PROBABILISTIC AND POSSIBILISTIC FAULT TREE ANALYSIS

12/28/2017

INTRODUCTION

In the design of nuclear power plants, it is important to analyze the probable and possible mechanisms of failure. Fault Tree Analysis is such a method of analysis where primary events that interact to produce secondary events can be related using simple logical relationships such as the OR, the AND, and the NOT logical operations.

A system function diagram or flow diagram is first constructed to show the pathways by which signals and materials flow between the system's components. A functional logical tree diagram is then constructed to depict the logical relationships of the different components to the overall system functioning. Successive failure events that can contribute to cause a "top event" described by the system's fault tree are then identified and linked to the top event by logical connective functions expressed through the Boolean expression of the tree.

INTERSECTION OF EVENTS: THE AND LOGIC GATE

It is natural to talk about the intersection of two events, A_1 and A_2, which is denoted as:

$$A_1 \cap A_2 \ or \ A_1 A_2$$

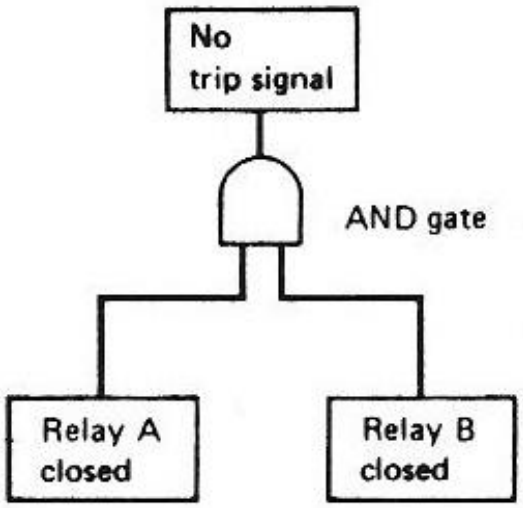


Fig.1: AND logical of an electrical system.

The product rule of probabilities can be stated to estimate the probability of occurrence of A_1 and A_2 as:

$$\begin{aligned} P(A_1A_2) &= P(A_1 \mid A_2)P(A_2) \\ &= P(A_2 \mid A_1)P(A_1) \end{aligned} \tag{1}$$

In general, if the events A_1 and A_2 are independent, then:

$$P(A_1 \mid A_2) = P(A_1)$$
$$P(A_2 \mid A_1) = P(A_2)$$

And subsequently if the events A_i are "mutually independent," then:

$$P(A_1A_2) = P(A_1)P(A_2) \tag{2}$$

And in general:

$$P(A_1A_2...A_N) = P(A_1)P(A_2)P(A_3)...P(A_N) \tag{3}$$

If the events are "mutually exclusive," then:

$$P(A_1A_2...A_N) = 0 \tag{4}$$

In possibility theory, the possibility of the intersection of the two events A_1 and A_2 is:

$$\Pi(A_1A_2) = Min[\Pi(A_1), \Pi(A_2)] \tag{5}$$

And in general:

$$\Pi(A_1A_2...A_N) = Min[\Pi(A_1), \Pi(A_2), \Pi(A_3), ..., \Pi(A_N)] \tag{6}$$

UNION OF EVENTS: THE OR LOGIC GATE

The union of two events, A_1 and A_2, is denoted as:

$$A_1 \cup A_2 \ \ or \ \ A_1 + A_2$$

Both symbols mean: A_1 OR A_2.

