0.871990685 \approx 0.8720}$

$Q_{System} = 1 - R_{System}$

$Q_{System} = 1 – 0.871990685$

$\mathbf{Q_{System} = 0.128009314 \approx 0.1280}$

Total System Cost for Option 1 (C_1):

$C_1 = C_0 + C_E + C_F + C_I + C_J$

$C_1 = 1800 + 500 + 200 + 150 + 200$

$\mathbf{C_1 = \$2850}$

For Z7 (Processing):

From previous calculations:

$R_{DE} = 0.9506$

For Z8 (Video):

From previous calculations:

$R_{J1J2} = 0.9964$

$R_{IJ1J2} = (R_I)(R_{J1J2})$
$R_{IJ1J2} = (0.96)(0.9964)$
$R_{IJ1J2} = 0.956544$

For Z6 (Outputs):

$R_{DEIJ1J2} = (R_{DE})(R_{IJ1J2})$
$R_{DEIJ1J2} = (0.9506)(0.956544)$
$R_{DEIJ1J2} = 0.909290726$

For Z5 (Inputs):

From previous calculations:

$R_{BC} = 0.9975$

For Z3 (I/O):

$R_{BCDEIJ1J2} = (R_{BC})(R_{DEIJ1J2})$
$R_{BCDEIJ1J2} = (0.9975)(0.909290726)$
$R_{BCDEIJ1J2} = 0.907017499$

For Z4 (Storage):

From previous calculations:

$R_{F1F2GH} = 0.99720192$

For Z2 (Hardware):

$R_{BCDEIJ1J2F1F2GH} = (R_{BCDEIJ1J2})(R_{F1F2GH})$
$R_{BCDEIJ1J2F1F2GH} = (0.907017499)(0.99720192)$
$R_{BCDEIJ1J2F1F2GH} = 0.904479592$

For Z1 (Software):

$R_{A1A2} = 1 – (Q_{A1})(Q_{A2})$
$R_{A1A2} = 1 – (0.1)(0.1)$
$R_{A1A2} = 1 – 0.01$
$R_{A1A2} = 0.99$

For T (System):

$R_{System} = (R_{A1A2})(R_{BCDEIJ1J2F1F2GH})$
$R_{System} = (0.99)(0.904479592)$
$\mathbf{R_{System} = 0.895434796 \approx 0.8954}$

$Q_{System} = 1 - R_{System}$
$Q_{System} = 1 – 0.895434796$
$\mathbf{Q_{System} = 0.104565203 \approx 0.1046}$

Total System Cost for Option 2 (C_2):

$C_2 = C_0 + C_A + C_F + C_J$

$C_2 = 1800 + 300 + 200 + 200$

C_2 = $2500

For Z7 (Processing):

From previous calculations:

$R_{DE} = 0.9506$

For Z8 (Video):

From previous calculations:

$R_{IJ} = 0.9024$

For Z6 (Outputs):

From previous calculations:

$R_{DEIJ} = 0.85782144$

For Z5 (Inputs):

$R_{C1C1} = 1 - (Q_{C1})(Q_{C2})$

$R_{C1C2} = 1 - (0.05)(0.05)$

$R_{C1C2} = 1 - 0.0025$

$R_{C1C2} = 0.9975$

$Q_{C1C2} = 1 - R_{C1C2}$

$Q_{C1C2} = 1 - 0.9975$

$Q_{C1C2} = 0.0025$

$R_{BC1C2} = 1 - (Q_B)(Q_{C1C2})$

$R_{BC1C2} = 1 - (0.05)(0.0025)$

$R_{BC1C2} = 1 - 0.000125$

$R_{BC1C2} = 0.999875$

For Z3 (I/O):

$R_{BC1C2DEIJ} = (R_{BC1C2})(R_{DEIJ})$

$R_{BC1C2DEIJ} = (0.99875)(0.85782144)$

$R_{BC1C2DEIJ} = 0.85674916$

For Z4 (Storage):

$R_{G1G2} = 1 - (Q_{G1})(Q_{G2})$

$R_{G1G2} = 1 - (0.04)(0.04)$

$R_{G1G2} = 1 - 0.0016$

$R_{G1G2} = 0.9984$

$Q_{G1G2} = 1 - R_{G1G2}$

$Q_{G1G2} = 1 - 0.9984$

$Q_{G1G2} = 0.0016$

$R_{G1G2H} = 1 - (Q_{G1G2})(Q_H)$
$R_{G1G2H} = 1 - (0.0016)(0.03)$
$R_{G1G2H} = 1 - 0.000048$
$R_{G1G2H} = 0.999952$

$R_{FG1G2H} = (R_F)(R_{G1G2H})$
$R_{FG1G2H} = (0.96)(0.999952)$
$R_{FG1G2H} = 0.95995392$

For Z2 (Hardware):
$R_{BC1C2DEIJFG1G2H} = (R_{BC1C2DEIJ})(R_{FG1G2H})$
$R_{BC1C2DEIJFG1G2H} = (0.85674916)(0.95995392)$
$R_{BC1C2DEIJFG1G2H} = 0.82243971$

For T (System):
$R_{System} = (R_A)(R_{BC1C2DEIJFG1G2H})$
$R_{System} = (0.9)(0.82243971)$
$\mathbf{R_{System} = 0.740195743 \approx 0.7402}$

$Q_{System} = 1 - R_{System}$
$Q_{System} = 1 - 0.740195743$
$\mathbf{Q_{System} = 0.259804256 \approx 0.2598}$

Total System Cost for Option 3 (C_3):
$C_3 = C_0 + C_C + C_G$
$C_3 = 1800 + 30 + 40$
$\mathbf{C_3 = \$1870}$

ANALYSIS

Total system costs and unreliabilities are summarized in Table XI.1.2:

Table XI.1.2. Summary of Costs and Unreliabilities

Option	Cost	Unreliability	Deltas	
Base	$1800	0.2616	Cost	Unreliability
1	$2850	0.1280	+$1050	-0.1336
2	$2500	0.1046	+$700	-0.1570
3	$1870	0.2598	+$70	-0.0018

We chart the cost of the options vs. their unreliabilities, as called for in the problem:

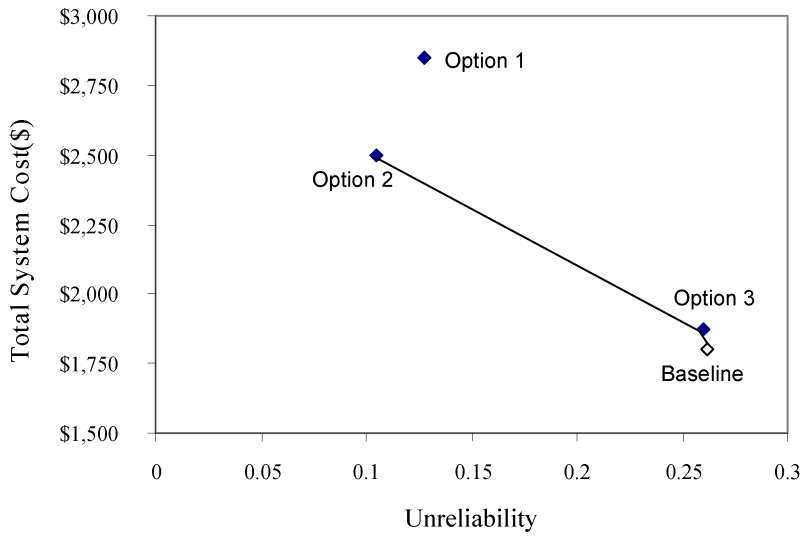

Figure XI.1.2. Total system cost vs. unreliability

Based on Table XI.1.2 and Figure XI.1.2, Option 1 is not acceptable. Its cost is higher than the cost for Option 2, and its unreliability is also higher than for Option 2. This indicates that Option 1 is NOT an optimal solution.

From the base option to Option 3 there is only about a 0.0017 decrease in unreliability for a cost of $70. For $700, the decrease in unreliability from the base option to Option 2 is 0.1570.

The student will have to decide if the reduction in unreliability using Option 2 is significant and worth the larger cost.

