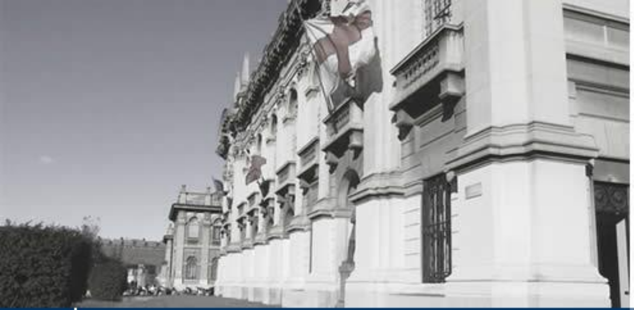


POLITECNICO DI MILANO

Logical Methods:
Fault Tree

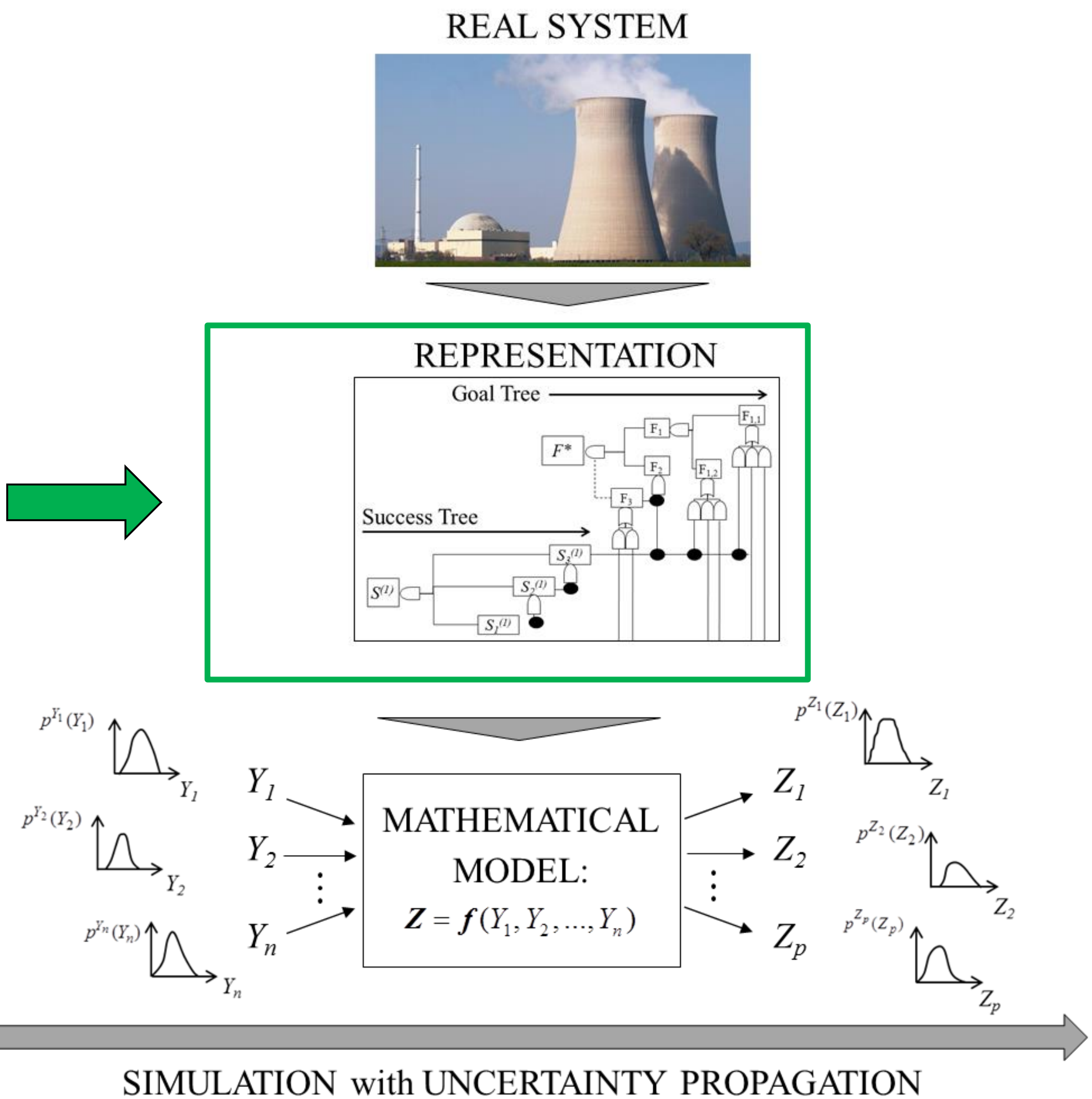
Prof. Francesco Di Maio
Dipartimento di Energia
Via La Masa 34, B12

