POLITECNICO DI MILANO

Logical Methods:
Fault Tree & Event Tree

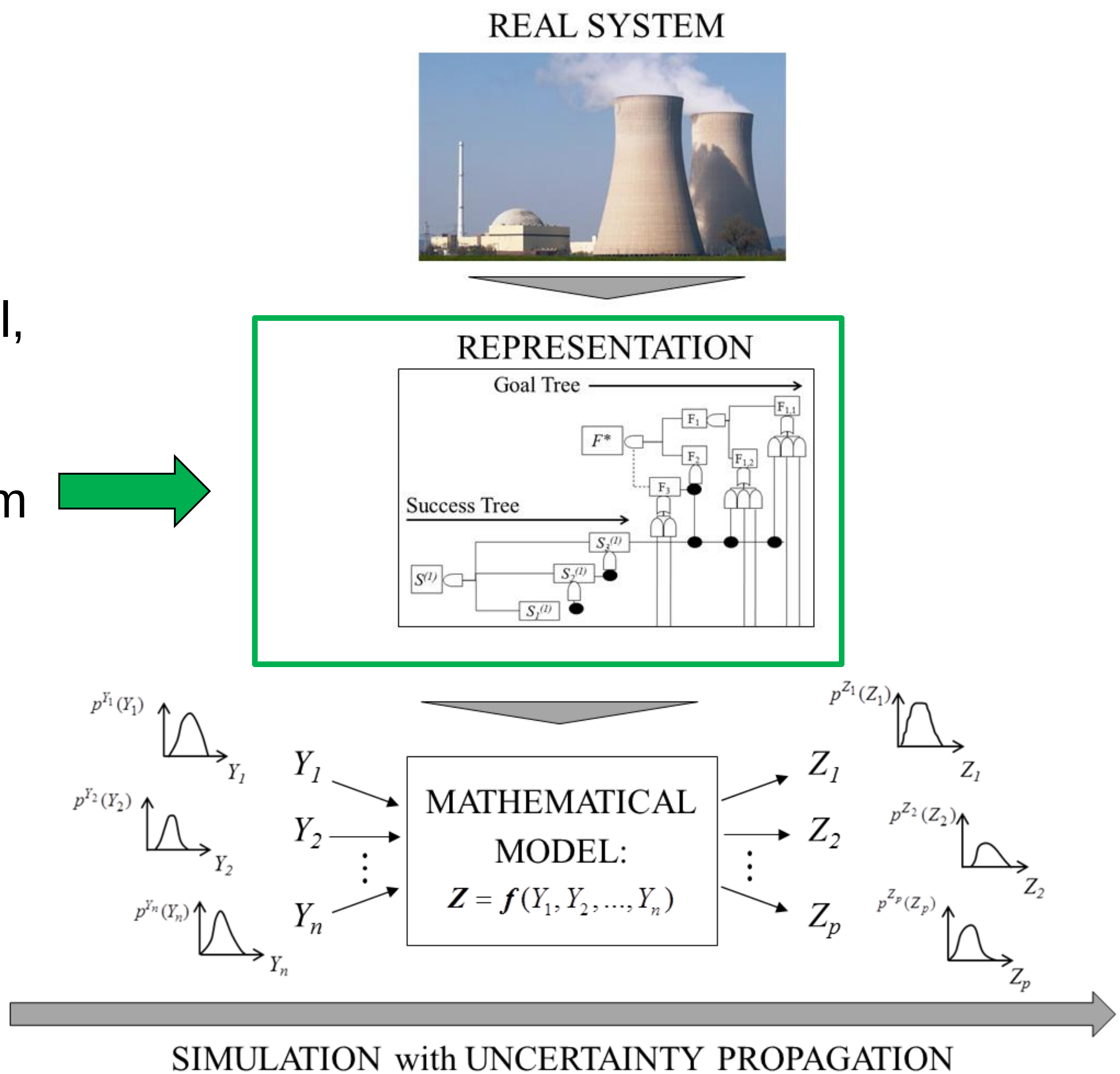
Ibrahim Ahmed
Dipartimento di Energia
Via La Masa 34, B12

ibrahim.ahmed@polimi.it

System representation

(complex) System representation

Definition of the structural, logical and functional relations among the components of the system



System representations in the scientific literature

Three main types of system representation techniques exist:

- Phenomenological/Functional methods
- Graph structure
    - Structural methods
    - Flow methods
- Hierarchycal
    - Logical methods (e.g., Fault Tree / Event Tree, Goal Tree Success Tree + (Dynamic) Master Logic Diagram)

Methods

Vulnerability assessment of CIs

- **Phenomenological/ Functional methods**
  e.g., Agent Based Modeling and Simulation, System Dynamic Model, Economic-Based Approaches, …
- **Structural/ Topological methods**
  e.g., Topology-based approaches
- **Flow methods**
  e.g., Flow-based approaches (maximum flow model, …)
- **Logical methods**
  e.g., Fault/Event trees, Probabilistic Modeling (Markov Chains, Bayesian network, …)

Logical methods: characteristics

Logical methods are:

- **apt to representation**;
- capable of capturing the **logic of the functioning/dysfunctioning** of a complex system;
- capable of identifying the **combinations of failures of elements** (hardware, software, and human and organization), which lead to the **loss of the system-of-systems function**.

Logical Methods:
Fault Tree

Objectives

1. Decompose the system failure in elementary failure events of constituent components
2. Computation of system failure probability, from component failure probabilities

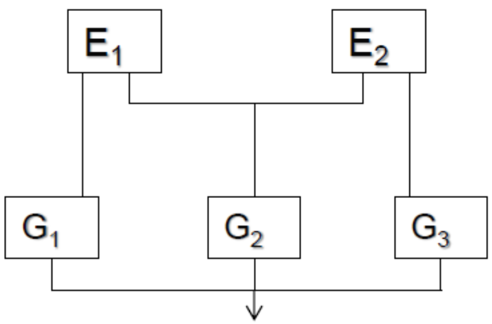
Fault Tree (FT)

- Systematic and quantitative
- Deductive (search for causes)

FT construction: Procedure steps

1. Define top event (system failure)

Electrical generating system



E1, E2 = engines

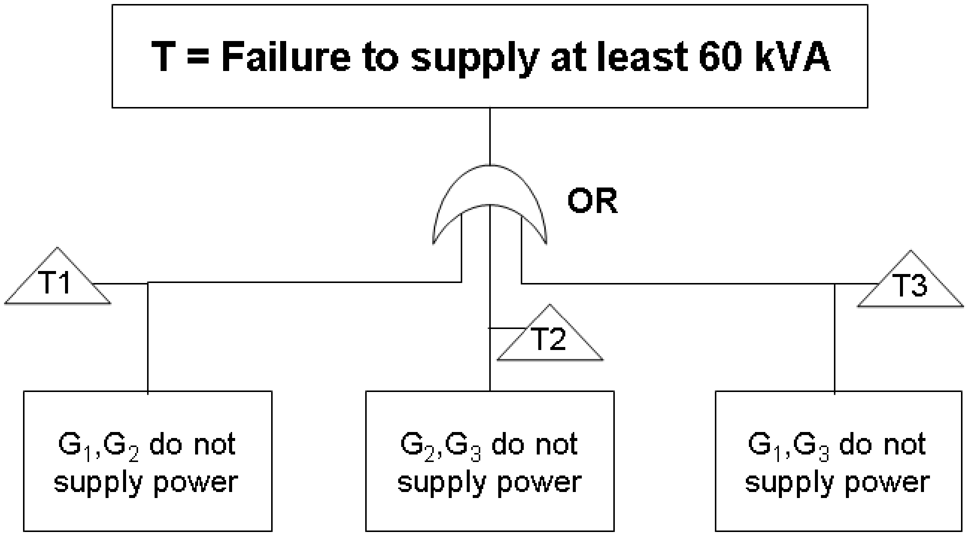
G1, G2, G3 = generators, each one is rated at 30 KVA

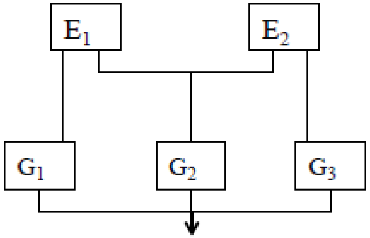
T = Failure to supply at least 60 kVA

FT construction: Procedure steps

1. Define top event (system failure)
2. **Decompose top event by identifying sub-events which can cause it.**

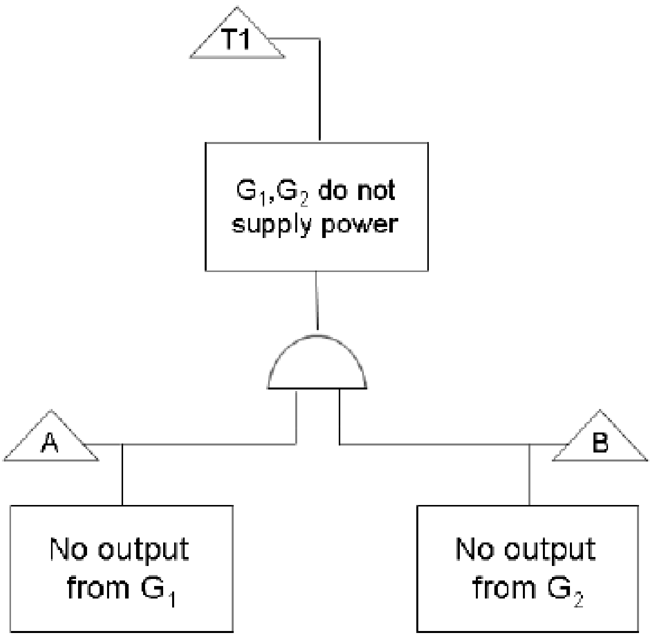
At least two out of the three generators do not work

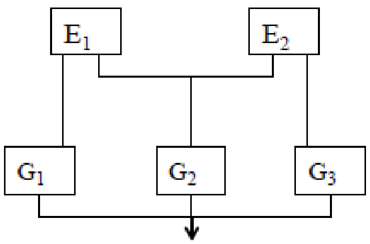




FT construction: Procedure steps

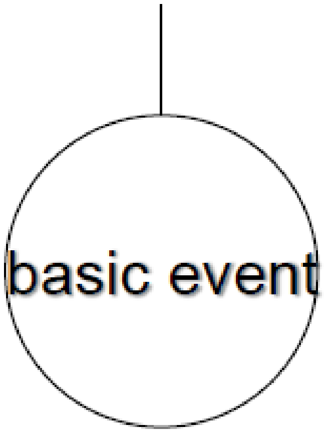
1. Define top event (system failure)
2. Decompose top event by identifying subevents which can cause it.
3. **Decompose each subevent in more elementary subevents which can cause it**





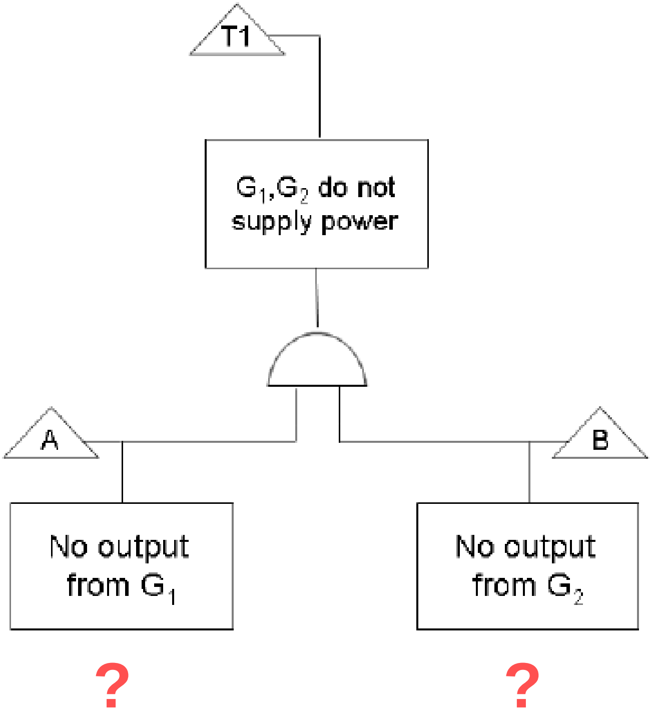
FT construction: Procedure steps

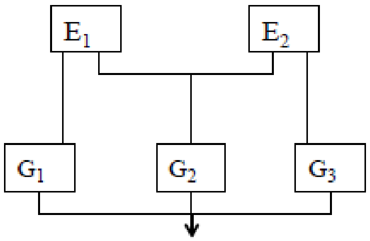
1. Define top event (system failure)
2. Decompose top event by identifying subevents which can cause it.
3. Decompose each subevent in more elementary subevents which can cause it
4. **Stop decomposition when subevent probability data are available (resolution limit): subevent = basic or primary event**