From this comparison, my recommendation would be Option 2, even though it is $630 more expensive than Option 3. Option 2 reduces the unreliability from greater than 25% to just over 10%, and the increased reliability would be worth the increased cost.

PROBLEM XI.2: An Integrated Bridge System (IBS)

The purpose of this problem is to support automated and safe ship navigation, with reduced manning. Both cost and reliability must be considered in proposed IBS designs.

DESCRIPTION

The Integrated Bridge System design facilitates automating time-consuming navigation tasks such as voyage planning/execution, steering control, and communicating throttle order. The IBS hardware and software together provide capabilities including voyage planning, an integrated navigational picture, collision and mine avoidance, and ship maneuvering (steering and propulsion) control. The IBS also includes interfaces to port/starboard steering gear to send commands for rudder control and receive feedback.

The IBS consists of two ensembles: the Voyage Management System (VMS) and the Steering and Thrust Control System (SCS).

The VMS provides an Electronic Charting Display and Information Systems-Naval (ECDIS-N)-certifiable system. The ECDIS-N features include: electronic chart display, route planning/ monitoring, backup arrangements, safety checking, manual heading correction, alarms and indications, sensor integration, CO approval of navigation plans, radar image overlay, and voyage recording and visual replay. In addition, the VMS provides bell and deck log recording/displays, man-overboard monitoring, collision avoidance, precision anchoring and anchor-drag monitoring, mine-avoidance support, Automatic Radar Plotting Aid (ARPA) radar control and display, contact information display, and other data displays. The VMS also provides automated control of the ship's heading and speed by generating and sending the desired heading and speed orders to the SCS in order to keep the ship on the pre-selected/approved route plan, depending on the task order given.

The SCS software and hardware together provide functionality to control the speed and heading of the ship. The SCS accepts steering and thrust commands either from the operator or from the VMS, depending on the steering mode selected. For operator control of the ship's heading and speed, the SCS provides a human-computer interface (HCI) for the operator to manually enter the steering and thrust commands. Additionally, the bridge and aft steering-control consoles are equipped with a helm wheel for manual entry of rudder orders.

METHODOLOGY

Designing the Integrated Bridge System (IBS) can be solved through Fault Tree Analysis, as follows:

Components:

1) Voyage Management System (VMS)
   VMS Components:
   A: Software (Cost: $100,000; R: 0.98)

B: Hardware (Cost: $1750; R: 0.99)
C: Operating System (Cost: $200; R: 0.95)

2) Steering Control System (SCS)
SCS Components:
D: Software (Cost: $40,000; R: 0.98)
E: Hardware (Cost: $50,000; R: 0.97)
F: Operating System (Cost: $250; R: 0.95)

Figure XI.2.1 shows the basic IBS Fault Tree:

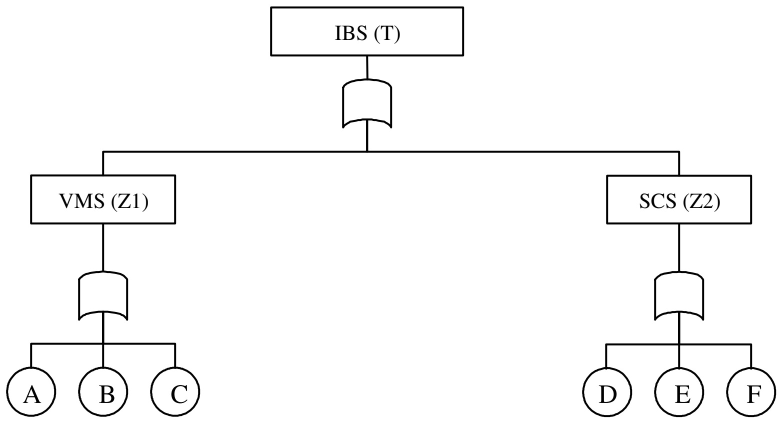

Figure XI.2.1. Fault Tree for Integrated Bridge System (IBS)

Given:

A = VMS Software
B = VMS Hardware
C = VMS Operating System
D = SCS Software
E = SCS Hardware
F = SCS Operating System

SOLUTION

The minimal cut set is determined as follows:

Let:

$Z1 = A + B + C$
$Z2 = D + E + F$

Let:

$Z1 = A + B + C$
$Z2 = D + E + F$
$T = Z1 + Z2$

Solution : T = A + B + C + D + E + F

The system has six minimal "one component" cut sets, as depicted in Figure XI.2.2:

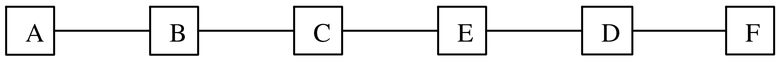

Figure XI.2.2. Minimal Cut Sets for IBS

Next, we calculate the system reliability (and unreliability) given the cost and performance data of the components as shown in Table XI.2.1.

Table XI.2.1. Given Values

Reliability	Unreliability	Cost
$R_A = 0.98$	$Q_A = 0.02$	C_A = \$100,000
$R_B = 0.99$	$Q_B = 0.01$	C_B = \$1750
$R_C = 0.95$	$Q_C = 0.05$	C_C = \$200
$R_D = 0.98$	$Q_D = 0.02$	C_D = \$40,000
$R_E = 0.97$	$Q_E = 0.03$	C_E = \$50,000
$R_F = 0.95$	$Q_F = 0.05$	C_F = \$250

For Z1 (VMS):

$R_{ABC} = (R_A)(R_B)(R_C)$
$R_{ABC} = (0.98)(0.99)(0.95)$
$R_{ABC} = 0.92169$

For Z2 (SCS):

$R_{DEF} = (R_D)(R_E)(R_F)$
$R_{DEF} = (0.98)(0.97)(0.95)$
$R_{DEF} = 0.90307$

For T (System):

$R_{System} = (R_{ABC})(R_{DEF})$
$R_{System} = (0.92169)(0.90307)$
$\mathbf{R_{System} = 0.832350588 \approx 0.8324}$

$Q_{System} = 1 - R_{System}$
$Q_{System} = 1 - 0.832350588$
$\mathbf{Q_{System} = 0.167649412 \approx 0.1676}$

Baseline Total System Cost $(C_0) = C_A + C_B + C_C + C_D + C_E + C_F$
$C_0 = 100{,}000 + 1750 + 200 + 40{,}000 + 50{,}000 + 250$
$\mathbf{C_0 = \$192{,}200}$

Suppose that 3 design options have been identified to improve the overall system reliability. The objective of the subsequent analysis is to determine the efficacy of each option relative to additional cost requirements and improvements in reliability.

Option 1: Increase number of VMS modules to 2.
Option 2: Increase number of SCS modules to 2.
Option 3: Increase number of both modules to 2.

Option 1:

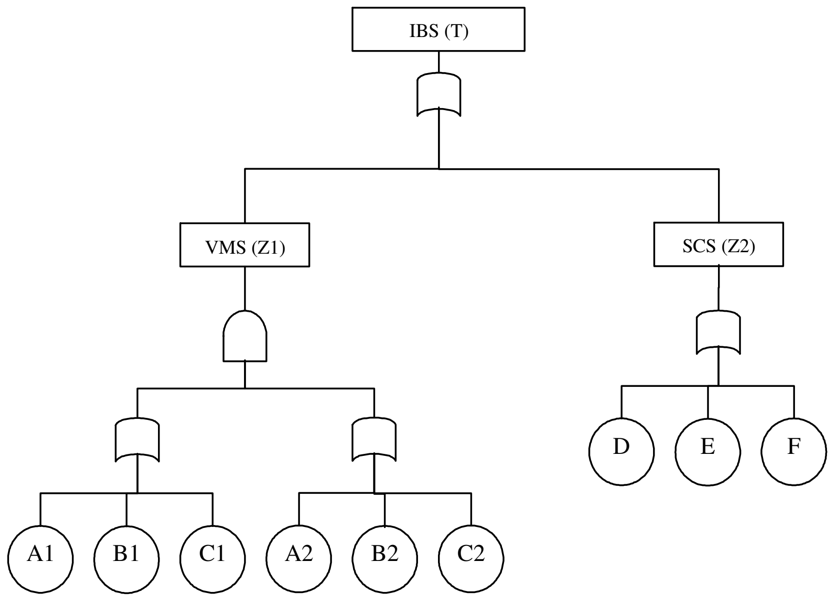

Figure XI.2.3. Fault Tree for Option 1

For Z2 (SCS):