francesco.dimaio@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

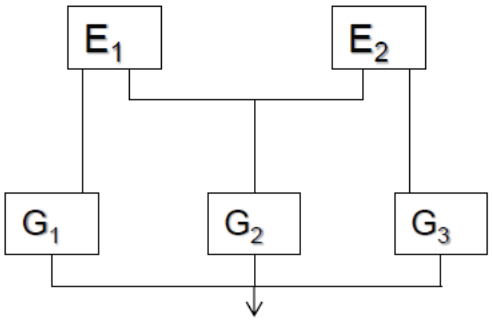
Fault Tree (FT)

- Systematic and quantitative
- Deductive (search for causes)

FT construction: Procedure steps

1. Define top event (system failure)

Electrical generating system



E1, E2 = engines

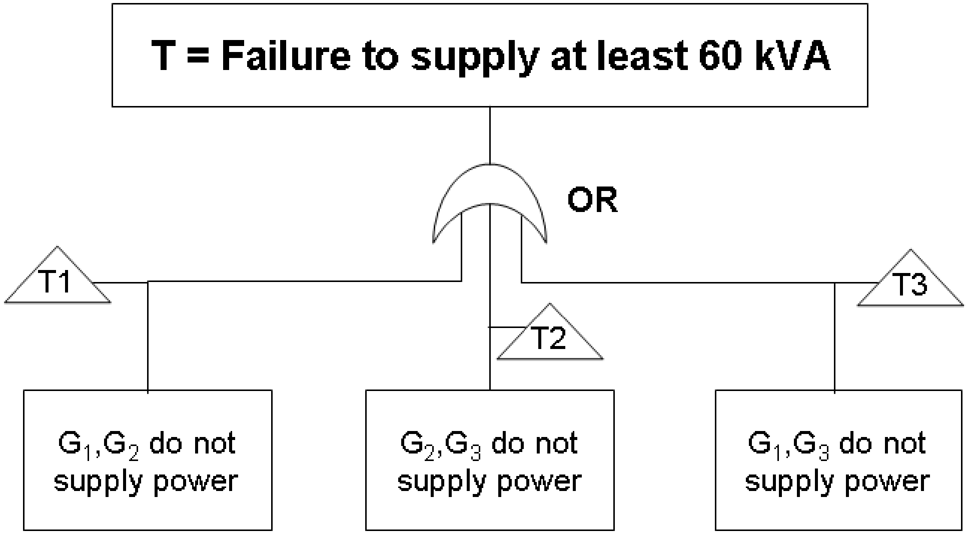
G1, G2, G3 = generators, each one is rated at 30 KVA