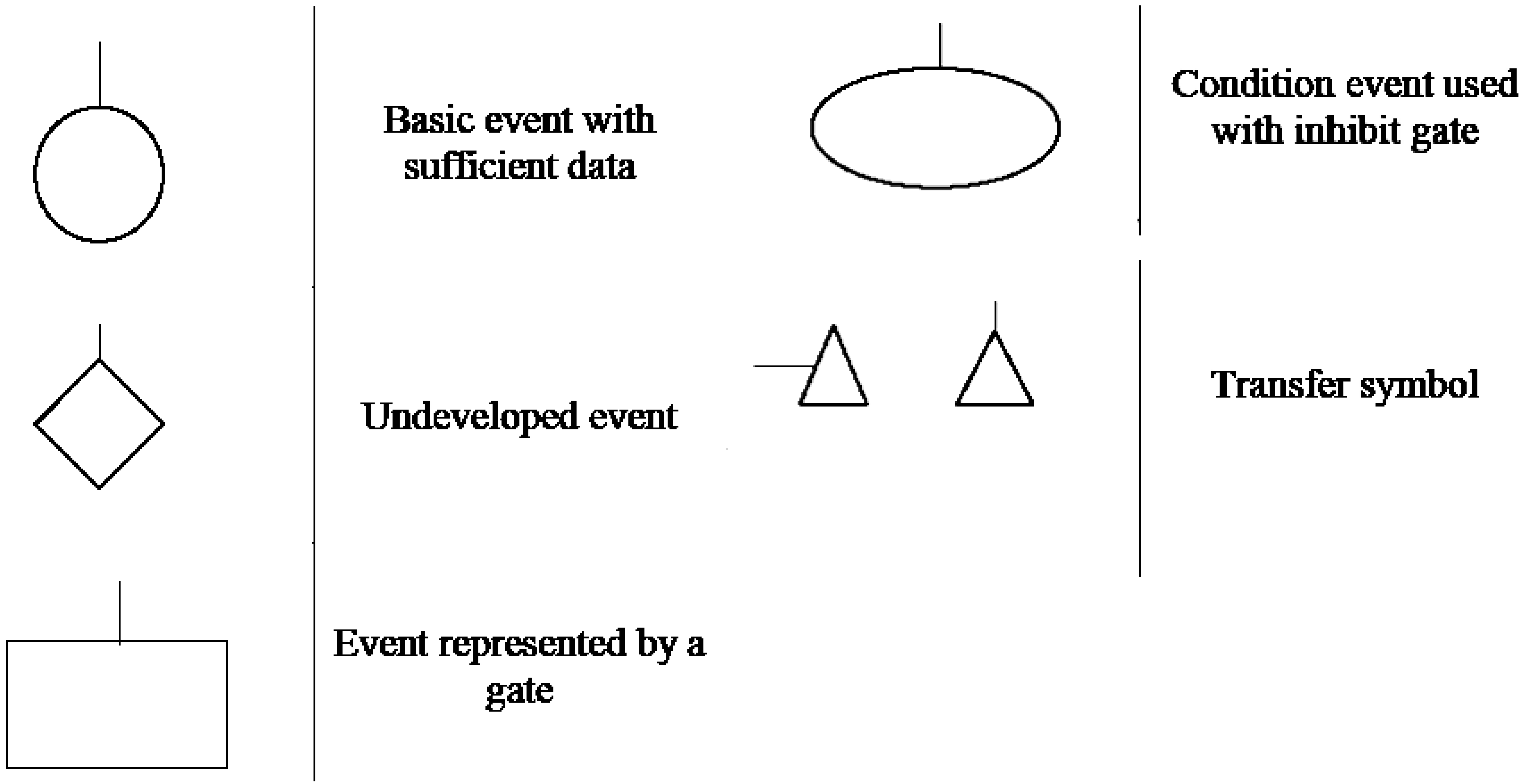
FT construction: Procedure steps

1. Define top event (system failure)
2. Decompose top event by identifying subevents which can cause it.
3. Decompose each subevent in more elementary subevents which can cause it
4. **Stop decomposition when subevent probability data are available (resolution limit): subevent = basic or primary event**

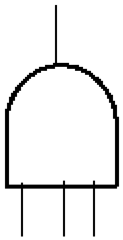
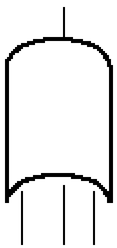
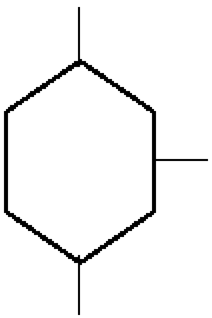




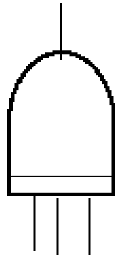
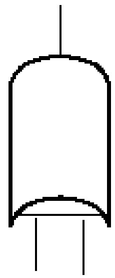
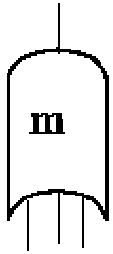
FT event symbols



FT gate symbols

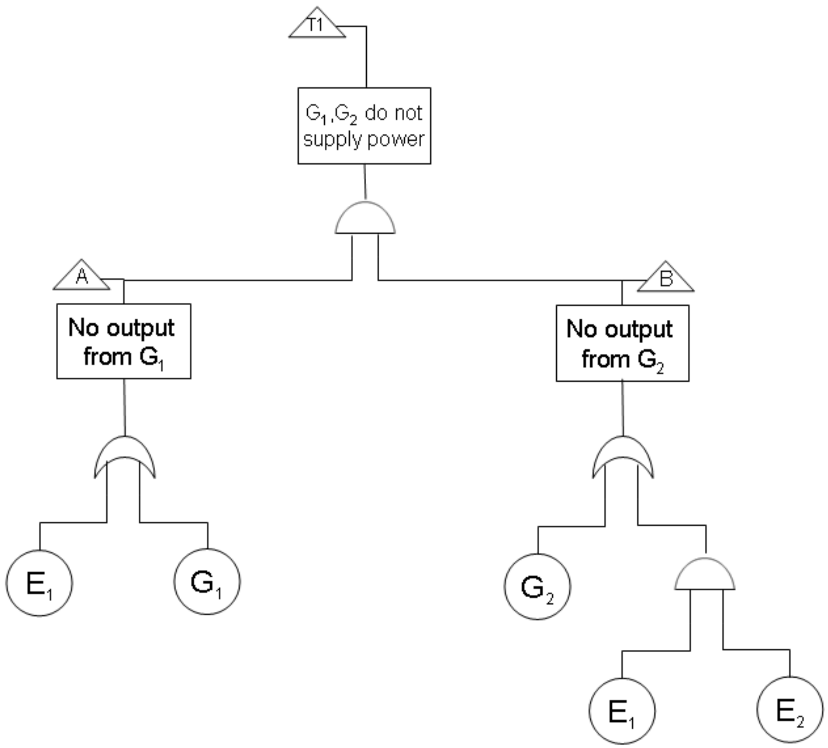
	AND gate	Output event occurs if all input events occur simultaneously.
	OR gate	Output event occurs if any one of the input events occurs.
	Inhibit gate	Input produces output when conditional event occurs.

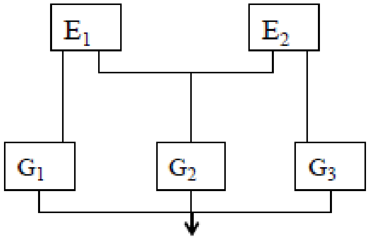
FT gate symbols

	Priority AND Gate	Output event occurs if all input events occur in the order from left to right
	Exclusive OR Gate	Output event occurs if one, but not both, of the input events occur.
 n input	m out of n gate (volume or sample gate)	Output event occurs if m out of n input events occur.

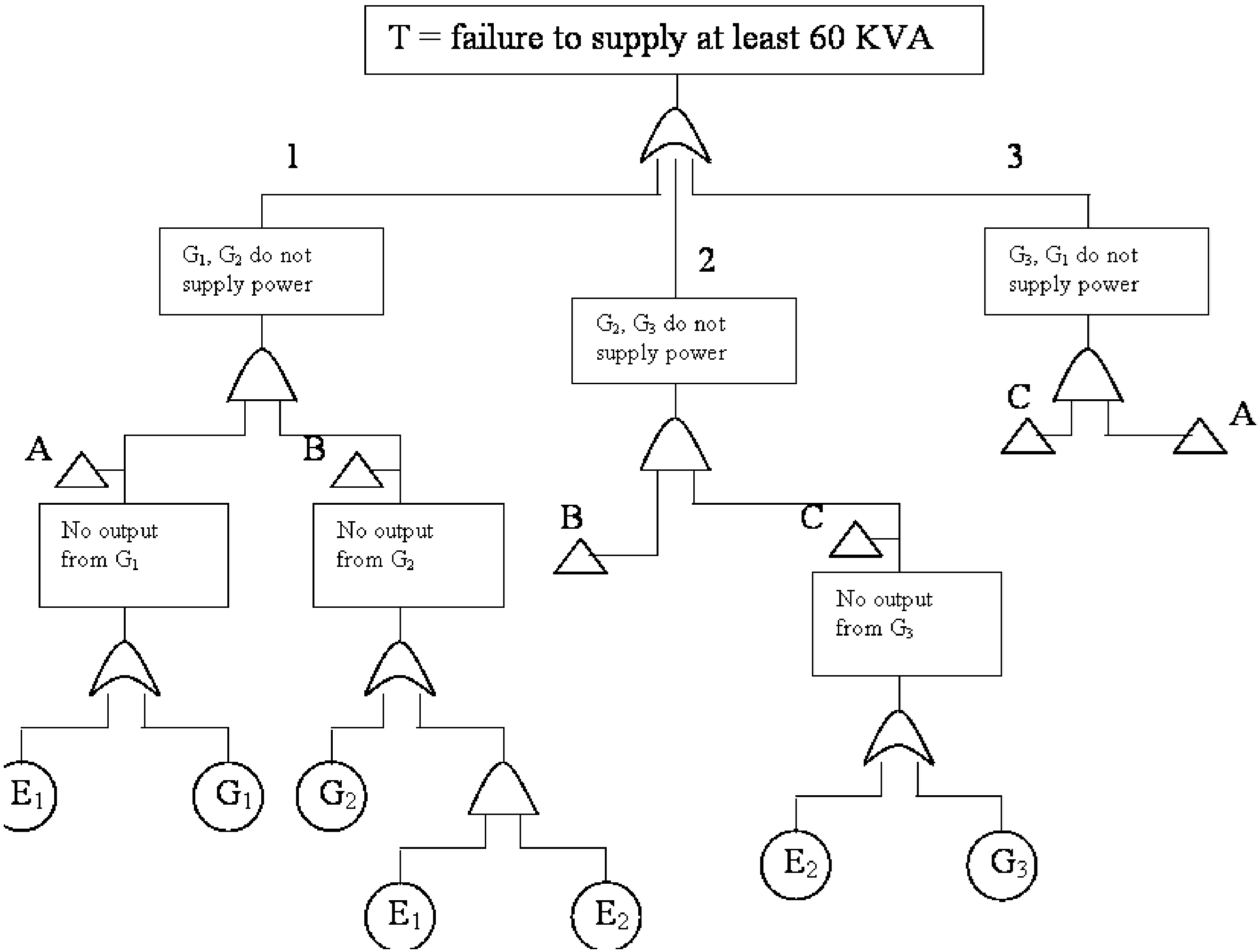
FT construction: Procedure steps

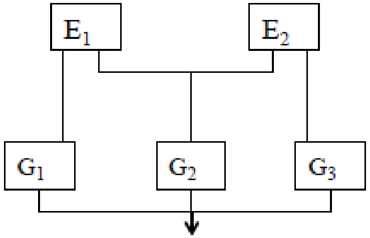
1. Define top event (system failure)
2. Decompose top event by identifying subevents which can cause it.
3. Decompose each subevent in more elementary subevents which can cause it
4. **Stop decomposition when subevent probability data are available (resolution limit): subevent = basic or primary event**