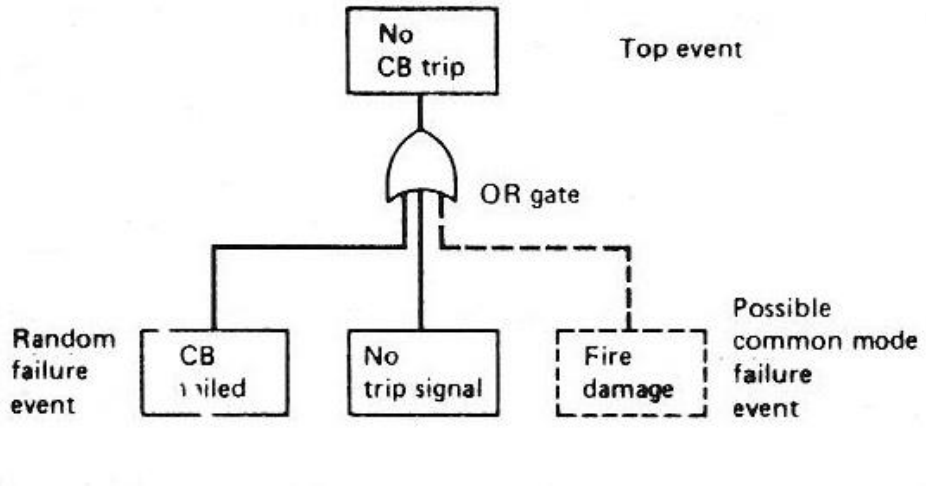


Fig. 2: OR logical gate of the failure of a circuit breaker to trip.

The probability of the union of two events A_1+A_2 is:

$$P(A_1 + A_2) = P(A_1) + P(A_2) - P(A_1A_2) \tag{7}$$

If the two events are independent, it follows from Eqn. 2 that:

$$P(A_1 + A_2) = P(A_1) + P(A_2) - P(A_1)P(A_2) \tag{8}$$

In general, for N events, we get the summation form:

$$\begin{aligned} P(A_1 + A_2 + \ldots A_N) = & \sum_{n=1}^{N} P(A_n) \\ & - \sum_{n=1}^{N-1} \sum_{m=n+1}^{N} P(A_n A_m) \\ & + \sum_{n=1}^{N-2} \sum_{m=n+1}^{N-1} \sum_{k=n+2}^{N} P(A_n A_m A_k) \\ & - \ \ldots \\ & + (-1)^{N-1} P(A_1 A_2 \ldots A_N) \end{aligned} \tag{9}$$

This Eqn. 9 also takes the simpler product form:

$$P(A_1 + A_2 + \ldots A_N) = 1 - \prod_{n=1}^{N} [1 - P(A_n)] \tag{10}$$

If the events are independent and highly infrequent, Eqn. 9 reduces to:

$$P(A_1 + A_2 + ...A_N) \simeq \sum_{n=1}^{N} P(A_n) \tag{11}$$

In possibility theory, the possibility of the events A_1 or A_2 becomes:

$$\Pi(A_1 + A_2) = Max[\Pi(A_1), \Pi(A_2)] \tag{12}$$

And in general:

$$\Pi(A_1 + A_2 + ... + A_N) = Max[\Pi(A_1), \Pi(A_2), \Pi(A_3), ..., \Pi(A_N)] \tag{13}$$

BOOLEAN ALGEBRA OF EVENTS

Some of the rules or laws of the Boolean algebra of events are here listed:

1. Commutative law

$$\begin{aligned} XY &= YX \\ X + Y &= Y + X \end{aligned} \tag{14}$$

2. Associative law

$$\begin{aligned} X(YZ) &= (XY)Z \\ X + (Y + Z) &= (X + Y) + Z \end{aligned} \tag{15}$$

3. Idempotent law

$$\begin{aligned} XX &= X \\ X + X &= X \end{aligned} \tag{16}$$

4. Absorption law

$$\begin{aligned} X(X + Y) &= X \\ X + XY &= X \end{aligned} \tag{17}$$

5. Distributive law

$$\begin{aligned} X(Y + Z) &= XY + XZ \\ (X + Y)(X + Z) &= X + YZ \end{aligned} \tag{18}$$

6. Complementation

$$
\begin{aligned}
&X\bar{X} = \varnothing, \textit{ null event} \\
&X + \bar{X} = \Omega, \textit{ universal event} \\
&\bar{\bar{X}} = X
\end{aligned}
\tag{19}
$$