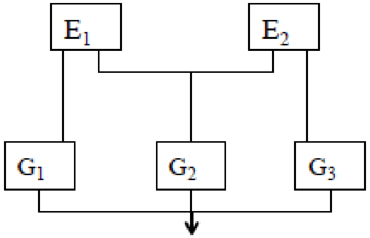
T = Failure to supply at least 60 kVA

FT construction: Procedure steps

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

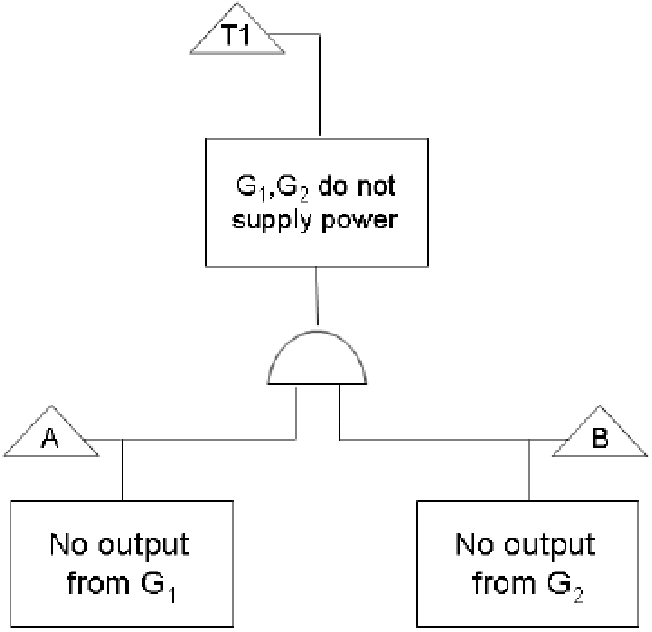
At least two out of the three generators do not work

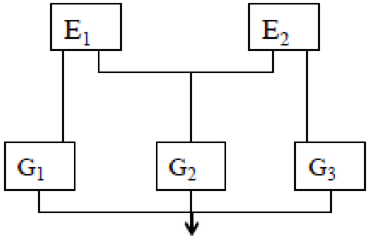




FT construction: Procedure steps

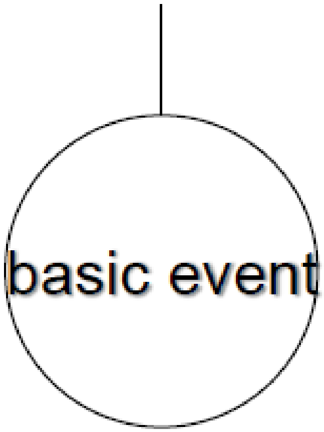
1. Define top event (system failure)
2. Decompose top event by identifying subevents which can cause it.
3. **Decompose each subevent in more elementary subevents which can cause it**