From original problem:

$R_{DEF} = 0.90307$

For Z1 (VMS):

From original problem:

$R_{A1B1C1} = 0.92169$

$Q_{A1B1C1} = 1 - R_{A1B1C1}$
$Q_{A1B1C1} = 1 - 0.92169$
$Q_{A1B1C1} = 0.07831$

From original problem:

$R_{A2B2C2} = 0.92169$

$Q_{A2B2C2} = 1 - R_{A2B2C2}$
$Q_{A2B2C2} = 1 - 0.92169$
$Q_{A2B2C2} = 0.07831$

$R_{A1B1C1A2B2C2} = 1 - (Q_{A1B1C1})(Q_{A2B2C2})$
$R_{A1B1C1A2B2C2} = 1 - (0.07831)(0.07831)$
$R_{A1B1C1A2B2C2} = 1 - 0.006132456$
$R_{A1B1C1A2B2C2} = 0.993867543$

For T (System):

$R_{System} = (R_{A1B1C1A2B2C2})(R_{DEF})$
$R_{System} = (0.993867543)(0.90307)$
$\mathbf{R_{System} = 0.897531962 \approx 0.8975}$

$Q_{System} = 1 - R_{System}$
$Q_{System} = 1 - 0.897531962$
$\mathbf{Q_{System} = 0.102468037 \approx 0.1025}$

Option 1 Total System Cost (C_1) = $C_0 + C_A + C_B + C_C$

$C_1 = 192{,}200 + 100{,}000 + 1750 + 200$
$\mathbf{C_1 = \$294{,}150}$

Option 2:

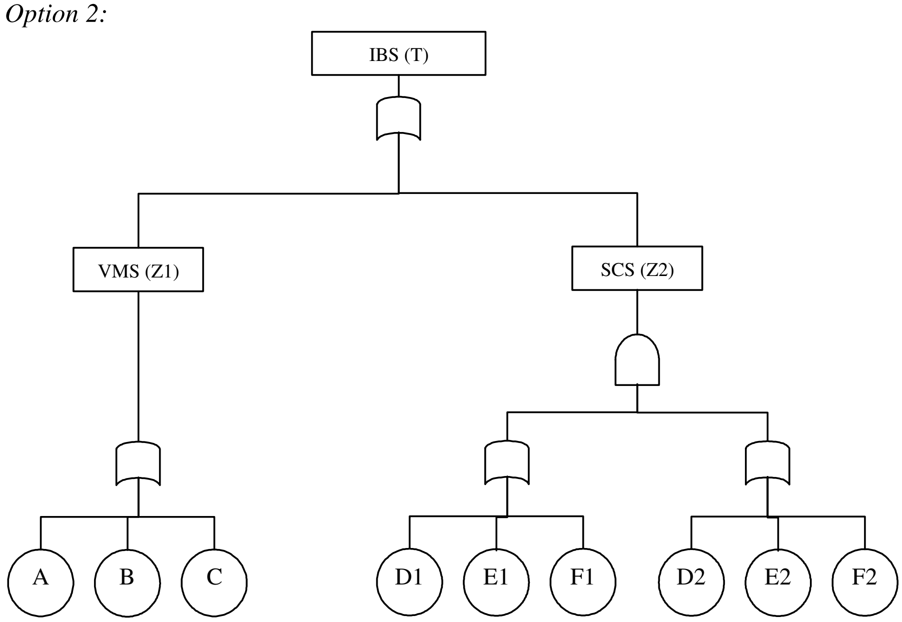

Figure XI.2.4. Fault Tree for Option 2

For Z2 (SCS):

From original problem:

$R_{D1E1F1} = 0.90307$

$Q_{D1E1F1} = 1 - R_{D1E1F1}$
$Q_{D1E1F1} = 1 - 0.90307$
$Q_{D1E1F1} = 0.09693$

From original problem:

$R_{D2E2F2} = 0.90307$

$Q_{D2E2F2} = 1 - R_{D2E2F2}$
$Q_{D2E2F2} = 1 - 0.90307$
$Q_{D2E2F2} = 0.09693$

$R_{D1E1F1D2E2F2} = 1 - (Q_{D1E1F1})(Q_{D2E2F2})$
$R_{D1E1F1D2E2F2} = 1 - (0.09693)(0.09693)$
$R_{D1E1F1D2E2F2} = 1 - 0.009395424$
$R_{D1E1F1D2E2F2} = 0.990604575$

For Z1 (VMS):

From original problem:

$R_{A1B1C1} = 0.92169$

For T (System):

$R_{System} = (R_{ABC})(R_{D1E1F1D2E2F2})$
$R_{System} = (0.92169)(0.990604575)$
$\mathbf{R_{System} = 0.91303033 \approx 0.9130}$

$Q_{System} = 1 - R_{System}$
$Q_{System} = 1 - 0.91303033$
$\mathbf{Q_{System} = 0.086969669 \approx 0.0870}$

Option 2 Total System Cost (C_2) = $C_0 + C_D + C_E + C_F$

$C_2 = 192{,}200 + 40{,}000 + 50{,}000 + 250$
$\mathbf{C_2 = \$282{,}450}$

Option 3:

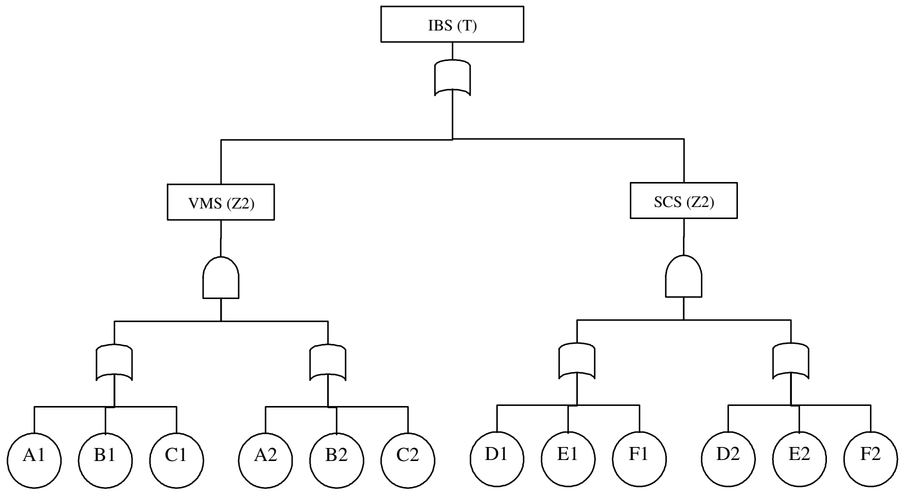

Figure XI.2.5. Fault Tree for Option 3

For Z2 (SCS):
From Option 2:

$R_{D1E1F1D2E2F2} = 0.990604575$

For Z1 (VMS):
From Option 1:

$R_{A1B1C1A2B2C2} = 0.993867543$

For T (System):

$R_{System} = (R_{A1B1C1A2B2C2})(R_{D1E1F1D2E2F2})$
$R_{System} = (0.993867543)(0.990604575)$
$\mathbf{R_{System} = 0.984529735 \approx 0.9845}$

$Q_{System} = 1 - R_{System}$
$Q_{System} = 1 - 0.984529735$
$\mathbf{Q_{System} = 0.015470264 \approx 0.0155}$

Option 3 Total System Cost (C_3) = $C_0 + C_A + C_B + C_C + C_D + C_E + C_F$

$C_3 = 192{,}200 + 100{,}000 + 1750 + 200 + 40{,}000 + 50{,}000 + 250$
$\mathbf{C_3 = \$384{,}400}$

Multiobjective tradeoff:

Table XI.2.2 shows the total system costs and reliabilities.