7. De Morgan's theorems

$$
\begin{aligned}
&\overline{XY} = \bar{X} + \bar{Y} \\
&\overline{X + Y} = \bar{X}\bar{Y}
\end{aligned}
\tag{20}
$$

8. Other relations

$$
\begin{aligned}
&X + \bar{X}Y = X + Y \\
&\bar{X}(X + Y) = \bar{X}\bar{Y}
\end{aligned}
\tag{21}
$$

In possibility theory, all these axioms apply except that the law of the excluded middle does not apply:

$$
\begin{aligned}
&X\bar{X} \neq \varnothing \\
&X + \bar{X} \neq \Omega
\end{aligned}
\tag{22}
$$

In this case we are dealing with a De Morgan or Fuzzy Algebra.

FAULT TREE CONSTRUCTION

The construction of Fault Trees is both an art and a science. Some of the symbols commonly used in Fault Tree construction are shown in Fig. 3.

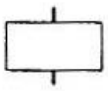
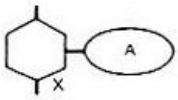
Symbol	Name	Description
	Rectangle	Fault event; it is usually the result of the logical combination of other events
	Circle	Independent primary fault event
	Diamond	Fault event not fully developed as to its causes; it is only an assumed primary fault event
	House	Normally occurring basic event; it is not a fault event
	OR Gate	The union operation of events; i.e., the output event occurs if one or more of the inputs occur
	AND Gate	The intersection operation of events; i.e., the output event occurs if and only if all the inputs occur
	INHIBIT Gate	Output exists when X exists and condition A is present; this gate functions somewhat like an AND gate and is used for a secondary fault event X
	Triangle-in	Triangle symbols provide a tool to avoid repeating sections of a fault tree, or to transfer the tree construction from one sheet to the next. The triangle-in appears at the bottom of a tree and represents that branch of the tree (in this case "A") shown someplace else. The triangle-out appears at the top of a tree and denotes that the tree "A" is a subtree to one shown someplace else.
	Triangle-out	

Fig. 3: Fault Trees commonly used symbols.

SYSTEM AND FAULT TREE DIAGRAMS

An example of the construction of a fault tree is the failure of a mechanical holding latch shown in Fig. 4.

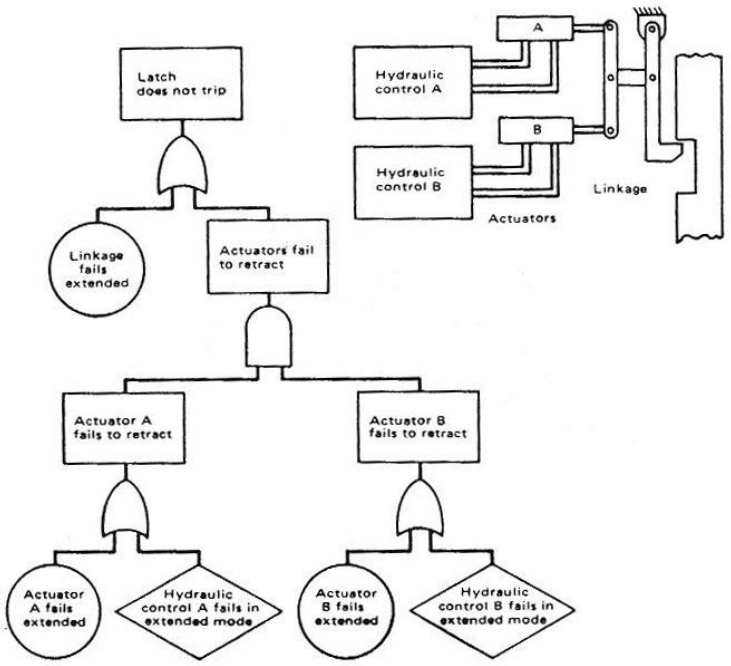


Fig. 4: Fault tree for a mechanical holding latch mechanism.