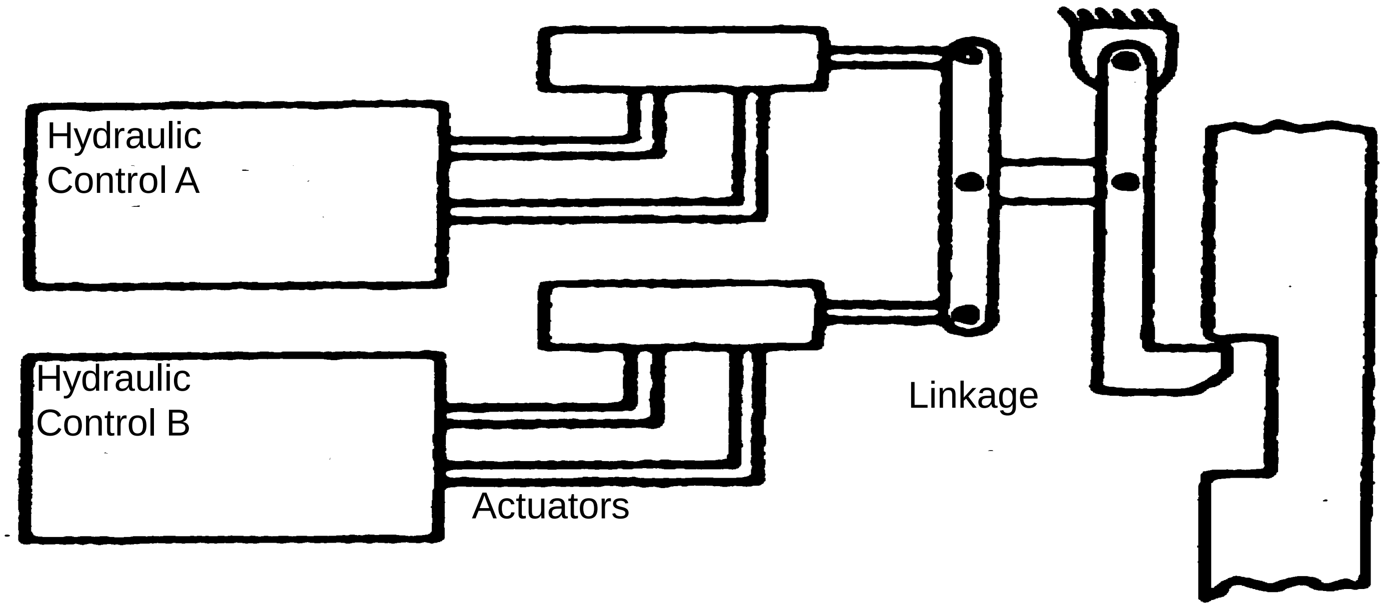


FT example 1

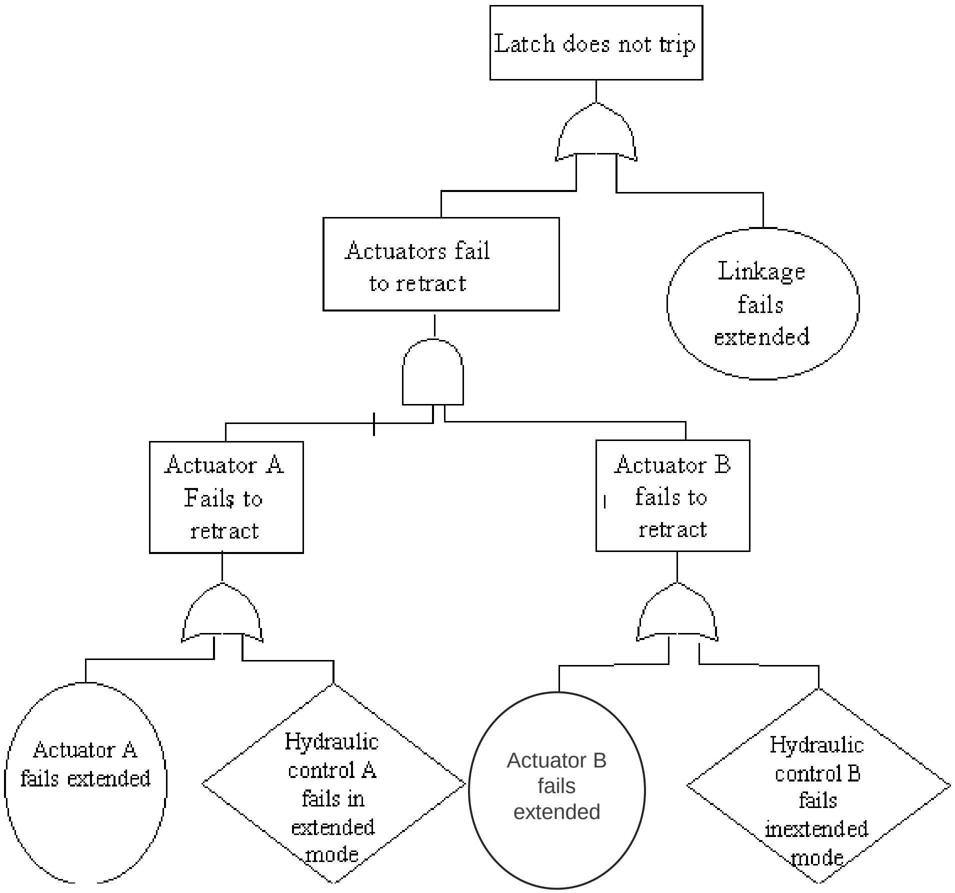

T = failure to supply at least 60 KVA
1
2
3
G1, G2 do not supply power
G2, G3 do not supply power
G3, G1 do not supply power
A
B
C
No output from G1
No output from G2
No output from G3
E1
G1
G2
E1
E2
E2
G3

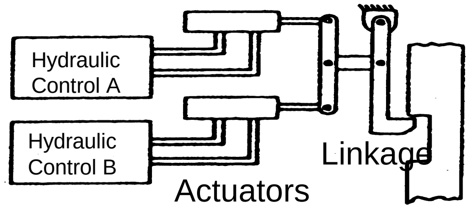

E1
E2
G1
G2
G3

FT Example 2: The System

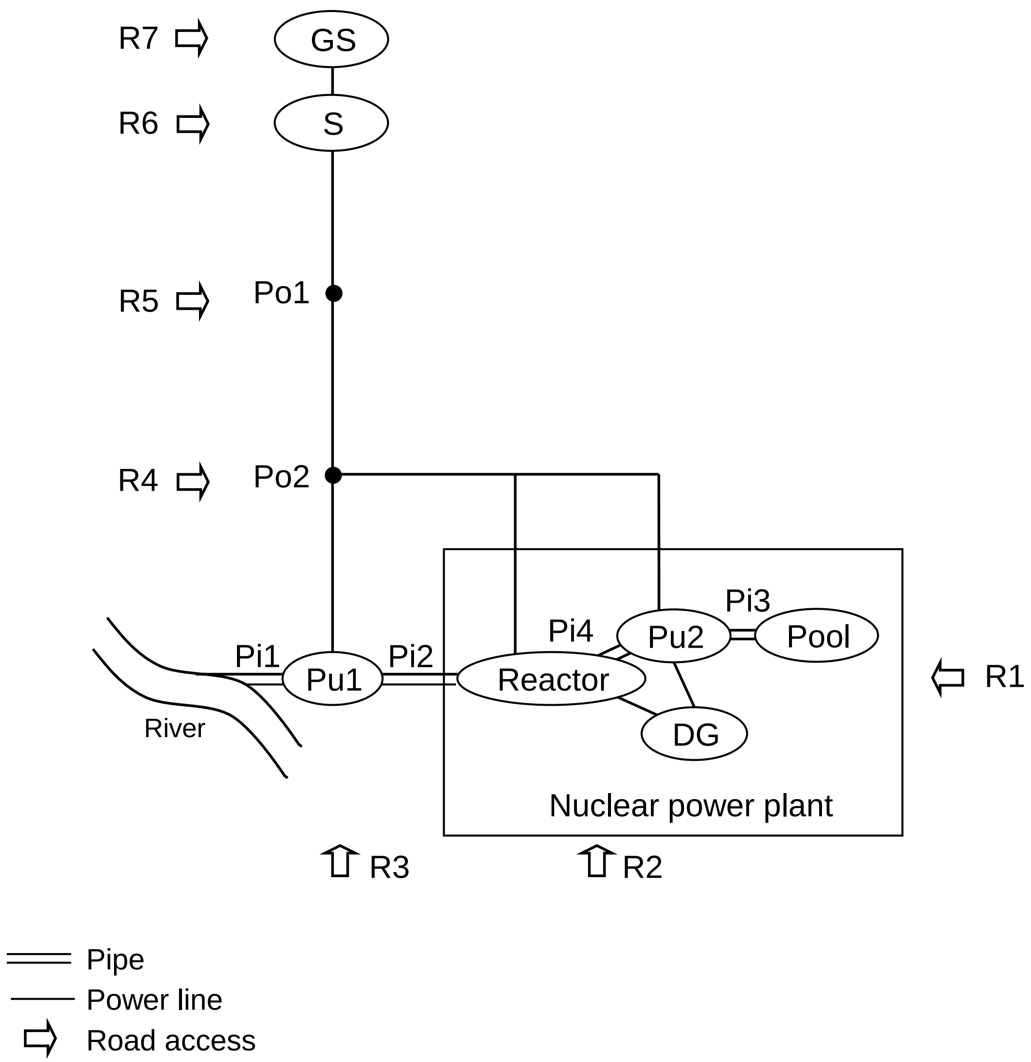


FT Example 2: Fault Tree





FT Example 3: The System of Systems



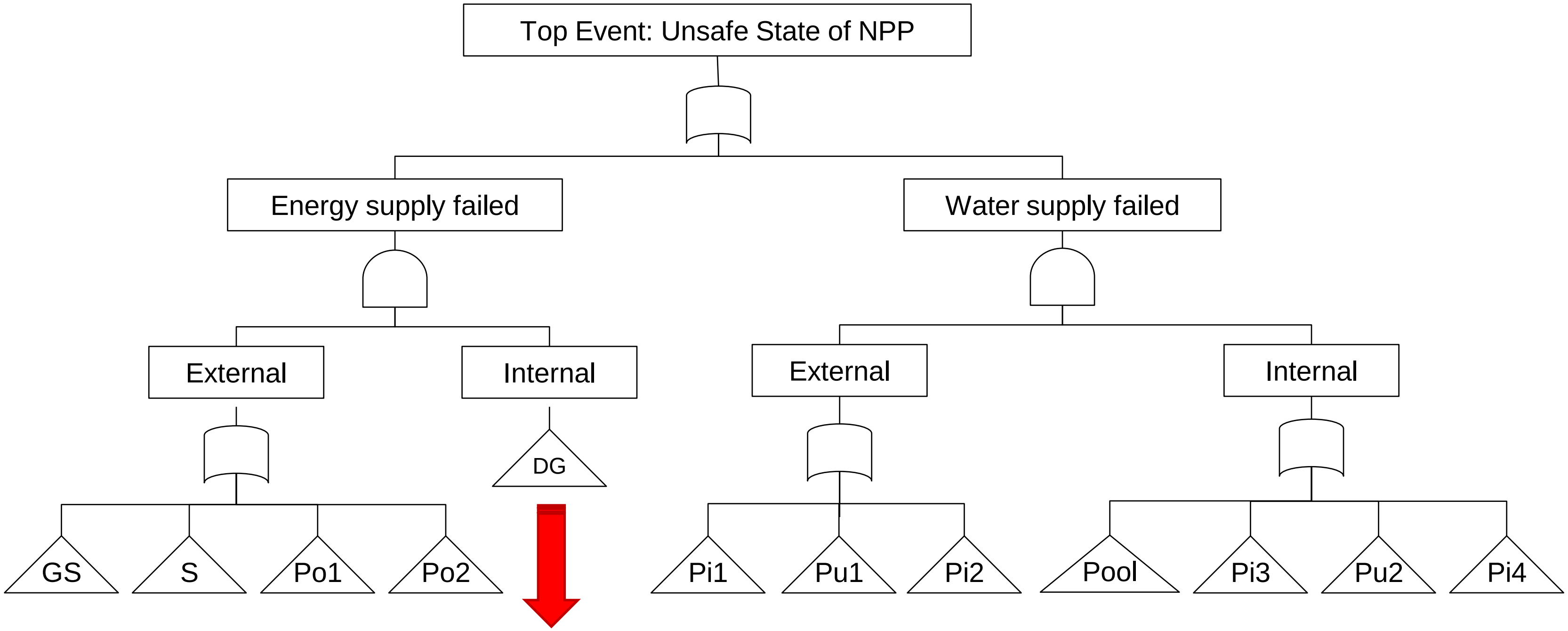
Internal emergency devices:

- Power system
  - Diesel Generator (DG)
- Water system
  - Pipe (Pi)
  - Pump (Pu)
  - Pool

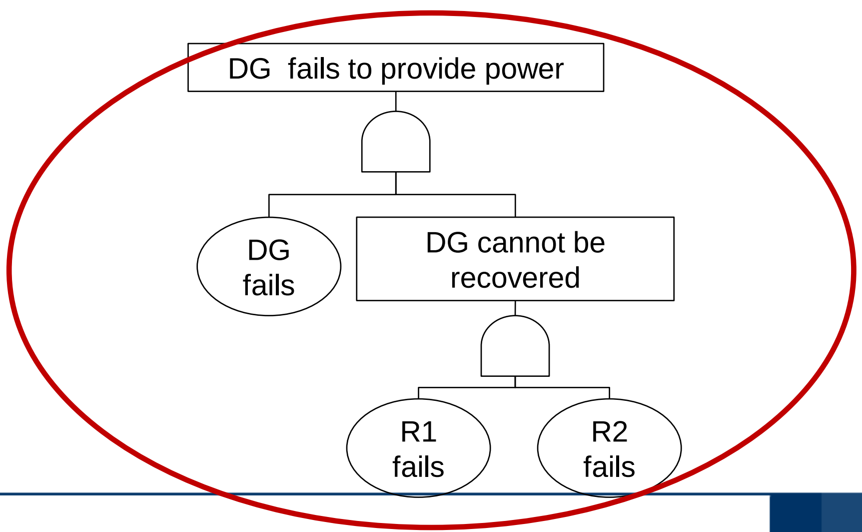
Interdependent CIs:

- Power system
  - Generation Station (GS)
  - Substation (S)
  - Pole (Po)
- Water system
  - Pipe (Pi)
  - Pump (Pu)
  - River
- Road transportation system
  - Road access (R)

FT Example 3: Fault Tree



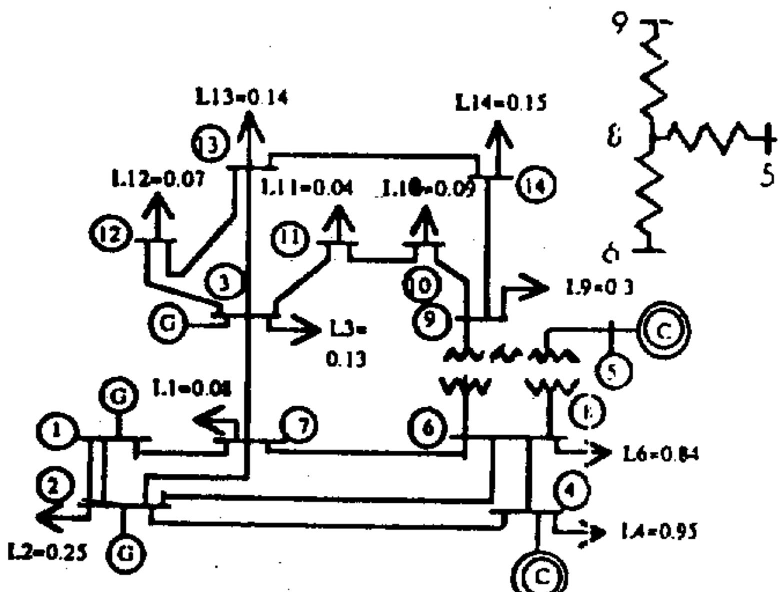
Example:



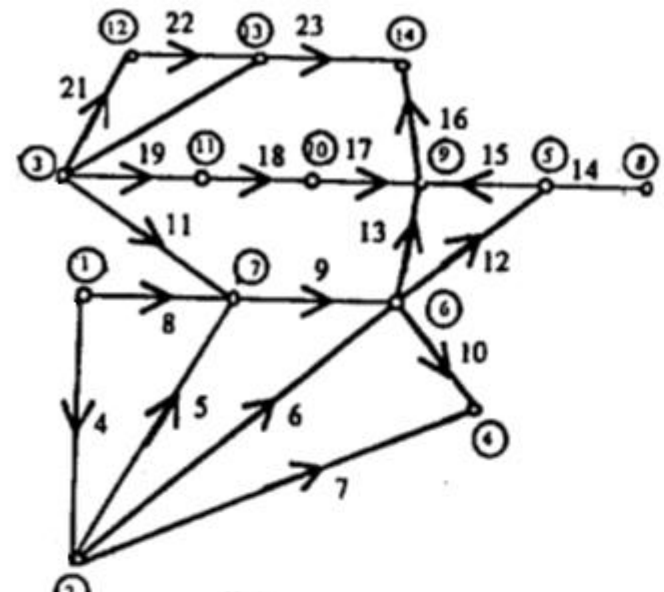
Elements that fail can be immediately repaired/replaced if the access through the road system does not fail → roads considered as “reserve components”.

FT Example 4: IEEE14 Bus Power Distribution System

Generators (G1, G2 , G3)
Loads (2, 3, 4, 6, 7, 9, 10, 11, 12, 13, 14)
Power delivery paths: lines (L) and buses (B).



(a)

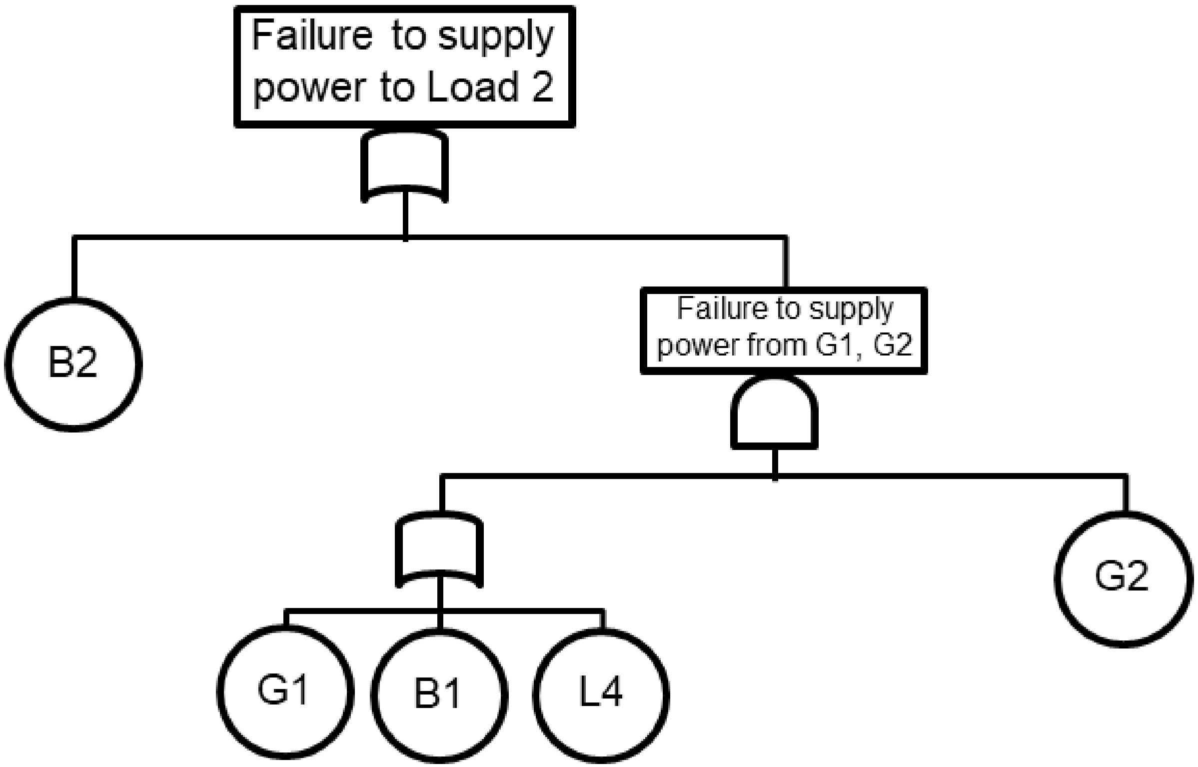

(b)

FT Example 4: IEEE14 Bus Power Distribution System

Draw a Fault Tree (FT) for the top event “failure to supply power Load2”

FT Example 4: IEEE14 Bus Power Distribution System

Draw a Fault Tree (FT) for the top event “failure to supply power to Load 2”



FT qualitative analysis

FT qualitative analysis

- Introducing:
- X_i : binomial indicator variable of i-th component state (basic event)

$$X_i = \begin{cases} 1 \text{ failure event } \underline{\text{true}} \\ 0 \text{ failure event } \underline{\text{false}} \end{cases}$$

- **FT = set of Boolean algebraic equations (one for each gate) => structure (switching) function *Φ:***

$$X_T = \Phi\,(X_1\,,\,X_2\,,\,\ldots,\,X_n)$$

Boolean Logic laws

1) Commutative Law:
   (a) $XY = YX$
   (b) $X + Y = Y + X$

2) Associative Law
   (a) $X(YZ) = (XY)Z$
   (b) $X + (Y + Z) = (X + Y) + Z$

3) Idempotent Law
   (a) $XX = X$
   (b) $X + X = X$

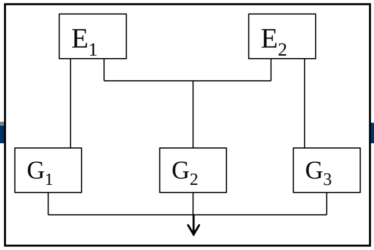
4) Absorption Law
   (a) $X(X + Y) = X$
   (b) $X + XY = X$

5) Distributive Law
   (a) $X(Y + Z) = XY + XZ$
   (b) $(X + Y)(X + Z) = X + YZ$

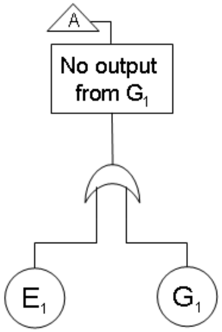
6) Complementation*
   (a) $X\overline{X} = \varnothing$
   (b) $X + \overline{X} = \Omega$
   (c) $\overline{\overline{X}} = X$

7) Unnamed relationships but frequently useful
   (a) $X + \overline{X}Y = X + Y$
   (b) $\overline{X}(X + Y) = \overline{X}\overline{Y}$

Structure function: Example 1

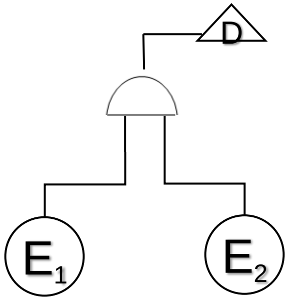


OR gate

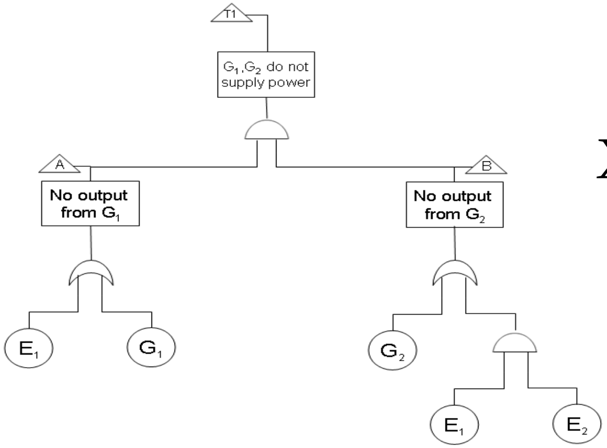


$$\mathbf{X_A} = \mathbf{X_{E_1}} + \mathbf{X_{G_1}} - \mathbf{X_{E_1}}\mathbf{X_{G_1}} = $$
$$= 1 - (1 - \mathbf{X_{E_1}})(1 - \mathbf{X_{G_1}})$$

AND gate



$$\mathbf{X_D} = \mathbf{X_{E_1}}\mathbf{X_{E_2}}$$



$$X_{T_1} = \Phi(X_{E_1}, X_{E_2}, X_{G_1}, X_{G2})$$

FT qualitative analysis

Structure functions can be expressed in reduced expressions in terms of minimal path or cut sets.

A path set is a set $\underline{X}$ such that $\Phi(\underline{X}) = 0$;

a cut set is a set X such that $\Phi(X) = 1$.

Physically, a path (cut) set is a set of components whose functioning (failure) ensures the functioning (failure) of the system.