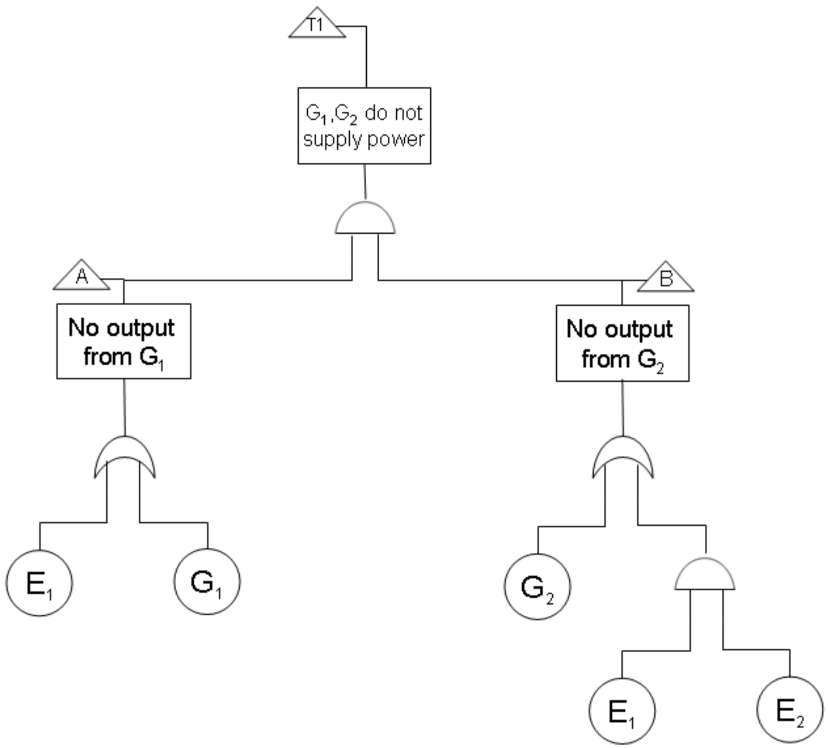
FT construction: Procedure steps

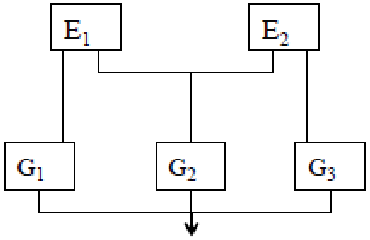
1. Define top event (system failure)
2. Decompose top event by identifying subevents which can cause it.
3. Decompose each subevent in more elementary subevents which can cause it
4. **Stop decomposition when subevent probability data are available (resolution limit): subevent = basic or primary event**