Table XI.2.2. Summary of Costs and Reliabilities

Option	***Cost***	***Reliability***	***Deltas***	
Baseline	$192,200	0.8324	*Cost*	*Reliability*
1	$294,150	0.8975	+$101,950	+0.0651
2	$282,450	0.9130	+$90,250	+0.0806
3	$384,400	0.9845	+$192,200	+0.1521

Figure XI.2.6 charts the cost vs. the reliability of the options.

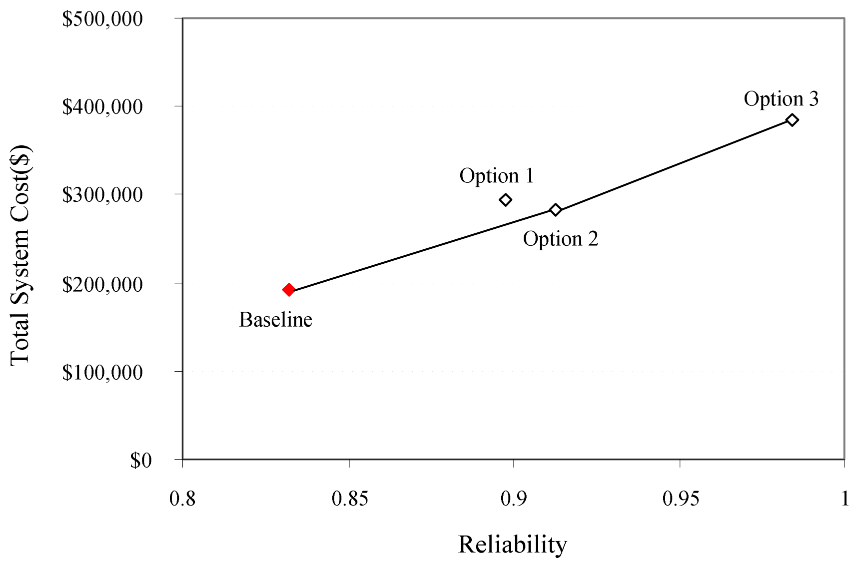

Figure XI.2.6. Pareto-Optimal Frontier

NOTE: The reliabilities are used rather than the unreliabilities.

ANALYSIS

Based on Table XI.2.2, Option 1 is not acceptable. Its cost is higher than the cost for Option 2, but its reliability is lower. This indicates that Option 1 is not an optimal solution.

Option 2 has an increase of 0.0806 in reliability over the baseline (to 0.9130) at a total cost increase of $90,250. Option 3 has an increase of 0.1521 in reliability over the baseline (to 0.9845) at a total cost increase of $192,200.

The decisionmakers will have to decide if the 0.0715 difference in reliability between Options 2 and 3 is worth the extra $101,950 that Option 3 will cost over Option 2. However, from this comparison our recommendation is Option 3, which increases the reliability from 0.8324 to 0.9845. Although it is entirely obvious that Option 2 is much less expensive, the significantly higher level of reliability would be worth the extra cost in terms of safety.

PROBLEM XI.3: Preventing Product Failure

The problem being addressed is the introduction of a faulty product to market by a large manufacturing company's Product Management Group (PMG).

DESCRIPTION

This problem is solved in two steps: 1) reorganizing the PMG's "chain of command," and 2) using Fault Tree Analysis to reduce the risk of product failure while minimizing cost.

METHODOLOGY

Step 1: *Reorganizing the "chain of command."*

Instead of the traditional corporate divisions along product lines only, the company organized itself into a two-dimensional matrix with profit centers (i.e., business types) as the row headings and cost centers (departments) as the column headings.

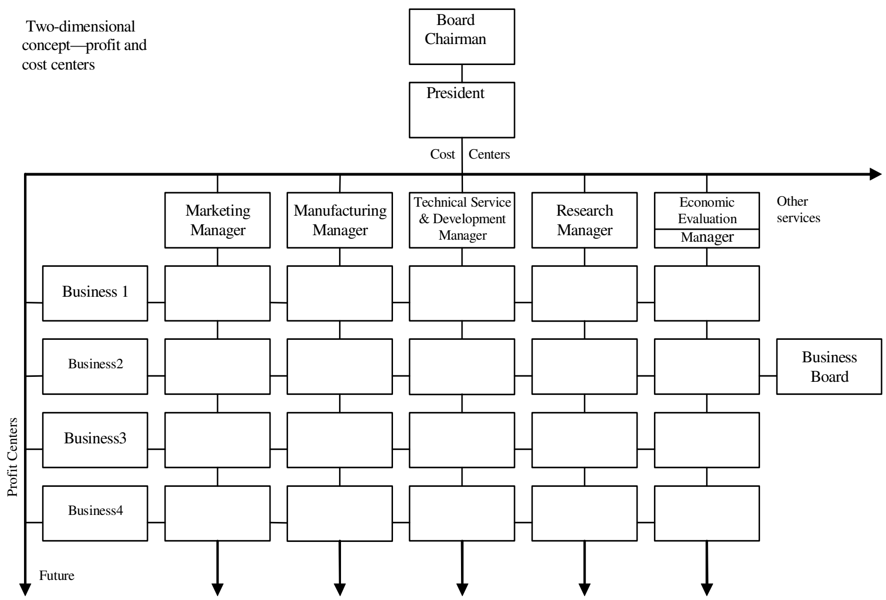

Figure XI.3.1. Two-Dimensional View of Company Matrix

As seen above, the resulting rows form business boards according to product category (e.g., electronics), each with one business manager and a representative from Marketing, Research, Manufacturing, Technical Service & Development, and Economics/Finance. Within this structure, the company formed Product Management Groups (PMGs), similar in form to the business boards, except that each PMG focuses on planning for specific product groups and consists of representatives from lower rungs of department ladders.

Step 2: Fault Tree Analysis

Using Fault Tree Analysis, the Product Management Group (PMG) seeks to minimize the probability of introducing a faulty product by selecting one of five policies. There are two objectives:

- to minimize the probability of introducing a faulty product, and
- to minimize the cost of the policy.

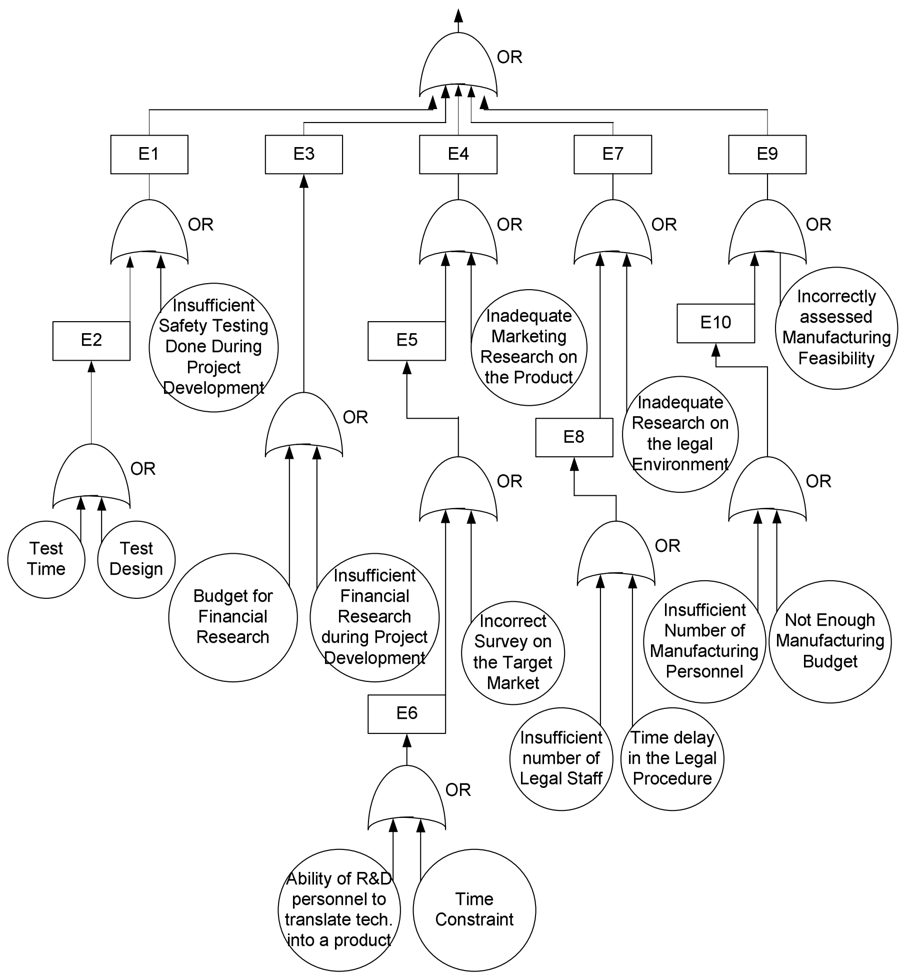

Figure XI.3.2. Fault Tree for the Faulty Product

The top layer of the fault tree in Figure XI.3.2 is the undesired event, the introduction of a faulty product. A product can be faulty because of any of the events listed in Table XI.3.1, which are depicted in the second, third, and bottom tiers of the tree. The bottom tier, which grows out from the third, shows which specific components of the company's product development program failed.