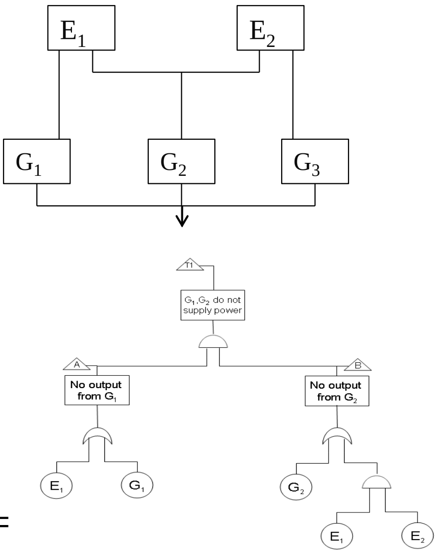
- **Reduce $\boldsymbol{\Phi}$ in terms of minimal cut sets (mcs)**
- **cut sets =** logic combinations of primary events which render true the top event
- **minimal cut sets =** cut sets such that if one of the events is not verified, the top event is not verified

FT qualitative analysis

- **FT = set of boolean algebraic equations (one for each gate) => structure (switching) function *Φ*:**

$$X_T = \Phi(X_1, X_2, \ldots, X_n)$$

- **Boolean algebra to solve FT equations**



$$X_{T_1} = X_A X_B =$$

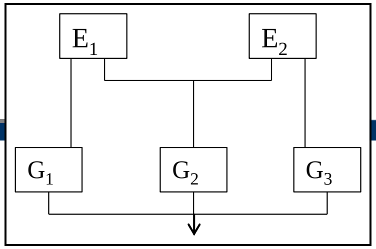
$$= (X_{E_1} + X_{G_1} - X_{E_1} X_{G_1})(X_{G_2} + X_{E_1} X_{E_2} - X_{E_1} X_{E_2} X_{G_2}) =$$

$$= X_{E_1} X_{G_2} + X_{E_1} X_{E_2} - X_{E_1} X_{E_2} X_{G_2} + X_{G_1} X_{G_2} + X_{E_1} X_{E_2} X_{G_1} +$$

$$- X_{E_1} X_{E_2} X_{G_1} X_{G_2} - X_{E_1} X_{G_1} X_{G_2} - X_{E_1} X_{E_2} X_{G_1} + X_{E_1} X_{E_2} X_{G_1} X_{G_2} =$$

$$= X_{E_1} X_{G_2} + X_{E_1} X_{E_2} + X_{G_1} X_{G_2} - X_{E_1} X_{E_2} X_{G_2} - X_{E_1} X_{G_1} X_{G_2}$$

mcs: Example 1



$$X_{T_1} = X_{E_1}X_{G_2} + X_{E_1}X_{E_2} + X_{G_1}X_{G_2} - X_{E_1}X_{E_2}X_{G_2} - X_{E_1}X_{G_1}X_{G_2}$$

$$= 1 - [1 - X_{E_1}X_{G_2} - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_2} + X_{E_1}X_{G_1}X_{G_2}] =$$

$$= 1 - [1 - X_{E_1}X_{G_2} - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_2} + X_{E_1}X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2} - X_{E_1}X_{E_2}X_{G_1}X_{G_2}] =$$

$$= 1 - [1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2} - X_{E_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_2} + X_{E_1}X_{G_1}X_{G_2} - X_{E_1}X_{E_2}X_{G_1}X_{G_2}] =$$

$$= 1 - [1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2} - X_{E_1}X_{G_2}(1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2})] =$$

$$= 1 - [(1 - X_{E_1}X_{G_2})(1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2})] =$$

$$= 1 - [(1 - X_{E_1}X_{G_2})(1 - X_{E_1}X_{E_2})(1 - X_{G_1}X_{G_2})]$$

3 minimal cut sets:

$$\begin{cases} M_1 = \{E_1 G_2\} \\ M_2 = \{E_1 E_2\} \\ M_3 = \{G_1 G_2\} \end{cases}$$

Alternative way of obtaining minimal cut sets

1. Label the primary events.

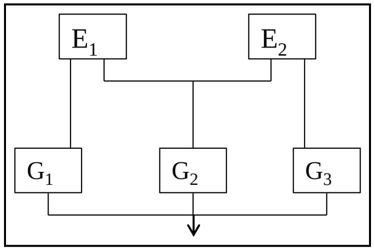
2. Label the gates and list the gates type and inputs.

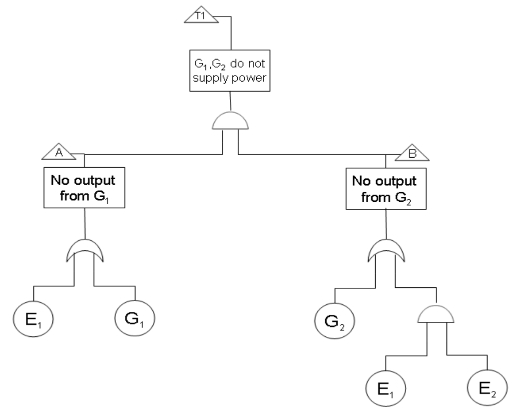
3. Write a Boolean equation for each gate.

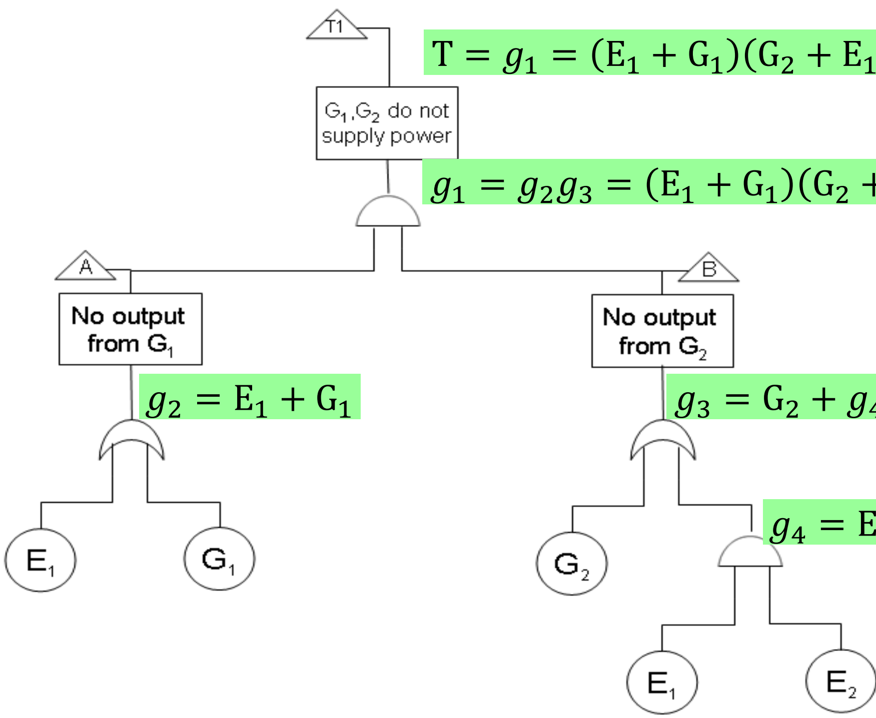
4. Use Boolean algebra to solve for the top event in terms of the cut sets.

5. Use Boolean algebra to eliminate the cut set redundancies to obtain the minimal cut sets.

mcs: Example 1







$$T = g_1 = (E_1 + G_1)(G_2 + E_1E_2)$$

$$g_1 = g_2 g_3 = (E_1 + G_1)(G_2 + E_1E_2)$$

$$g_2 = E_1 + G_1$$

$$g_3 = G_2 + g_4 = G_2 + E_1E_2$$

$$g_4 = E_1E_2$$

$$T = (E_1 + G_1)(G_2 + E_1E_2)$$

$$T = E_1G_2 + E_1E_1E_2 + G_1G_2 + E_1E_2G_1$$

$$T = E_1G_2 + E_1E_2 + E_1E_2G_1 + G_1G_2$$

$$T = E_1G_2 + E_1E_2(1 + G_1) + G_1G_2$$

$$T = E_1G_2 + E_1E_2 + G_1G_2$$

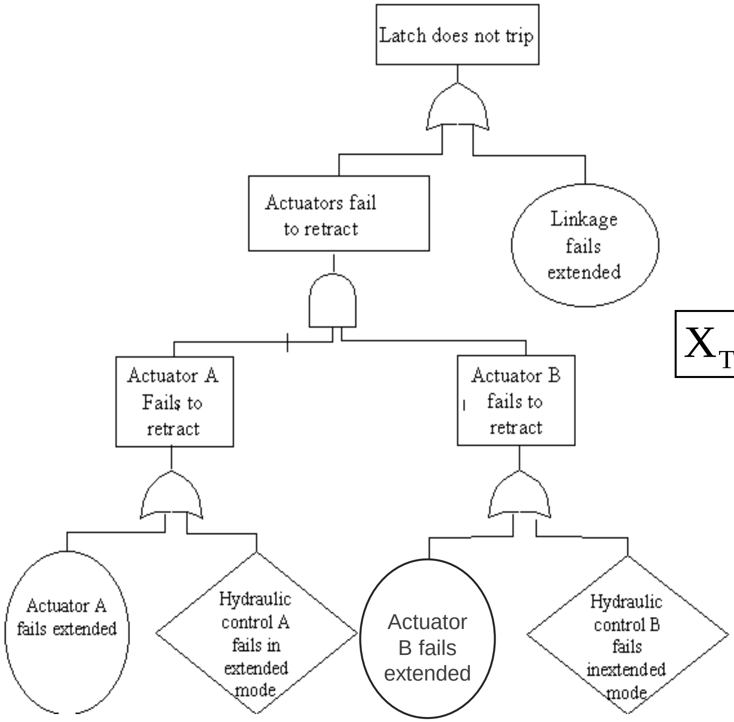
3 minimal cut sets:

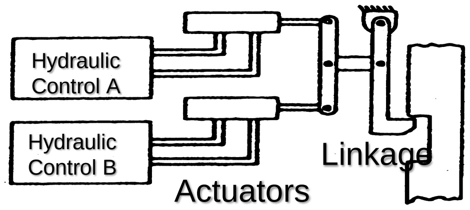
$$M_1 = \{E_1G_2\}$$

$$M_2 = \{E_1E_2\}$$

$$M_3 = \{G_1G_2\}$$

mcs: Example 2





$$X_T = 1-(1-X_L)(1-(X_A + X_{HA} - X_A X_{HA})(X_B + X_{HB} - X_B X_{HB}))$$

5 minimal cut sets:

$M_1 = X_L$

$M_2 = X_A X_B$

$M_3 = X_A X_{HB}$

$M_4 = X_{HA} X_B$

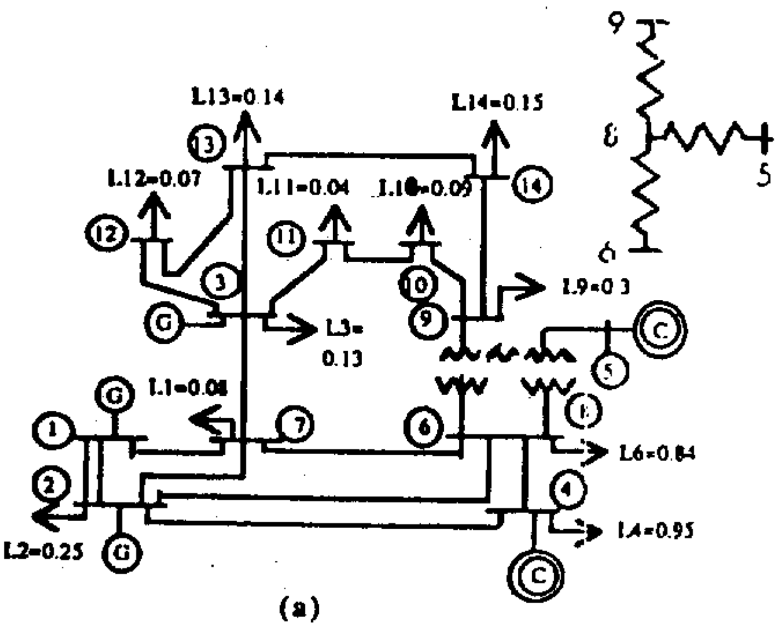
$M_5 = X_{HA} X_{HB}$

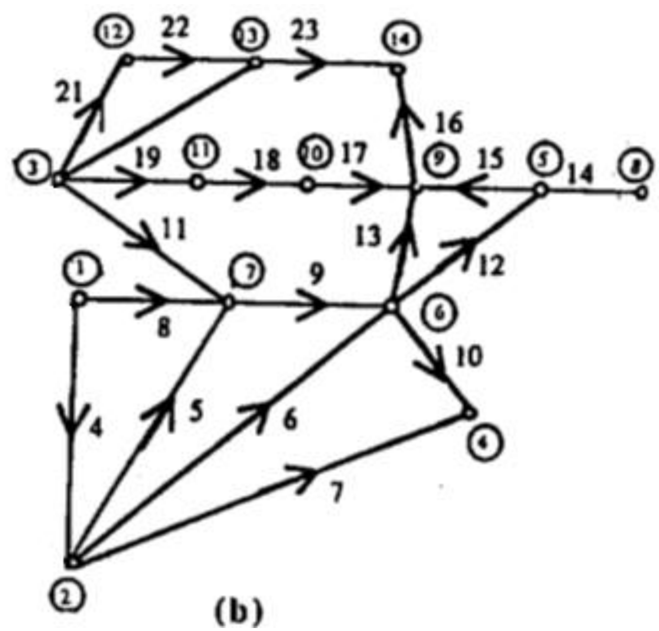
FT qualitative analysis: results

1. **mcs identify the component basic failure events which contribute to system failure**
2. **qualitative component criticality: those components appearing in low order mcs or in many mcs are most critical**