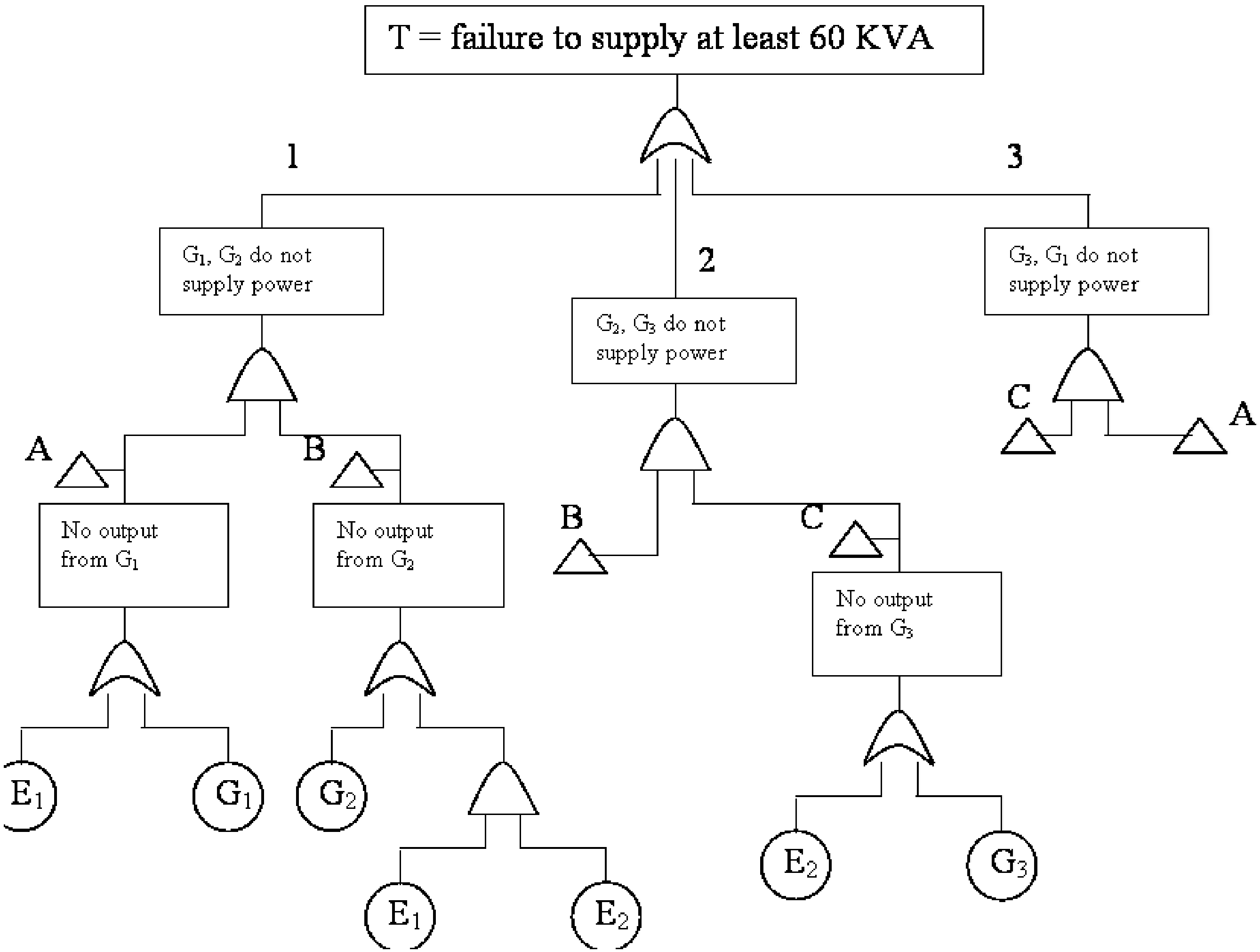
FT construction: Procedure steps

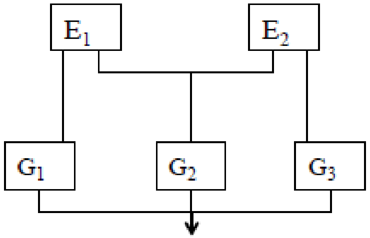
1. Define top event (system failure)
2. Decompose top event by identifying subevents which can cause it.
3. Decompose each subevent in more elementary subevents which can cause it
4. **Stop decomposition when subevent probability data are available (resolution limit): subevent = basic or primary event**



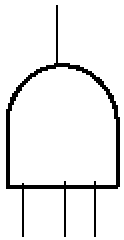
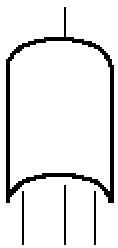
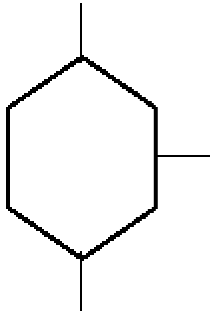