Table XI.3.1. Description of the Basic Events

Basic Event	Description	Reliability
N21	Test time	.99
N22	Test design	.92
N12	Insufficient safety testing during product development	.98
N31	Budget for financial research	.93
N32	Insufficient financial research during the product development	.99
N41	Inadequate marketing research on the product	.98
N51	Incorrect marketing survey	.99
N61	Ability of R&D personnel to translate technology into a product	.99
N62	Time constraints	.98
N71	Inadequate research on the legal environment	.98
N81	Insufficient number of legal staff	.99
N82	Time delay in the legal procedure	.99
N91	Incorrectly assessed manufacturing feasibility	.99
N01	Insufficient number of manufacturing personnel	.94
N02	Not enough manufacturing budget	.95

SOLUTION

There are 5 policy options:
Policy A – Do nothing.
Policy B – Improve test design. (N22)
Policy C – Increase financial research budget. (N31)
Policy D – Increase number of manufacturing personnel. (N01)
Policy E – Increase manufacturing budget. (N02)

Each of these policies lessens the probability of failure of the component it involves, and has a reliability and cost associated with it as seen in Tables XI.3.1 and XI.3.2. When these policy changes are folded back through the tree, the result is a new probability of failure for the first tier (i.e., probability of introducing a faulty product). Table XI.3.2 lists the policies with their associated probabilities of system failure (introducing the faulty product) after the option is implemented, and the cost of each option.

Table XI.3.2. Summary of Policy Costs and Probabilities of System Failure

Policy	Changes in Reliability	Cost
A	Nothing	\$0
B	R(N22) = 0.9667	\$10,000
C	R(N31) = 0.9765	\$20,000
D	R(N01) = 0.9870	\$30,000
E	R(N02) = 0.9975	\$40,000

Using the probabilities of failure assigned to each component (i.e., the contribution of each component to the failure of the top event) on the *Policy A: Do Nothing*, we propagated the probability of failure up the tree according to the rules in the book. For instance, calculating the probability through an "or" gate is done by: P(A or B) = P(A) + P(B) – P(AB). We assumed all our component failures to be independent, so that P(AB) = P(A)*P(B). We had all "or" gates, which uses the rule just mentioned, or attachments, where the probability from the previous node is just folded up the tree. Using this fault tree method, we found the probability of introducing a faulty product (the undesired event on the first tier) to be .0306.

Since all the subsystems (or basic events) are connected in series, the system fails when at least one of its components fails. Thus, the reliability of the entire system is just a multiplication of the reliability of all the subsystems. The overall system reliability for each policy option is summarized in Table XI.3.3.

Table XI.3.3. Summary of Probabilities of System Reliability and Failure

Policy	Probability of System Reliability	Probability of System Failure
A	0.6569	0.3431
B	0.6897	0.3103
C	0.6897	0.3103
D	0.6897	0.3103
E	0.6897	0.3103

We graph the options in Figure XI.3.3, with the x-axis as the probability of system failure and the y-axis as the cost of the policy, and the Pareto-optimal frontier is formed by connecting all the points except for Policy E. (Policy E is dominated by the policies along the Pareto-optimal frontier line below it.) We would then use tradeoff analysis to determine acceptable tradeoffs between the cost and probability of system failure, to decide which policy to use.

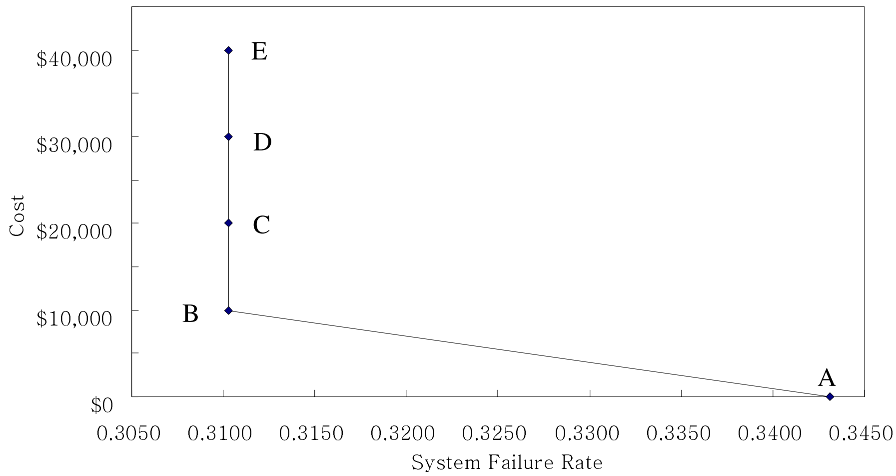

Figure XI.3.3. Cost and Probability of System Failure for each policy options

ANALYSIS

Since the reliabilities for Policies B, C, D, and E are same, the best policy option would be B. By choosing Policy B, the decisionmaker could decrease the system's failure rate by more than 10% at an expense of only $10,000.

PROBLEM XI.4: Reliability of a Machine Gun

The machine gun is a complex system that requires its many parts to be reliable. The top risk event that occurs is that the gun fails to shoot all the bullets in its magazine.

DESCRIPTION

Figure XI.4.1 shows how a machine gun with a gas system works, before the trigger is pulled. Each component must work properly for a round of bullets to be fired and reloaded.

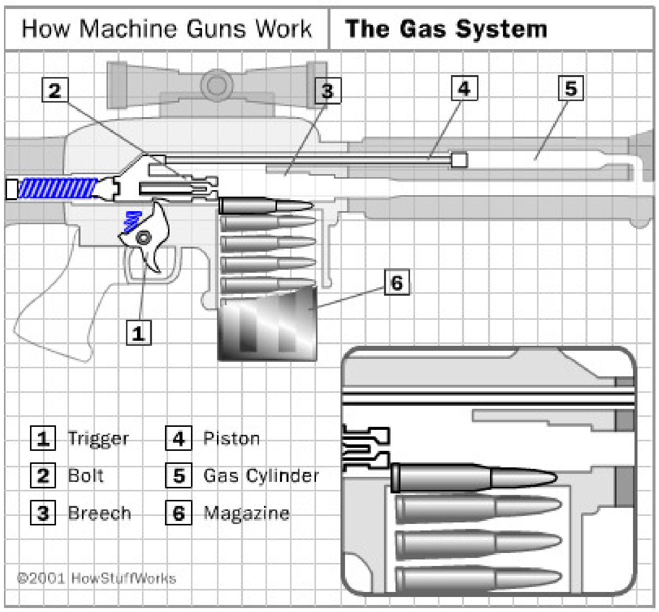

Figure XI.4.1. Machine Gun before Failure Event
(Source: www.howstuffworks.com)

For the gun to function perfectly, first the rear spring must begin to move forward. As this happens, the lower part of the bolt starts to move forward, pushing a bullet up into the breach. The bolt continues to move forward and locks into the barrel of the gun, pushing the bullet through. The expanding gases caused by this process get pushed up into the cylinder above the barrel. The piston then gets pushed backward, causing the bolt to unlock from the barrel. This allows a new bullet to enter the breach, starting the process over again. Figure XI.4.2 shows a machine gun in action, after the trigger has been pulled.