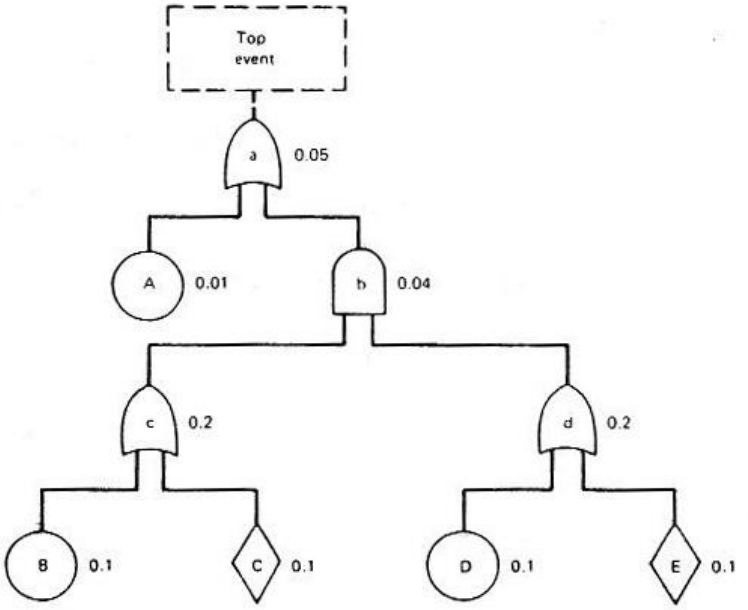


Fig. 5: Fault Tree showing the failure probabilities propagation in the tree.

BOOLEAN EXPRESSION, GRAPHICAL AND ANALYTICAL FAULT TREE CALCULATIONS

The fault tree of Fig. 4 can be shown in a coded form in Fig. 5. It can thus be described by asset of Boolean algebraic equations for each logical gate in the tree.

Let us use small letters to code the logical gates, and capital letters to code the basic events. For the mechanical latch mechanism we use:

A: the linkage fails in extended mode
B: the actuator A fails in the extended mode
C: the control element A fails in the extended mode
D: the actuator B fails in the extended mode
E: the control element B fails in the extended mode

We now can write the following Boolean logical statements describing the functioning of the latch mechanism in terms of the basic input events:

$$\begin{aligned} a &= A + b \\ c &= B + C \\ b &= cd \\ d &= D + E \end{aligned} \tag{23}$$

Through substitution, we can express the top failure event in terms of the primary basic events as:

$$\begin{aligned} a &= A + b \\ &= A + cd \\ &= A + (B + C)(D + E) \end{aligned} \tag{24}$$

Using the rules of a Boolean Algebra we can get the Boolean expression for the top failure event as:

$$a = A + BD + BE + CD + CE \tag{25}$$

The probability of occurrence of the top failure event becomes, using the small probabilities approximation:

$$\begin{aligned} P(a) &= P(A) + P(BD) + P(BE) + P(CD) + P(CE) \\ &= P(A) + P(B)P(D) + P(B)P(E) + P(C)P(D) + P(C)P(E) \end{aligned} \tag{26}$$

In possibility theory the possibility of the top event becomes:

$$\begin{aligned}\Pi(a) &= Max[\Pi(A), \Pi(BD), \Pi(BE), \Pi(CD), \Pi(CE)] \\ &= Max\{\Pi(A), \\ &\qquad Min[\Pi(B), \Pi(D)], \\ &\qquad Min[\Pi(B), \Pi(E)], \\ &\qquad Min[\Pi(C), \Pi(D)], \\ &\qquad Min[\Pi(C), \Pi(E)]\}\end{aligned} \tag{27}$$

EXAMPLE

If we are given the following failure probabilities:

$$P(A) = 0.01$$
$$P(B) = P(C) = P(D) = P(E) = 0.1$$

Substituting in Eqn. 11, we get for the probability of failure at the top event:

$$\begin{aligned}P(a) &= P(A) + P(B)P(D) + P(B)P(E) + P(C)P(D) + P(C)P(E) \\ &= 0.01 + (0.1)^2 + (0.1)^2 + (0.1)^2 + (0.1)^2 \\ &= 0.05\end{aligned}$$

This result could also be obtained by following the propagation of the probabilities in the graph of the Fault tree.