FT example 1

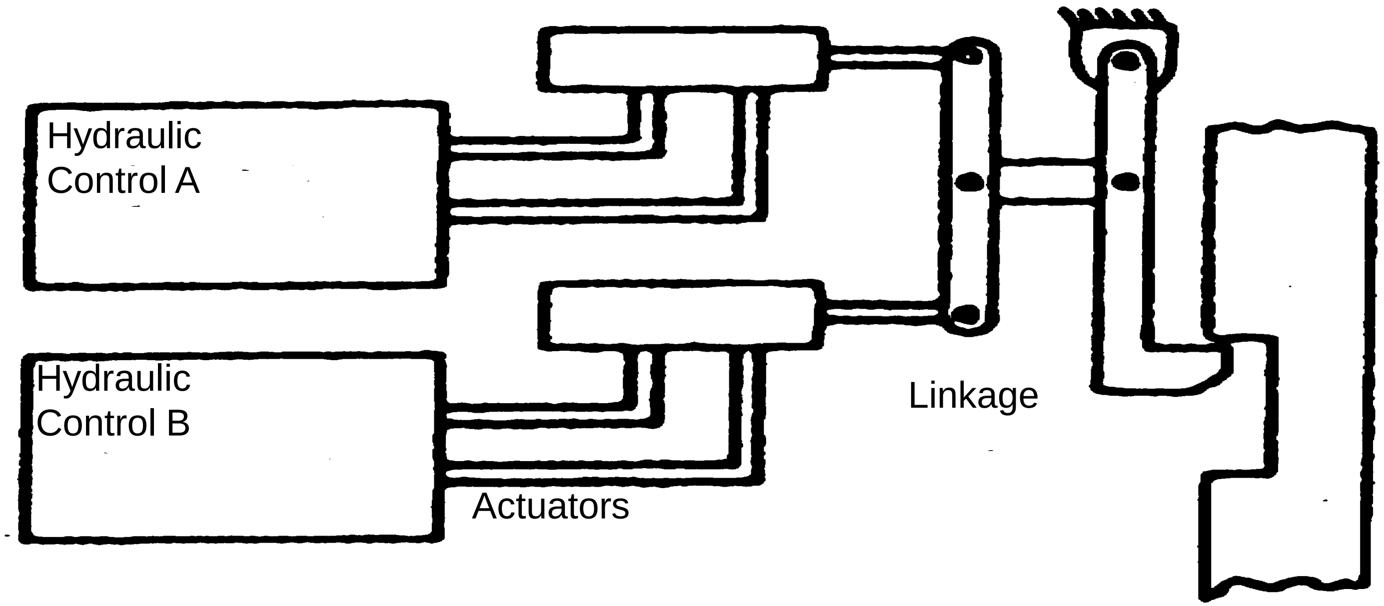

T = failure to supply at least 60 KVA
1
2
3
G1, G2 do not supply power
G2, G3 do not supply power
G3, G1 do not supply power
A
B
C
A
B
C
A
No output from G1
No output from G2
No output from G3
E1
G1
G2
E1
E2
E2
G3