FT Example 4: IEEE14 Bus Power Distribution System

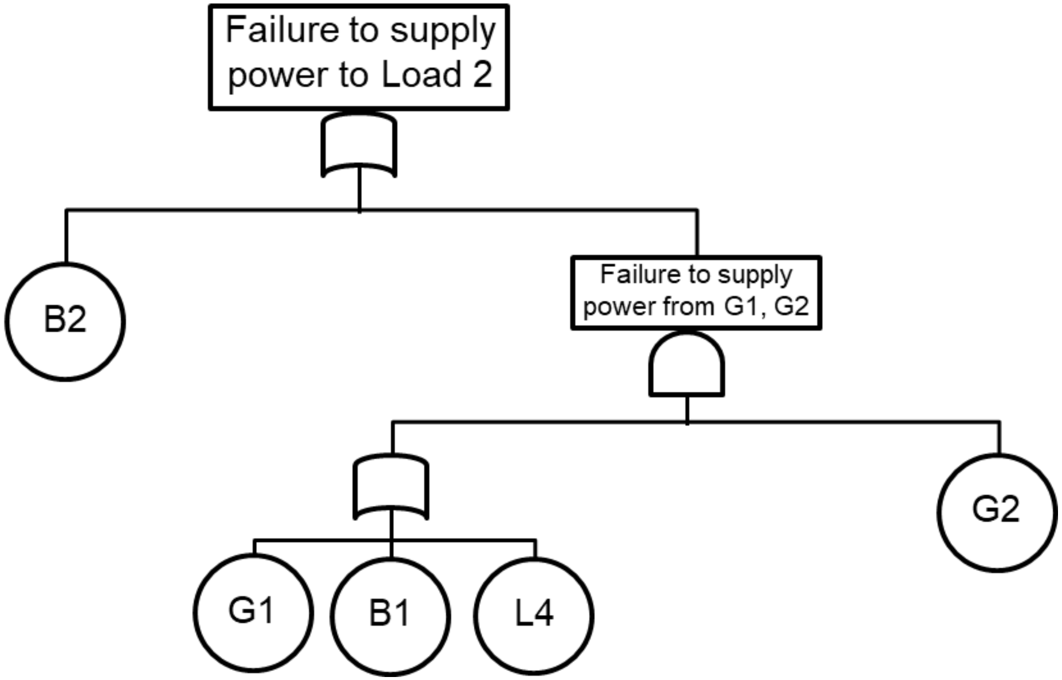
Generators (G1, G2 , G3)
Loads (2, 3, 4, 6, 7, 9, 10, 11, 12, 13, 14)
Power delivery paths: lines (L) and buses (B).





FT Example 4: IEEE14 Bus Power Distribution System

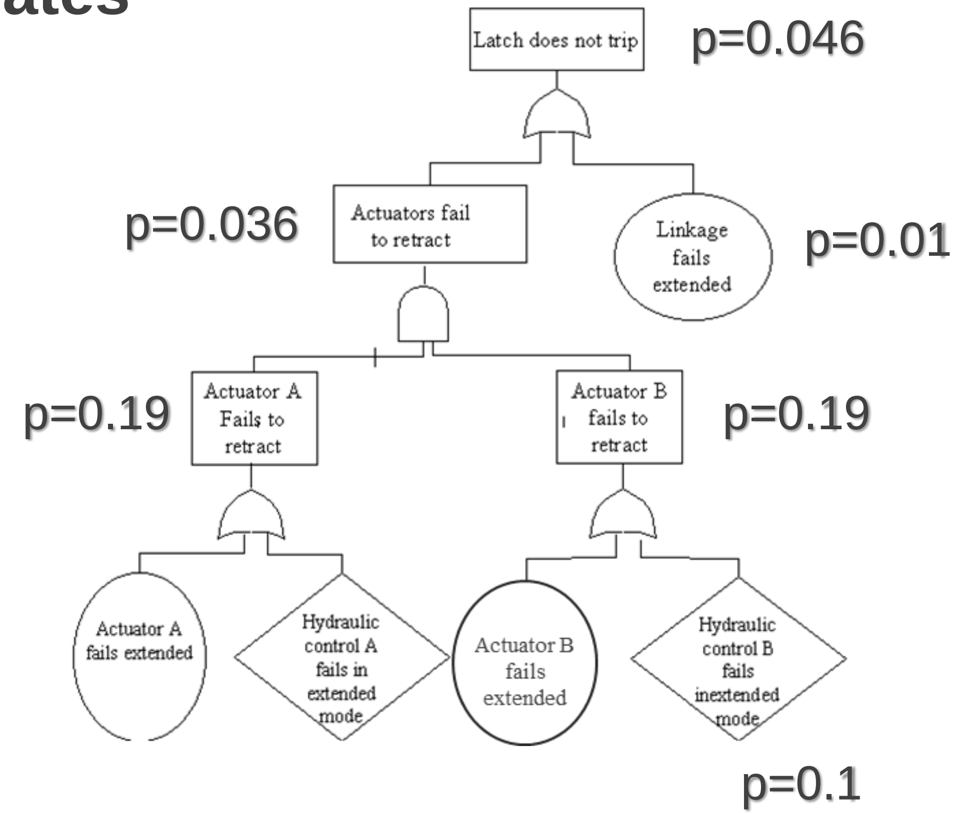
Find the Mcs for the top event “failure to supply power Load 2”

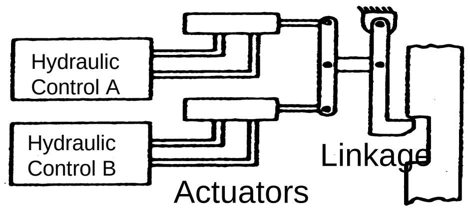


FT quantitative analysis

Compute system failure probability from primary events probabilities by:

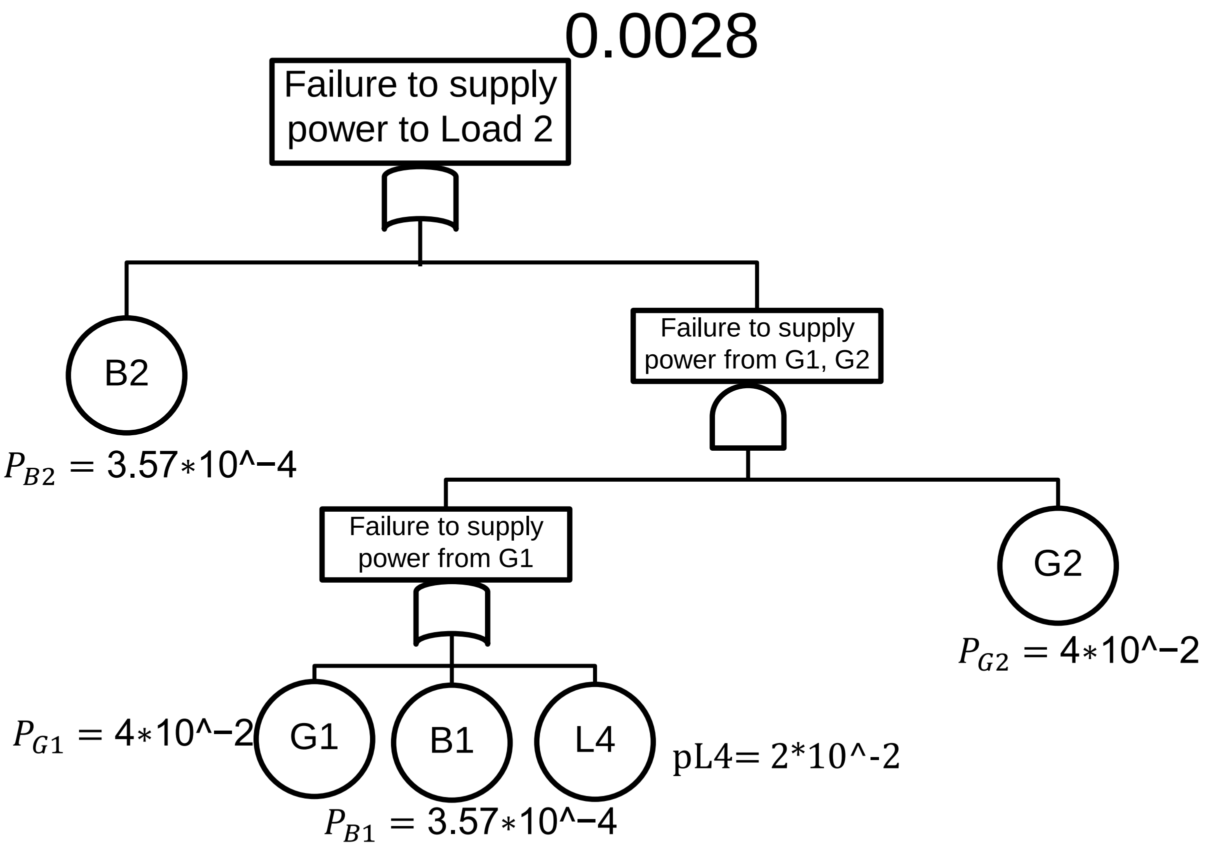
1. **using the laws of probability theory at the fault tree gates**





FT Example 4: IEEE14 Bus Power Distribution System

1. using the laws of probability theory at the fault tree gates



FT quantitative analysis

Compute system failure probability from primary events probabilities by:

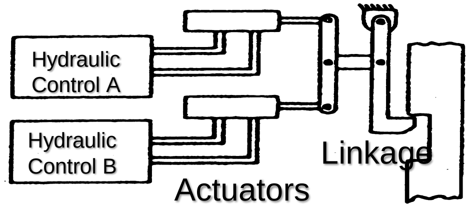
1. using the laws of probability theory at the fault tree gates
2. **using the mcs found from the qualitative analysis**

$$P[\Phi(\underline{X})=1]=\sum_{j=1}^{mcs}P[M_j]-\sum_{i=1}^{mcs-1}\sum_{j=i+1}^{mcs}P[M_iM_j]+\cdots+(-1)^{mcs+1}P[\prod_{j=1}^{mcs}M_j]$$

It can be shown that:

$$\sum_{j=1}^{mcs}P[M_j]-\sum_{i=1}^{mcs-1}\sum_{j=i+1}^{mcs}P[M_iM_j]\le P[\Phi(\underline{X})=1]\le\sum_{j=1}^{mcs}P[M_j]$$

FT quantitative analysis: Example 2



5 mcs:

$P(M_1) = P(X_L=1) = 0.01$

$P(M_2) = P(X_A X_B=1) = 0.1 \cdot 0.1 = 0.01$

$P(M_3) = P(X_A X_{HB}) = 0.1 \cdot 0.1 = 0.01$

$P(M_4) = P(X_{HA} X_B=1) = 0.1 \cdot 0.1 = 0.01$

$P(M_5) = P(X_{HA} X_{HB}) = 0.1 \cdot 0.1 = 0.01$

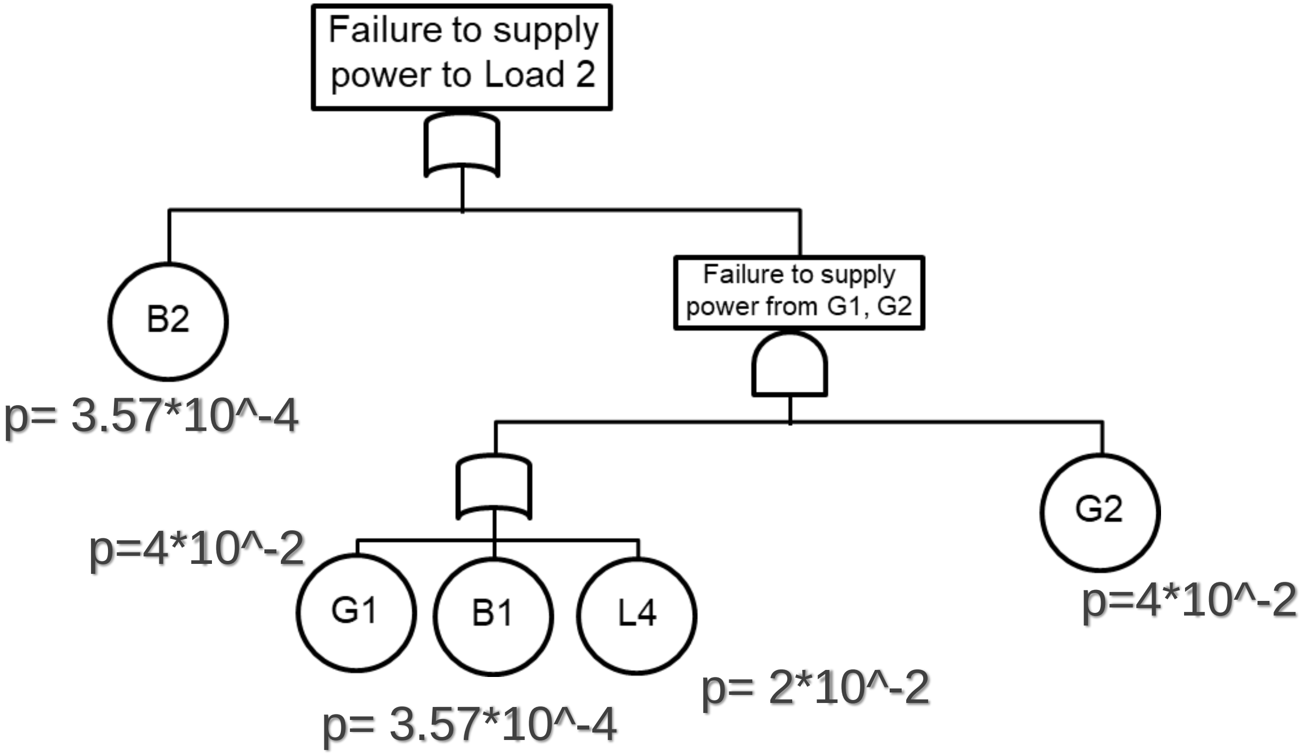
⇓

$$P[\Phi(\underline{X})=1] \leq \sum_{j=1}^{mcs} P[M_j] = 0.05$$

$$P[\Phi(\underline{X})=1] \geq \sum_{j=1}^{mcs} P[M_j] - \sum_{i=1}^{mcs-1} \sum_{j=i+1}^{mcs} P[M_i M_j] = 0.0464$$

FT Example 4: IEEE14 Bus Power Distribution System

Find the Mcs for the top event “failure to supply power to bus 2” (Load2)



```
%%%%%%% case 14bus %%%%%%%%
branch_R=[0.999 0.9971 0.9980 0.9800 0.9908 0.8651 0.8634 0.8492 0.8333 0.9636
0.8651 0.9998 0.9998 0.9998 1 1 0.8655 0.9536 0.9005 0.8974];
% Failure probability for power generation bus, load bus and transmission
% bus.
P_bus=3.57*10^-4;
L_bus=2.33*10^-5;
bus=3*10^-5;
% Generator failure probability
Gen=4*10^-2;
%%%%%%%%%%%%%%LOAD2
% Components identified in mcs for Load2
B2=P_bus;  G1=Gen;   G2=Gen;   B1=P_bus;   L4=1-branch_R(4);
% mcs
M_1=B2;
M_2=G1*G2;
M_3=B1*G2;
M_4=L4*G2;
 %Probability of failure of Load2
XT_Load2= 1-(1-M_1)*(1-M_2)*(1-M_3)*(1-M_4)=0.0028
```

FT: Advantages

1. Straightforward modelization via few, simple logic operators.
2. Physical elements represented in a well-defined structure, according to the logic of the system that leads to the identification of the minimal cut sets.
3. Minimal cut sets are a synthetic result which identifies the critical components.
4. Providing a graphical communication tool whose analysis is transparent.
5. Providing an insight into system behaviour.

FT: Limitations

1. Additional factors (operational, organizational, etc.) are not included. The exhaustive identification and manipulation of the minimal cut sets can be difficult for large systems.
2. Difficult to build the FT (in particular , in the case of large number of components and complicated logic dependencies).
3. No flexibility: the addition of a new component can change the entire structure of the FT.
4. No accounting for the strength of the relationships (Boolean-logic).

Logical Methods:
Event Tree

Objectives

1. Identification of possible scenarios (accident sequences), developing from a given accident initiator

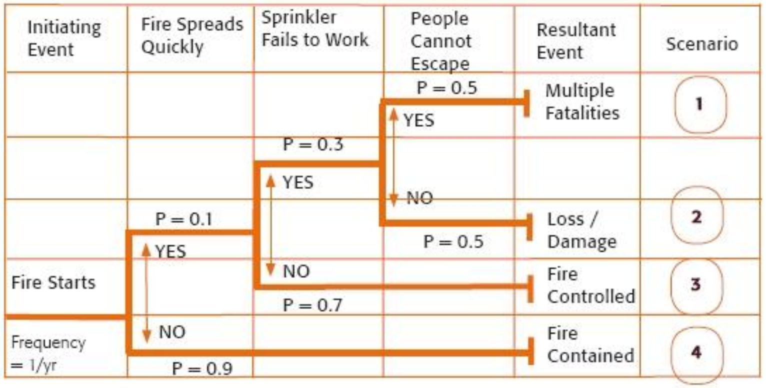
2. Computation of accident sequence probability

ETs typologies

- **System event tree**

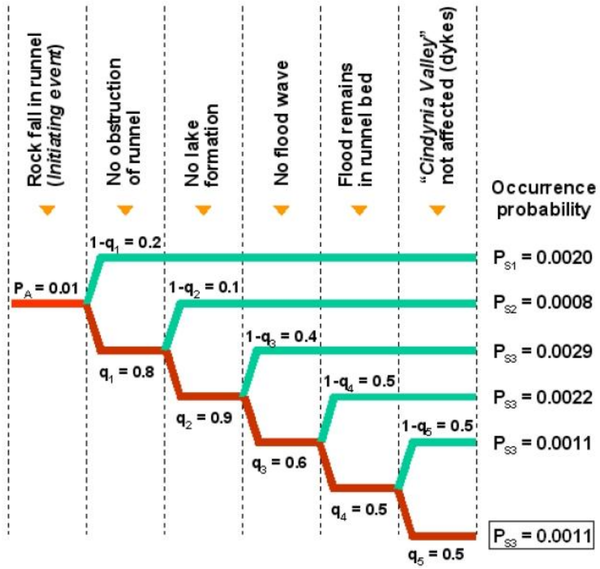
  The accident sequences **in the system/infrastructure** are identified with respect to the protection and safety systems/components involved (valves, pumps, pipes, tanks, etc.)

Quantification of Event Tree for Building Protected by Sprinkler System



- **Phenomenological event tree**

  Description of the accident phenomenological evolution **that affect the system/infrastructure** (winds, sea currents, animals/plants, etc.)



Event Tree Analysis (ETA)

- Systematic and quantitative
- Inductive (search for consequences)

ETA: Procedure steps

1. Define an accident **initiating** event **IE**
   - a system failure
   - an external, potentially disruptive event (e.g., an earthquake)

2. Identify "**headings**" $\boldsymbol{S_k}$:
   - **safety/protection functions**, **systems**, **procedures** demanded by IE
   - **phenomena** potentially influencing the development of an accident sequence

3. Specify **failure/success** states of S_k

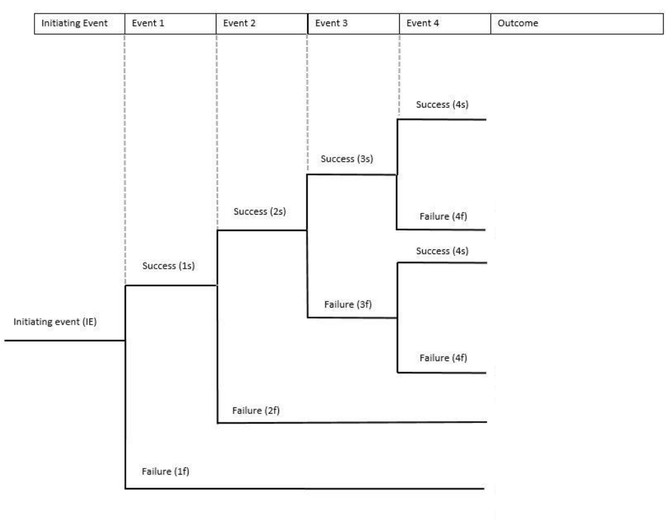
4. Combine the states of all S_k to generate accident sequences

ETA: some general comments (2)

Conditional probabilities are assigned to S_k states (upon previous identification, e.g. by **FTA**)

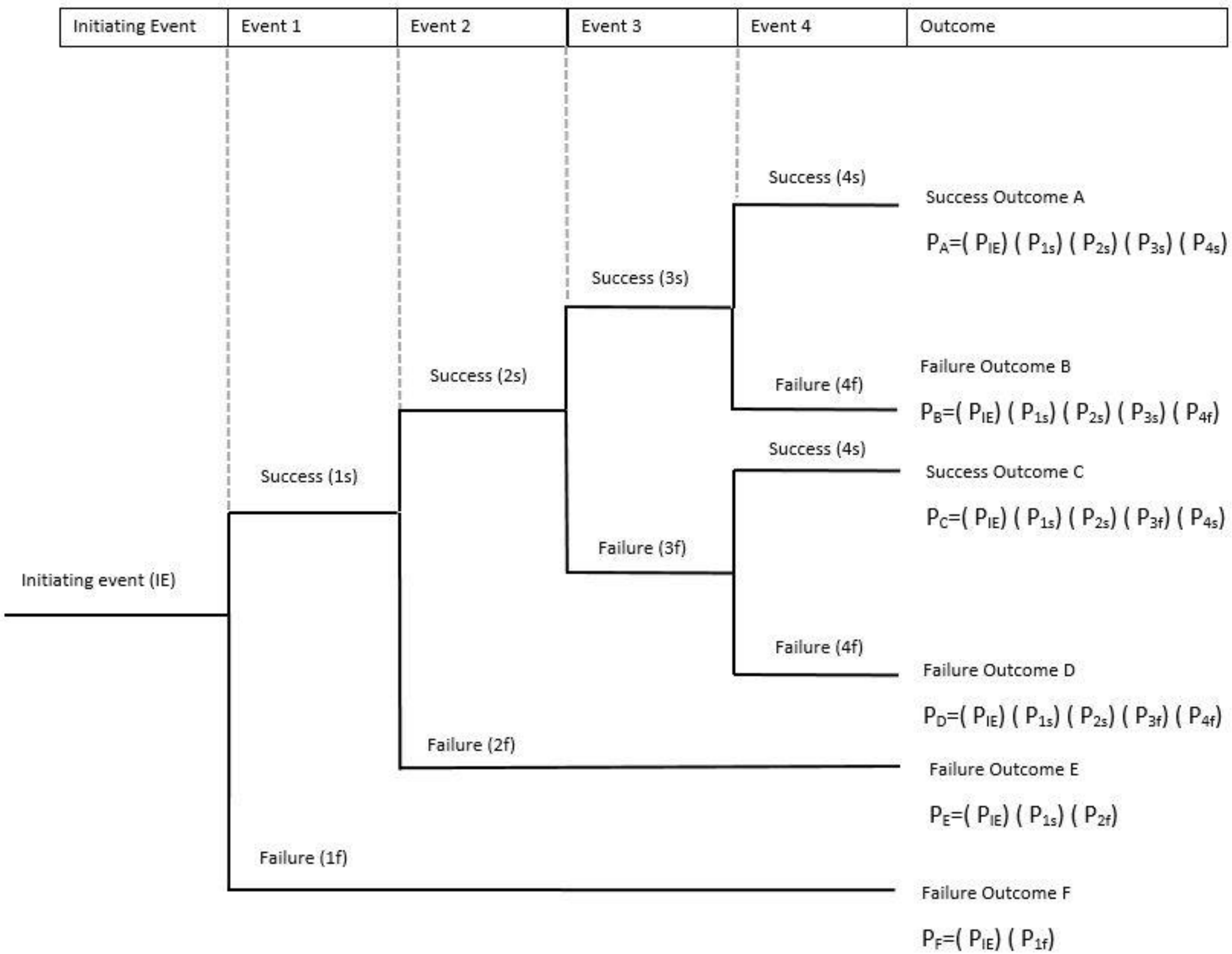
Sequence probability = **product** of the conditional probabilities of the events in a branch