EXAMPLE

If we are given the following failure possibilities:

$$\Pi(A) = 0.01$$
$$\Pi(B) = \Pi(C) = \Pi(D) = \Pi(E) = 0.1$$

Substituting in Eqn. 27, we get for the possibility of failure at the top event:

$$\begin{aligned}\Pi(a) &= Max\{0.01, Min[0.1, 0.1], Min[0.1, 0.1], Min[0.1, 0.1], Min[0.1, 0.1]\} \\ &= Max\{0.01, 0.1, 0.1, 0.1, 0.1\} \\ &= 0.1\end{aligned}$$

This result could also be obtained by following the propagation of the posibilities in the graph of the Fault tree.

FAULT TREES OF COMPLEX SYSTEMS

Real life systems are more complex than the mechanical latch case. For instance, Fig. 6 shows the fault tree of an electric motor circuit. A primary failure event is that of the failure of the motor itself through a wiring failure.

The "switch opened" event is not developed for lack of information about the human error involved of leaving the switch open.

The event "fuse fails open" happens if a primary or secondary fuse failure occurs. The "secondary fuse failure" event occurs if the fuse does not open every time an overload is present in the circuit. The inhibit gate is used to account for the secondary failure.

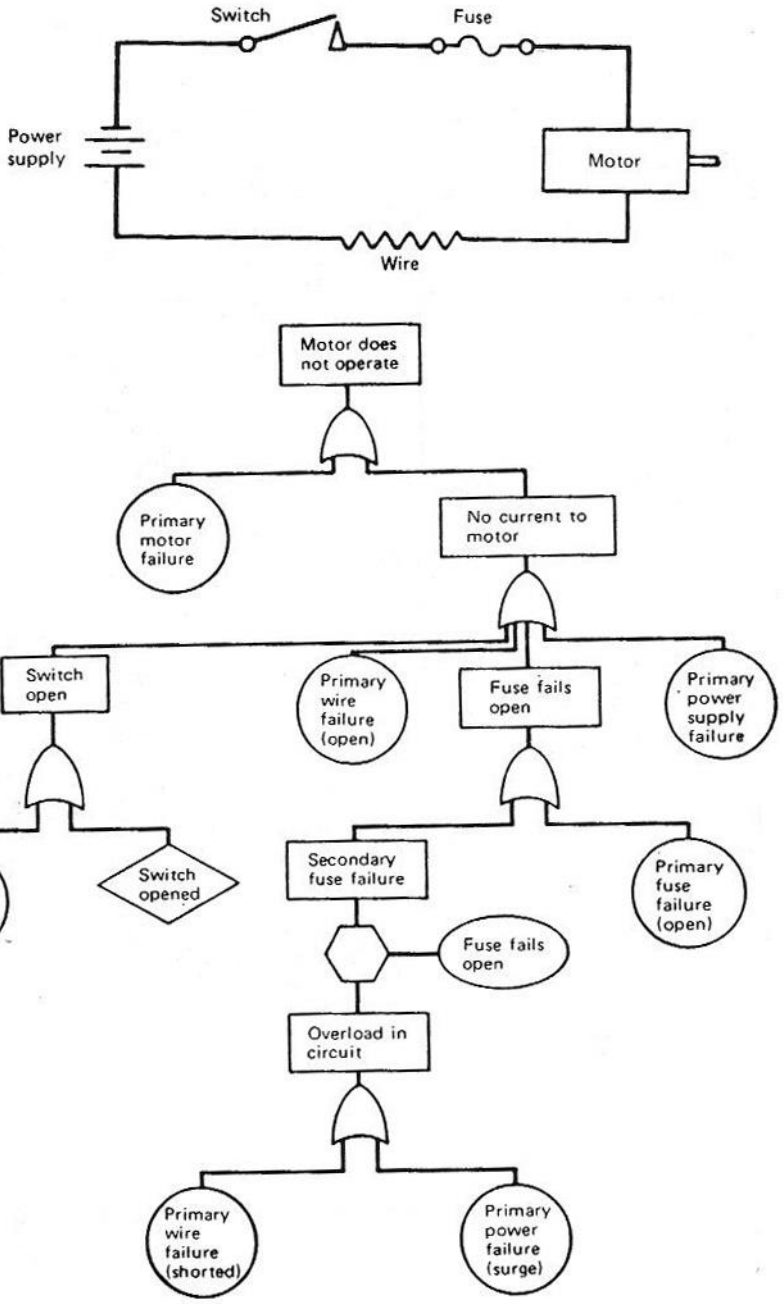


Fig. 6: Fault Tree of an electrical motor system.

NUCLEAR REACTOR TRIP FAULT TREE

A nuclear reactor is designed to "trip" or "scram" if an out of tolerance signal is received by a combination of sensors which are of different types. A diagram of such a trip logic is shown in Fig. 7.

The two trip logics monitor:

1. Two out of three logic matrix low pressure reactor transducers and instrumentation.
2. Two out of three logic matrix of temperature change transducers and instrumentation.
3. Three channels of reactor water level transducers and instrumentation.