METHODOLOGY

The reliability of the machine gun components can be evaluated using fault tree analysis. The three main steps are:

1. Construct a fault tree for a machine gun.
2. Find the minimal cut set(s).
3. Show the real general reliability of a machine gun.

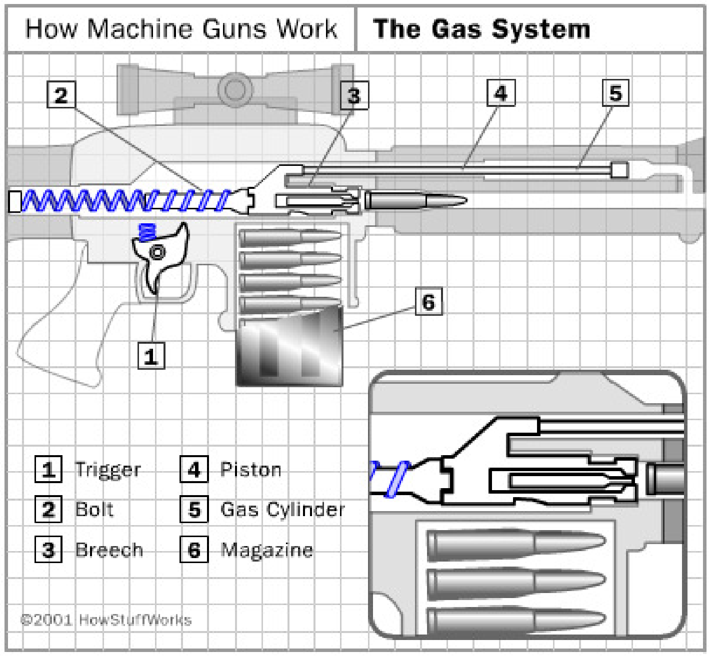

Figure XI.4.2. Machine Gun in Action
(Source: www.howstuffworks.com)

SOLUTION

The following notations are used to characterize the events in the fault tree:

Top Event: T = Gun fails to shoot all bullets in magazine

Intermediate and basic initiating events:
E_1 = Problem with Firing Mechanism
E_2 = Problem with Bullet Cartridge
E_3 = Problem with Reloading Mechanism
E_4 = Problem with Belt Feed
E_5 = Problem with Ejection System
A = Trigger gets jammed
B = Rear Spring fails to move forward
C = Bolt fails to attach to Barrel
D = Piston gets stuck
F = Primer fails

G = Feed Cam fails
H = Ammunition Belt Link breaks
I = Belt-feed Pawl fails
J = Ejector fails
K = Extractor fails

Figure XI.4.3 represents the fault tree for the machine gun.

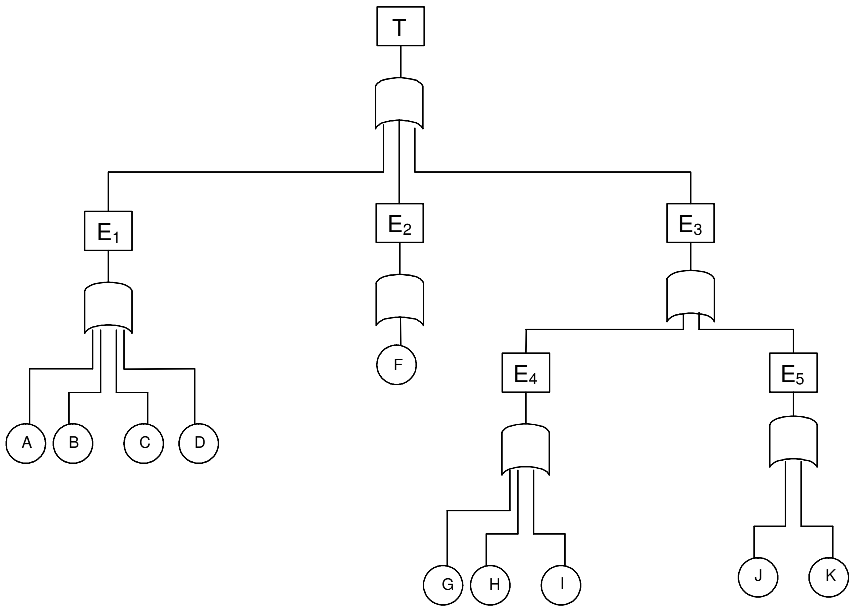

Figure XI.4.3. Fault Tree for Machine Gun

It is clear that there are no parallel components; thus everything must work in order for the system to work. Simplifying the fault tree gives us:

T = (A + B + C + D) + F + {(G + H + I) + (J + K)}
= A + B + C + D + E + F + G + H + I + J + K

Thus, the minimal cut sets are A, B, C, D, F, G, H, I, J, K.

ANALYSIS

When subsystems are connected in series, the system fails when at least one of its components fails. Thus, the reliability of the system is equal to the multiplied reliability of each component. The notation *t* denotes time as component reliabilities are expected to diminish.

$$R(t) = R_A(t)R_B(t)R_C(t)R_D(t)R_F(t)R_G(t)R_H(t)R_I(t)R_J(t)R_K(t)$$

However, remember that the process of firing and reloading must occur successfully for each bullet in the magazine. Thus, the real reliability of the system is $[R(t)]^n$ where n represents the number of bullets in the magazine.

PROBLEM XI.5: Reliability Analysis of an Airplane System

Calculate the reliability of a simplified airplane system with 11 components.

DESCRIPTION

Consider a simple airplane system with the following components:

3 Processors: P_1, P_2, P_3
2 Buses: C_1, C_2
Engine: E
- Motor: M
- Electrical: EL
- Cooling: EC

Navigator: N
- Type I: I
- Type II: T
  - Aviator: A
  - Compass: K

where M_1, etc. is defined as the probability of component failure.

METHODOLOGY

A Fault Tree Analysis is useful to calculate the airplane's reliability. By simplifying the system through minimal cut sets, the reliability of the overall system can be calculated. The final step is to check the importance of each minimal cut set. Figure XI.5.1 shows the fault tree.

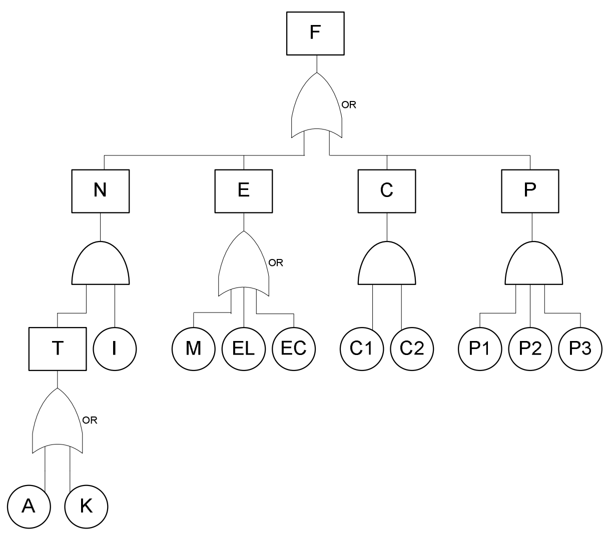

Figure XI.5.1. Fault tree diagram of airplane system

SOLUTION

The probability of system failure, F, is:

$$
\begin{aligned}
F &= N + E + C + P \\
&= (I \bullet T) + (M + EL + EC) + (C_1 \bullet C_2) + (P_1 \bullet P_2 \bullet P_3) \\
&= I(A + K) + M + EL + EC + C_1 \bullet C_2 + P_1 \bullet P_2 \bullet P_3
\end{aligned}
$$

$$F = \underbrace{I \bullet A}_{M_1} + \underbrace{I \bullet K}_{M_2} + \underbrace{M}_{M_3} + \underbrace{EL}_{M_4} + \underbrace{EC}_{M_5} + \underbrace{C_1 \bullet C_2}_{M_6} + \underbrace{P_1 \bullet P_2 \bullet P_3}_{M_7}$$

Thus, the minimal cut set is:

$$I \bullet A + I \bullet K + M + EL + EC + C_1 \bullet C_2 + P_1 \bullet P_2 \bullet P_3$$