"Failure" probability = sum of the probabilities of the sequences leading to failures

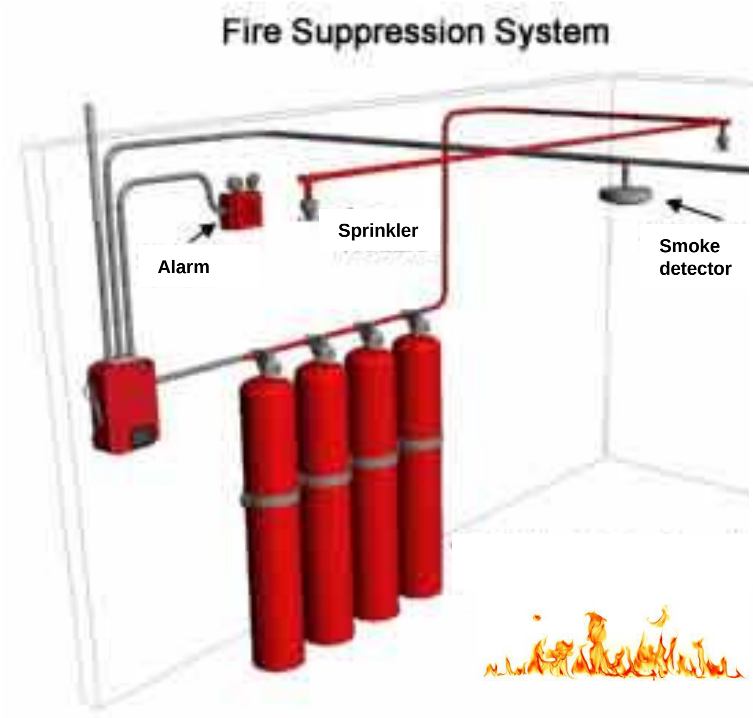


$$P(I 1_s 2_s \qquad) = P(4_s | 3_s \qquad I) \cdot P(\qquad\qquad)$$
$$= \qquad\qquad P(2_s | 1_s I) \cdot P(1_s | I) \cdot P(I)$$

Event Tree (independent events)



Event Tree Example 1: Fire protection system



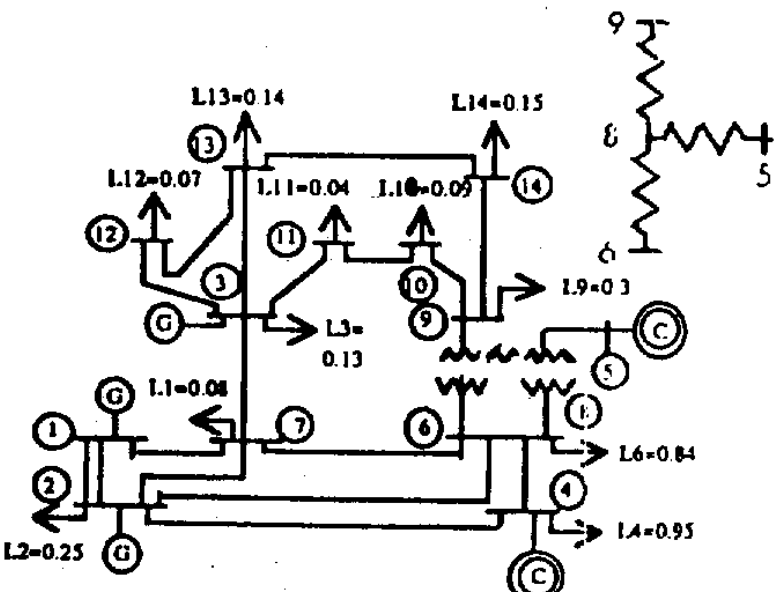
Event Tree Example 1: Fire protection system

INITIATING EVENT	FIRE SPREADS QUICKLY	SPRINKLER FAILS TO WORK	PEOPLE CANNOT ESCAPE	RESULTANT EVENT	SCENARIO

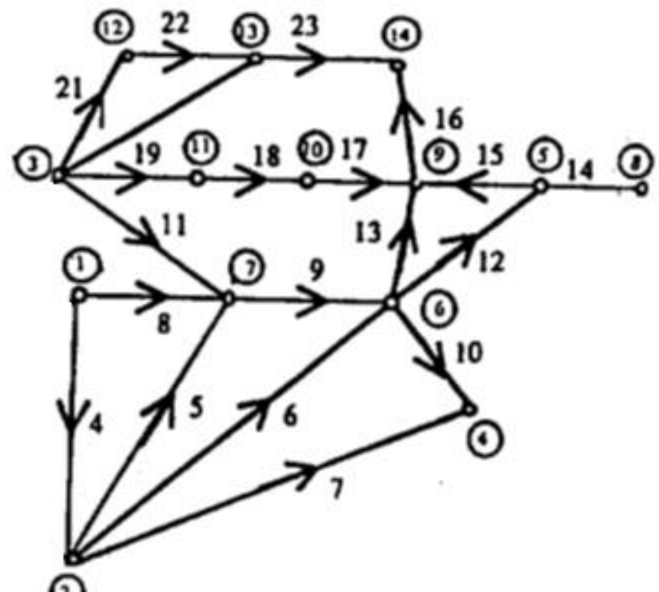
ETA: some general comments (1)

1. One event tree for each accident initiator
2. **Time** and **logic** of S_k interventions are important for the tree structure (**simplifications possible**)
3. S_k states are, in general, **conditional** on accident initiator and previous S_j's states

Generators (G1, G2 , G3)
Loads (2, 3, 4, 6, 7, 9, 10, 11, 12, 13, 14)
Power delivery paths: lines (L) and buses (B).



(a)

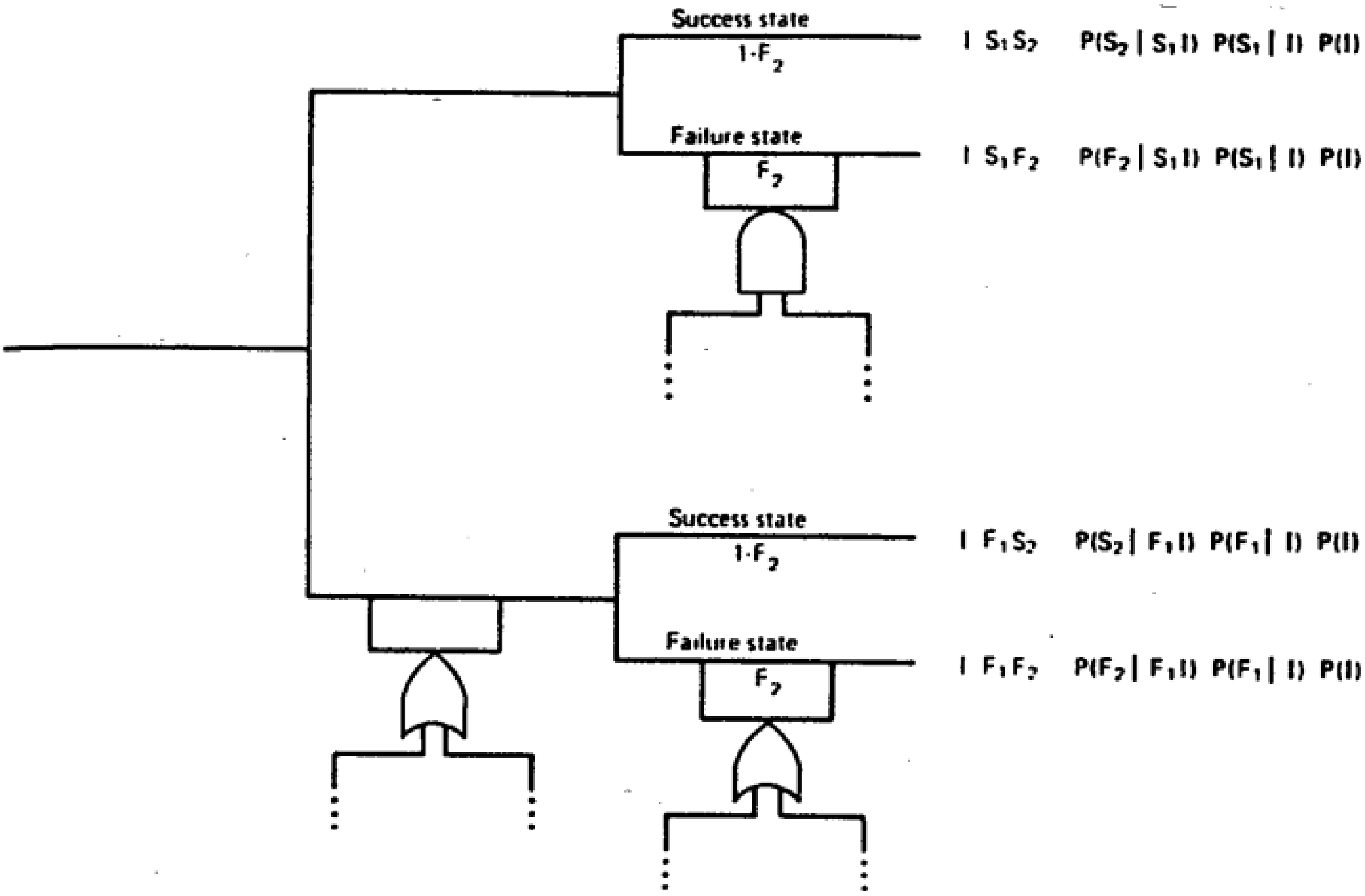


(b)

FT Example 4: IEEE14 Bus Power Distribution System

Draw the ET and calculate the probability of “failure to supply power to bus 2” (Load2)

ETA+FTA



Success state
1-F2
Failure state
F2
Success state
1-F2
Failure state
F2
I S1S2 P(S2 | S1 I) P(S1 | I) P(I)
I S1F2 P(F2 | S1 I) P(S1 | I) P(I)
I F1S2 P(S2 | F1 I) P(F1 | I) P(I)
I F1F2 P(F2 | F1 I) P(F1 | I) P(I)

1. One event tree for each accident initiator
2. **Time** and **logic** of S_k interventions are important for the tree structure (**simplifications possible**)
3. S_k states are, in general, **conditional** on accident initiator and previous S_j's states

References

[Curtois 1985] Courtois, P. J. (1985). "On Time and Space Decomposition of Complex Structures.“ Communications of the Acm, 28(6), 590-603.

[Hu and Modarres 1999] Hu Y.S., Modarres M. (1999) Evaluating system behavior through Dynamic Master Logic Diagram (DMLD) modeling. Reliability Engineering and System Safety 64; 241–269.

[Kim and Modarres 1987] Kim I.S., Modarres M. (1987) Application of Goal Tree Success Tree model as the knowledge-base of operator advisory systems. Nuclear Engineering and Design 104, 67-81.

[LaRocca et al. 2011] La Rocca, S., Guikema, S. D., Cole, J., and Sanderson, E. (2011). "Broadening the discourse on infrastructure interdependence by modeling the “Ecology” of infrastructure systems." Applications of Statistics and Probability in Civil Engineering, M. Faber, J. Köhler, and K. Nishijima, eds., London, 1905–1912.

[Modarres 1999] Modarres M. (1999) Functional modeling of complex systems with applications. IEEE Proceedings Annual Reliability and Maintenability Symposium.

[Modarres et al. 1999] Modarres, M., Kaminskiy, M., and Krivtsov, V. (1999). *Reliability engineering and risk analysis: a practical guide*, CRC press, New York.

[Nozick et al. 2005] Nozick, L. K., Turnquist, M. A., Jones, D. A., Davis, J. R., and Lawton, C. R. (2005). "Assessing the performance of interdependent infrastructures and optimising investments " International Journal of Critical Infrastructures, 1(2-3), 144-154.

[Sanderson 2009] Sanderson, E. (2009). *Mannahatta: a natural history of New York City*, Abrams, New York.

[Zio 2007] Zio, E. (2007). *An Introduction to the Basics of Reliability and Risk Analysis*, World Scientific Publishing Co. Pte. Ltd.