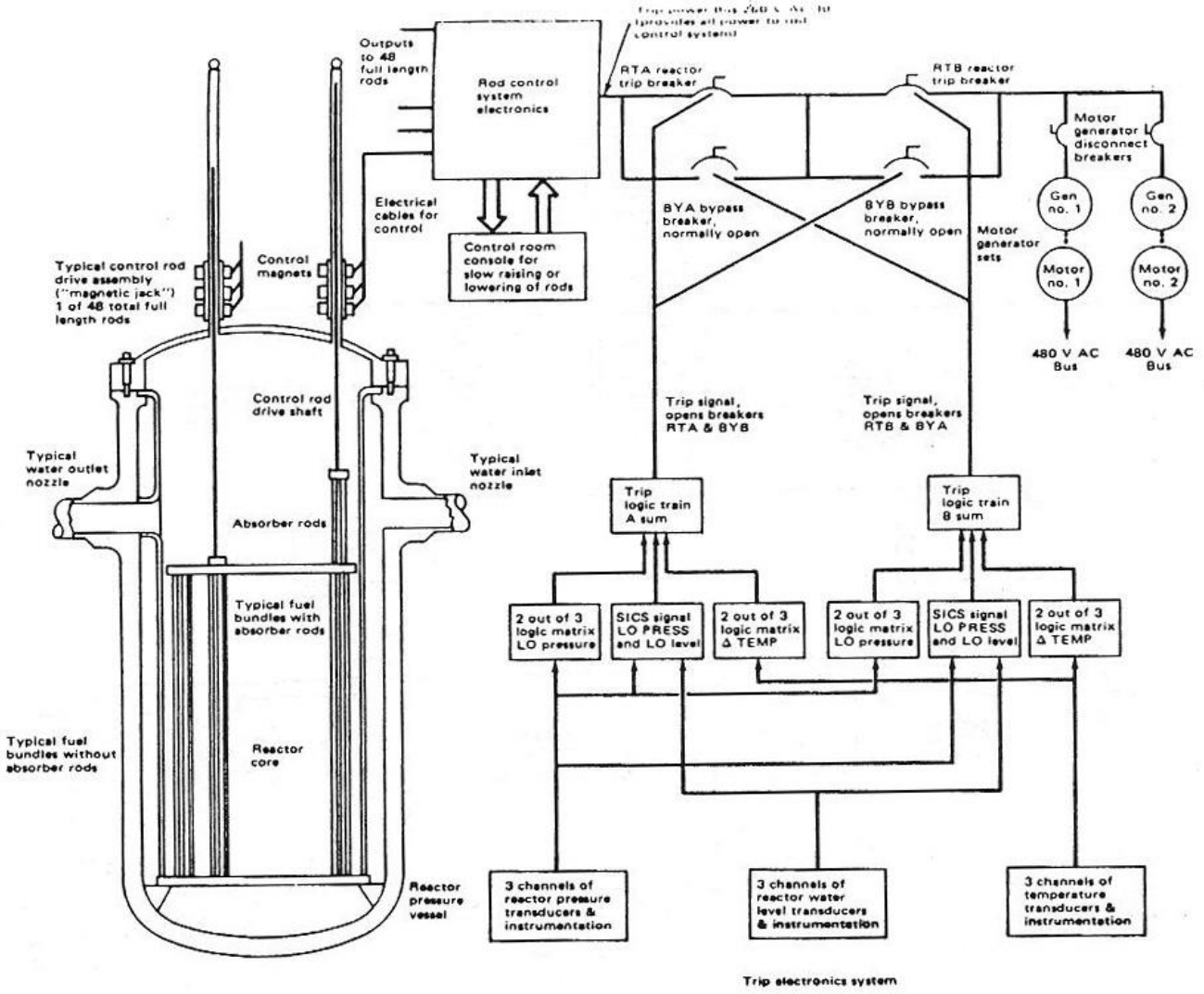


Fig. 7: Functional diagram of a nuclear reactor control rod protection system.

The fault tree representation could be quite complex as shown in Fig. 8. The trip system accounts for the control rods and their magnetic jack assembly.