Now, let us define the probability failures set for $t = 100$ hours:

P_i:	0.1
C_i:	0.25
M:	0.02
EL:	0.04
EC:	0.09
I:	0.2
A:	0.08
K:	0.07

Minimal cut set unreliabilities are:

$Q_1 = 0.016$	{0.2•0.08}
$Q_2 = 0.014$	{0.2•0.07}
$Q_3 = 0.02$	
$Q_4 = 0.04$	
$Q_5 = 0.09$	
$Q_6 = 0.0625$	{0.25•0.25}
$Q_7 = 0.001$	{0.1•0.1•0.1}

$$Q_s = \sum_{i=1}^{7} Q_i \qquad \Rightarrow \qquad Q_s = 0.2435 \qquad \text{(Total System Unreliability)}$$

The importance ratio of each component of the minimal cut set (normalized with respect to Q_s) is as follows:

$$E_i = \frac{Q_i}{Q_s}$$

$$E_1 = 6.6\ \%$$
$$E_2 = 5.7\ \%$$
$$E_3 = 8.2\ \%$$
$$E_4 = 16.4\%$$
$$E_5 = 37.0\ \%$$
$$E_6 = 25.7\ \%$$
$$E_7 = 0.4\ \%$$

ANALYSIS

Seen in the importance of a minimal cut set, E_5 is the most critical to the reliability of an airplane system because it is responsible for 37% of unreliability in the system. Therefore, a system engineer in the airplane manufacturing plant should focus on maintaining or improving the reliability of E_5, which is *cooling*.

PROBLEM XI.6: Electric Power Demand

Preventing electric-power failure is an ongoing infrastructure concern A power generating plant is at risk of not fulfilling its electric power demand. Figure XI.6.1 displays the fault tree for the current system where the top event (T) corresponds to unfulfilled demand.

Construct a fault tree of the potential power demand failure and derive minimal cut sets in the analysis.

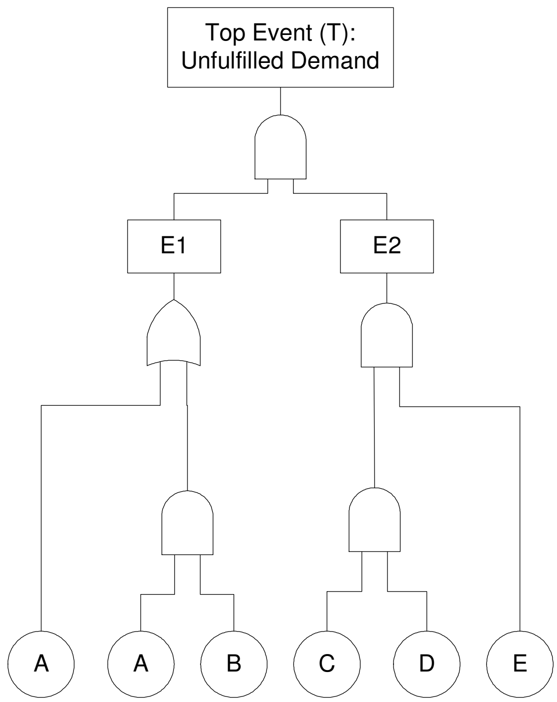

Figure XI.6.1. Fault Tree for Electric Power Demand

Intermediate and basic initiating events:

E1 = Failure of System 1
A = Failure of Generator A
B = Failure of Generator B
E2 = Failure of back-up System 2
C = Insufficient stock (inventory) of coal
D = Delayed delivery of coal
E = Delayed delivery of oil and gas

PROBLEM XI.7: Reliability Analysis of a Bicycle Brake System

A 10-speed bicycle has two identical brake systems, one for each wheel. These systems are totally independent and both must fail for the entire brake system to fail. Basic risk scenarios for each are a brake pad failure, a brake cable failure, and a lever failure. Any of these will cause a component system to fail.

It is useful to do a Fault Tree Analysis and simplify the system through minimal cut sets. With this procedure, we can easily figure out the reliability of the overall system and check the importance of each minimal cut set.

The Fault Tree is shown in Figure XI.7.1:

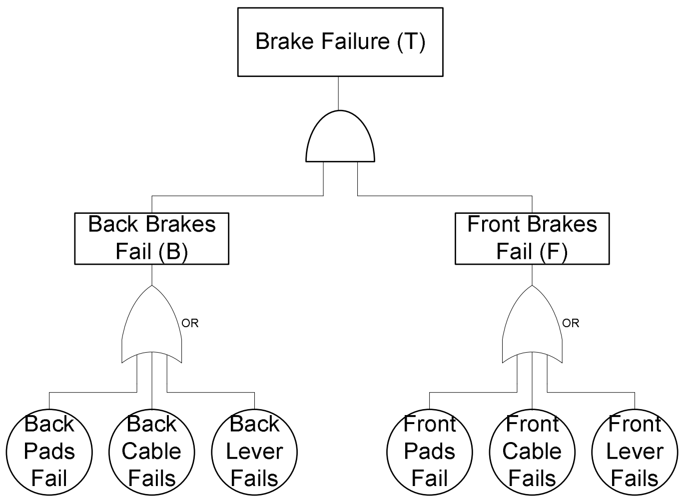

Figure XI.7.1. Fault tree diagram of bicycle brake system

Based on the above fault tree derive the minimal cut sets and analyze your results.

PROBLEM XI.8: Fault-Tree Analysis of a Train Wreck

This exercise examines a simple train wreck scenario using fault tree analysis.

Five factors (or risk scenarios) have been identified to contribute to a disastrous train wreck event as follows:

A. Excessive Speed
B. Mechanical Failure on Train (e.g., brakes, engine)
C. Obstruction on Tracks
D. Improper Switching (e.g., transfer to wrong track)
E. Incorrect Signaling (e.g., stop instead of go)

The following probabilities for the above five factors are given as follows:

$P(A) = 0.25$
$P(B) = 0.00025$
$P(C) = 0.01$
$P(D) = 0.00010$
$P(E) = 0.00010$

Assumptions:

1) An obstruction on the track is not enough to cause a wreck <u>in itself</u> (we assume for this problem that once an obstruction is seen, there is sufficient time to come to a stop before impact)
2) We have purposely omitted human error since it plays into many parts of the tree and since its impact is different to analyze.
3) Excessive speed is also not sufficient to cause a train wreck (many times trains will speed up in order to reduce late arrivals), but it can lead to an accident if complied with other factors.

The train wreck scenario is analyzed using the fault tree depicted in Figure XI.8.1. In addition to the five factors specified in the problem description, the following hierarchies of events are denoted as follows:

T = Train Wreck
E_1 = Hitting Something
E_{11} = Hitting Something due to excessive speed
E_{12} = Hitting Something due to malfunction of train
E_2 = Malfunction
E_{21} = Train Malfunction
E_{22} = Outside Malfunction

Derive minimal cut sets from given the fault tree, calculate the reliability of the train and the importance of each minimal cut set in the analysis and analyze your results

PROBLEM XI.9: Reliability of a Combat Helicopter Computer Chip

The objective of this problem is to maximize the reliability of a circuit-chip subsystem for a helicopter mission of 3-hour duration.

An integrated circuit chip for use in the computer for a combat helicopter has a mean failure rate of 0.05 ($\lambda = 0.05$) per hour, and a standard deviation of 0.02 (assuming normal distribution). The cost of each chip is $100. Maximizing the reliability of this circuit chip can be done by placing the chips in parallel.

The failure rate for such a parallel system is given by λ^n, where N is the total number of parallel components used. Assume that the standard deviation of the parallel system is the same as for each individual chip.

Suppose N identical components are tested for one time period. Let $N_f(t)$ be the number of components that have failed, and $N_O(t)$ be the number of components that are operating. The failure rate (λ) of the components is given by

$$\lambda = \frac{N_f(t)}{N} = \frac{N_f(t)}{N_O(t) + N_f(t)}$$

The reliability $R(t)$ of a system is defined as the conditional probability that a system performs correctly throughout an interval of time [t_0, t], given that the system was performing correctly at time t_0. For components having exponential time to failure distribution, the reliability is given by

$$R(t) = e^{-\lambda t}$$

You may want to use the following equations:

$$f_4^N(\cdot) = \mu + \sigma\sqrt{2\ln(n)}$$

(i) Consider 4 design options for the chip subsystem, each with 1, 2, 3, and 4 chips in parallel. Compute the mean reliability of the subsystem for the 3-hour mission for each of the four design options.