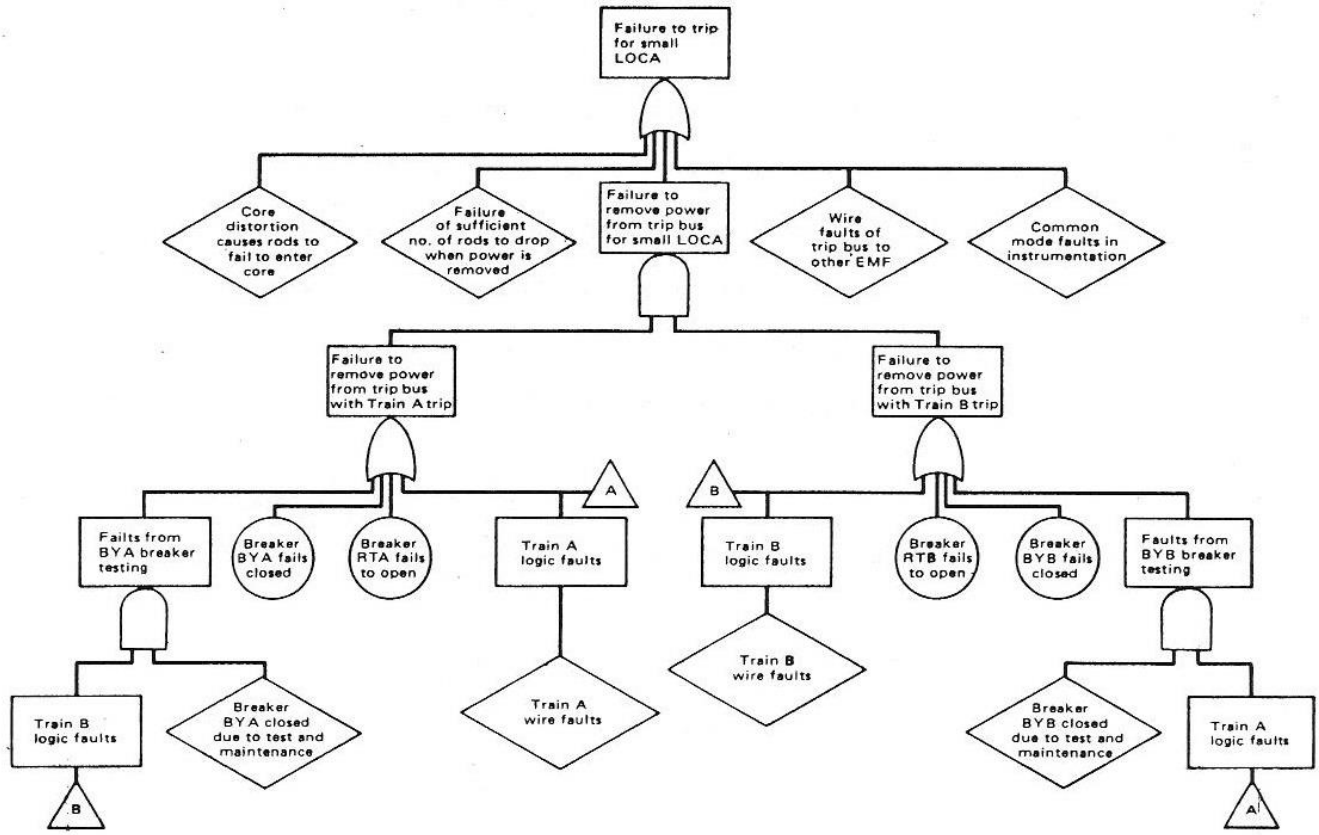


Fig. 8: Fault Tree for reactor protection system.

EXERCISE

1. Consider the Boolean expression that represents a Fault Tree:

$$T = A + (B.C.D) + (E.F.G)$$

a. Derive the expression for the Operational Tree as the complement: T'.
b. Graph the Fault Tree.
c. Graph the Operational Tree.
d. Calculate the probability of the top event T in the Fault Tree, using the small probabilities approximation, given the following probabilities:
$P(A) = P(B) = P(C) = P(D) = P(E) = P(F) = P(G) = 10^{-3}$.
e. Calculate the possibility of the top event T in the Fault Tree, given the following possibilities:
$\Pi(A) = 10^{-2}, \Pi(B) = 10^{-3}, \Pi(C) = 10^{-4}, \Pi(D) = 10^{-5}, \Pi(E) = 10^{-4}, \Pi(F) = 10^{-3}, \Pi(G) = 10^{-2}$.

2. Consider the Boolean expression that represents a Fault Tree:

$$T = A + (B.C) + (D.E)$$

a. Construct the corresponding Fault Tree.

b. Calculate the probability of the top event T,
if: $P(A)=10^{-2}, P(B)=10^{-3}, P(C)=10^{-4}, P(D)=10^{-3}, P(E)=10^{-2}$.
c. Calculate the possibility of the top event T,
if: $\Pi(A)=10^{-2}, \Pi(B)=10^{-3}, \Pi(C)=10^{-4}, \Pi(D)=10^{-3}, \Pi(E)=10^{-2}$.

3. Consider the Boolean expression that represents a Fault Tree:

$$T = A + (B.C)$$

a. Plot the Fault Tree.
b. Calculate the probability of the top event T in the Fault Tree, using the small probabilities approximation, given the following probabilities:
$P(A) = P(B) = P(C) = 10^{-3}$.
c. Modify the tree for the considered device to reduce its probability of failure and compare it to the reference case.

4. Calculate the possibility of the top event T in the Fault Tree: $T = A + (B.C)$, given the following possibilities:
$\Pi(A)=10^{-2}, \Pi(B)=10^{-3}, \Pi(C)=10^{-4}$.
Is it feasible to modify the tree for the considered device to reduce its possibility of failure compared with the reference case?