(ii) Calculate $f_4(\cdot)$ for each design option for a partition point of 85 % on the reliability axis (see hint).

(iii) Calculate $f_4(\cdot)$ for each design option using a partition point of 0.99 on the probability axis.

Hint: To compute the partition point on the probability axis from the partition point on the reliability axis, calculate the corresponding value of the failure rate using

$$R(t) = e^{-\lambda t}$$

PROBLEM XI.10: SCADA System Reliability

Supervisory Control and Data Acquisition (SCADA) systems have now been widely used in the manufacturing industry to control production. This problem deals with improving their reliability.

Figure XI.10.1 shows a typical SCADA system that consists of a number of Programmable Logic Controllers (PLCs). This SCADA system uses four types of PLCs as shown in Figure XI.10.1: PLCs 1, 2, 3, and 4. Their reliabilities are: PLC 1 - 0.95; PLC 2 - 0.93; PLC 3 - 0.95; and PLC 4 - 0.94. Four plans are proposed to improve the overall reliability of the current SCADA system.

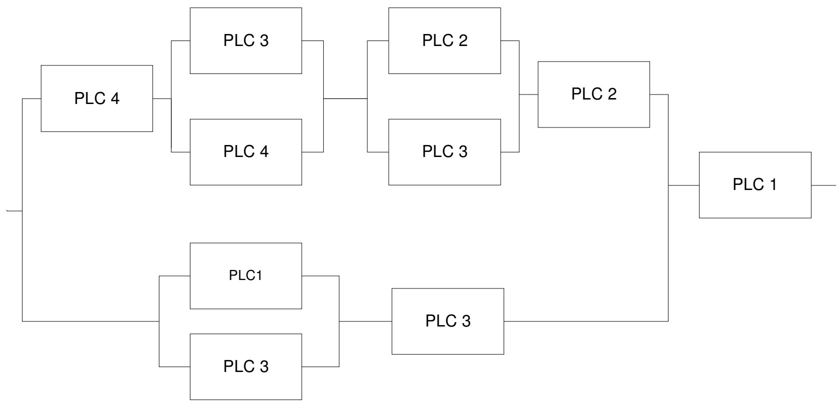

Figure XI.10.1. SCADA System for Manufacturing Control

Each plan suggests replacing one PLC with a more reliable new design. The reliability and estimated costs are as follows:

A: PLC 1—0.99 reliability—$600,000
B: PLC 2—0.95 reliability—$100,000
C: PLC 3—0.98 reliability—$400,000
D: PLC 4—0.95 reliability—$200,000

Build a fault tree and derive the minimal cut set for the above SCADA System. Compute the probabilities of failure for each option and analyze the results.

PROBLEM XI.11: Computer System Risk

The purpose of this research is to determine the overall probability of computer failure given the probability of failure of each of its essential components.

The modern computer is made up of various components, some of which are more independent than others. However, they are all essential in order for the computer to be fully operational. Any parts that are not necessary, such as those installed to increase reliability or additional functionality, will not be depicted in the following fault tree analysis.

For this fault tree analysis example, we will decompose the computer into three categories: 1) *motherboard* and *motherboard-connected devices,* 2) *hard drives,* and 3) *power supply.* These can be decomposed further into other devices and possible failure events. See Figure XI.11.1 below for more details.

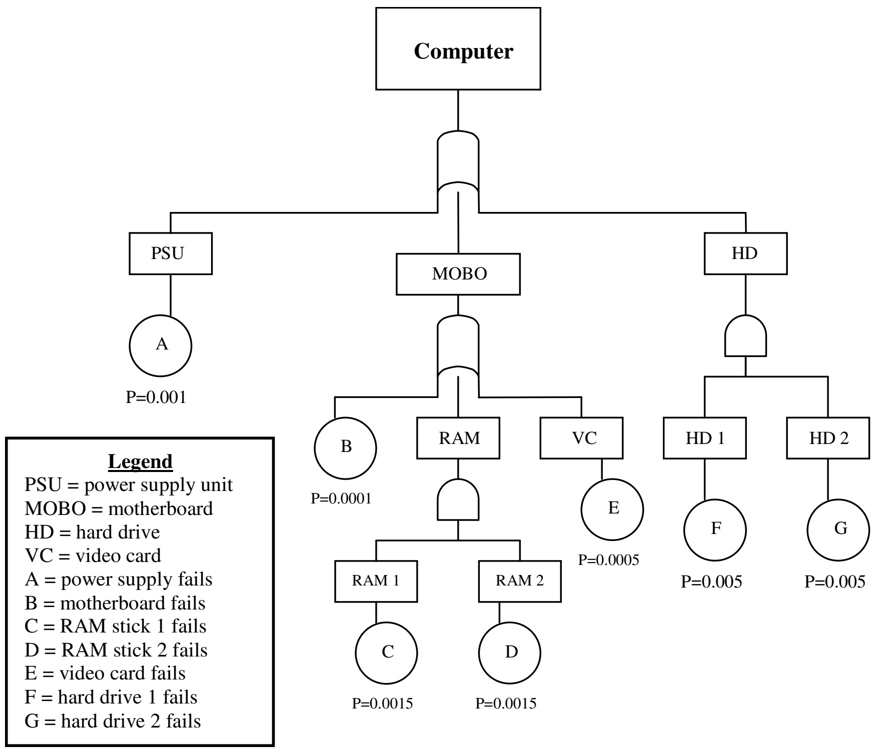

Figure XI.11.1. Fault Tree for Analyzing Computer Risk

Derive the minimal cut set in above the fault tree and compute the probability of a computer failure. Analyze your results.

PROBLEM XI.12: Calculating Reliability of an Electronic Subsystem

This problem will demonstrate how to model the reliability of a simplified electronic product. An electronic product will be dissected part by part and aggregated by functional groups.

The electronic subsystem consists of three components, A, B, and C. They are constructed and connected as shown in Figure XI.12.1:

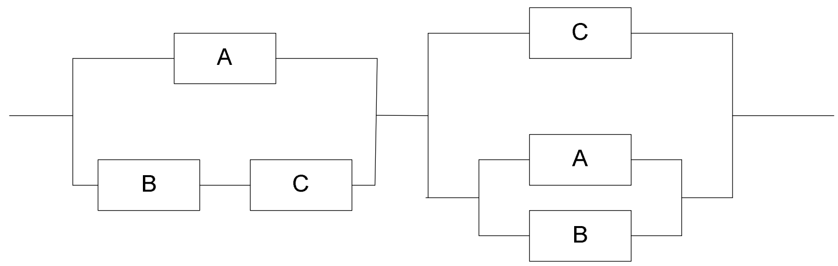

Figure XI.12.1. Simplification of an Electronic Subsystem

Given the component reliabilities of $R_A(t)=0.9$, $R_B(t)=0.8$, $R_C(t)=0.7$, do the following:

1. Draw the fault tree.
2. Find the minimal cut sets.
3. Calculate the reliability of the entire system.

PROBLEM XI.13: Purchasing a New Machine

A company is considering installing a new machine in its factory. Before making the purchase, the top executives want to know how long the machine can survive before it fails to run.

The failure rate of a machine is defined as follows:

$$\lambda(t) = \begin{cases} \lambda_1 & 0 \le t \le a \\ \lambda_2 & t \ge a \end{cases}$$

For this problem:

(a) Derive the reliability function $R(t)$.

(b) Derive the failure density function $f(t)$.

(c) If a = 30 months, $\lambda_1 = (1200 \text{ months})^{-1}$, and $\lambda_2 = (600 \text{ months})^{-1}$, calculate the time such that the machine's reliability will have degraded to a value of 0.95.

(d) Calculate the mean time to failure (MTTF) given the parameters in (c).