E1
E2
G1
G2
G3

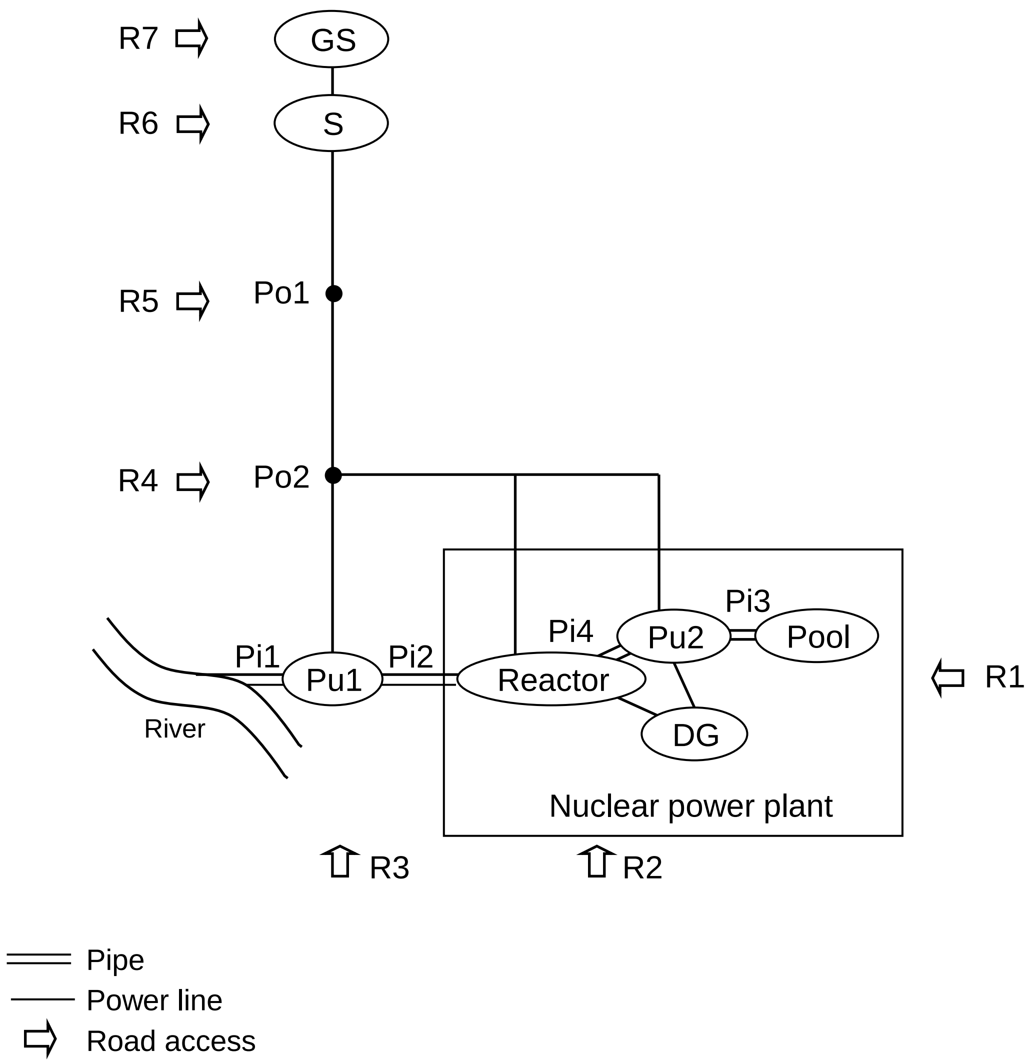
FT gate symbols

	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 Example 2: The System



FT Example 3: The System of Systems



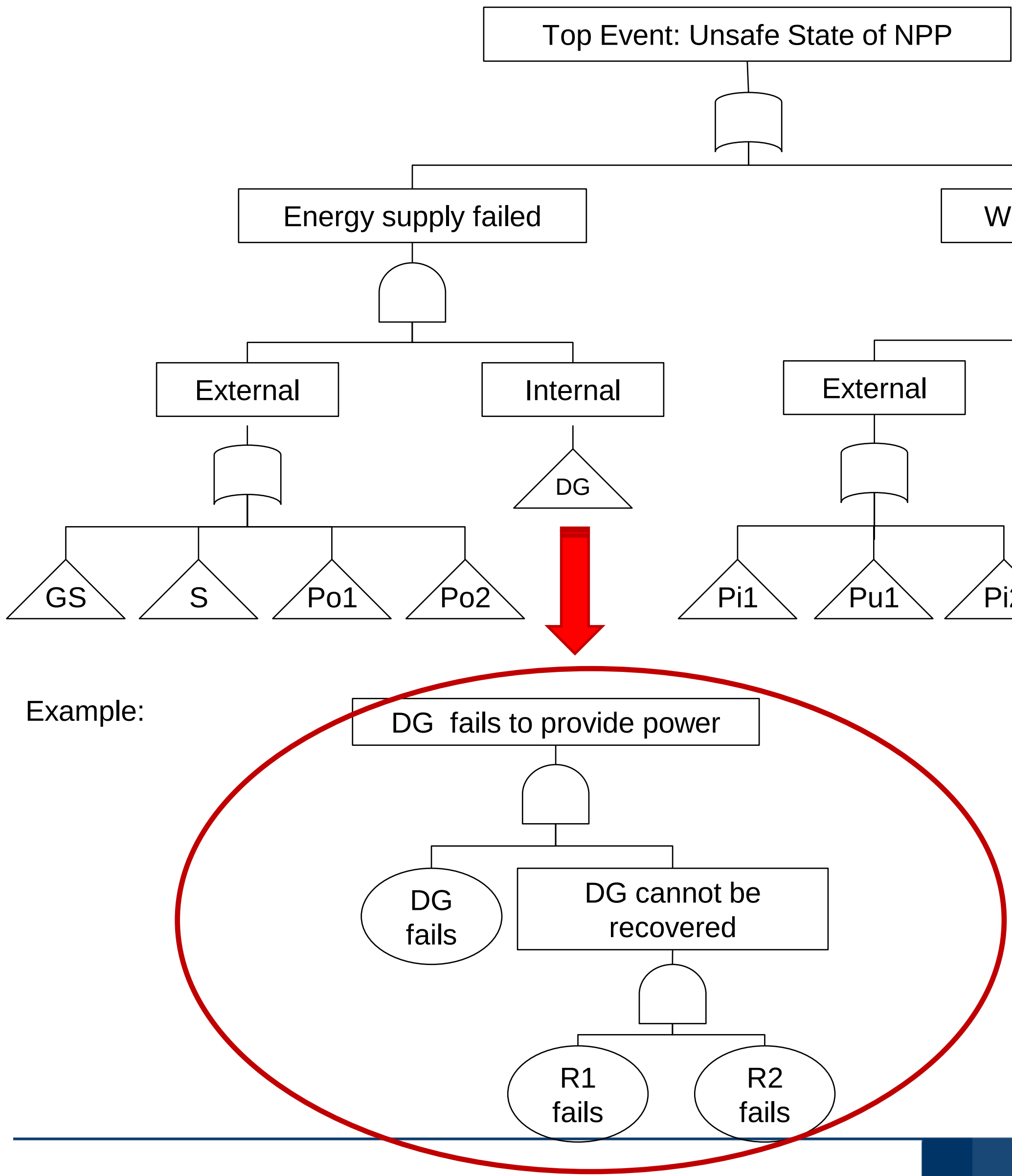
Internal emergency devices:

- 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)

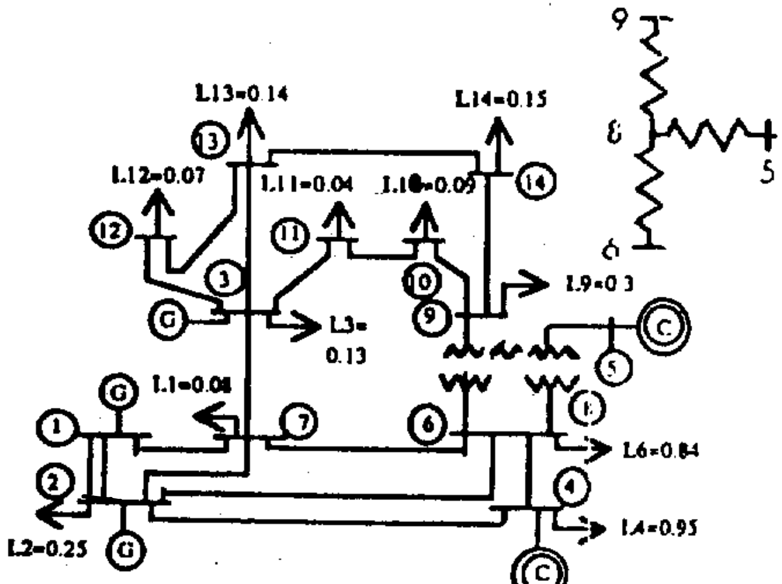
FT Example 3: Fault Tree



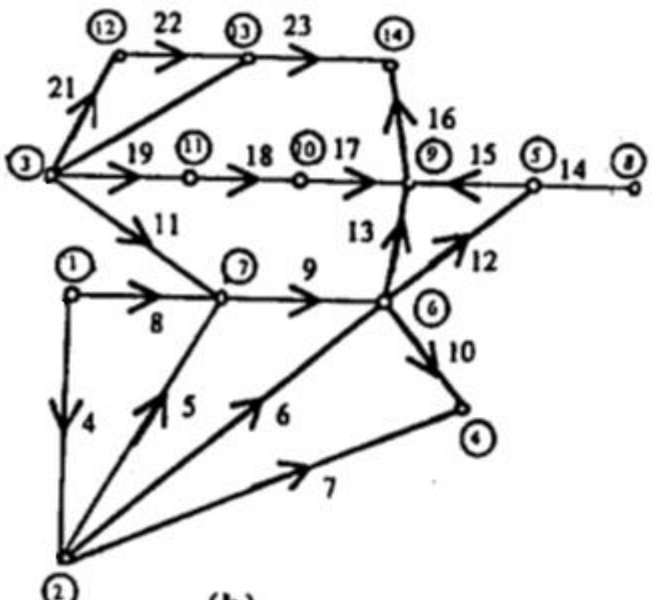
Hp: elements that fail can be immediately repaired/replaced if the access through the road system does not fail → roads considered as "reserve components".

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)

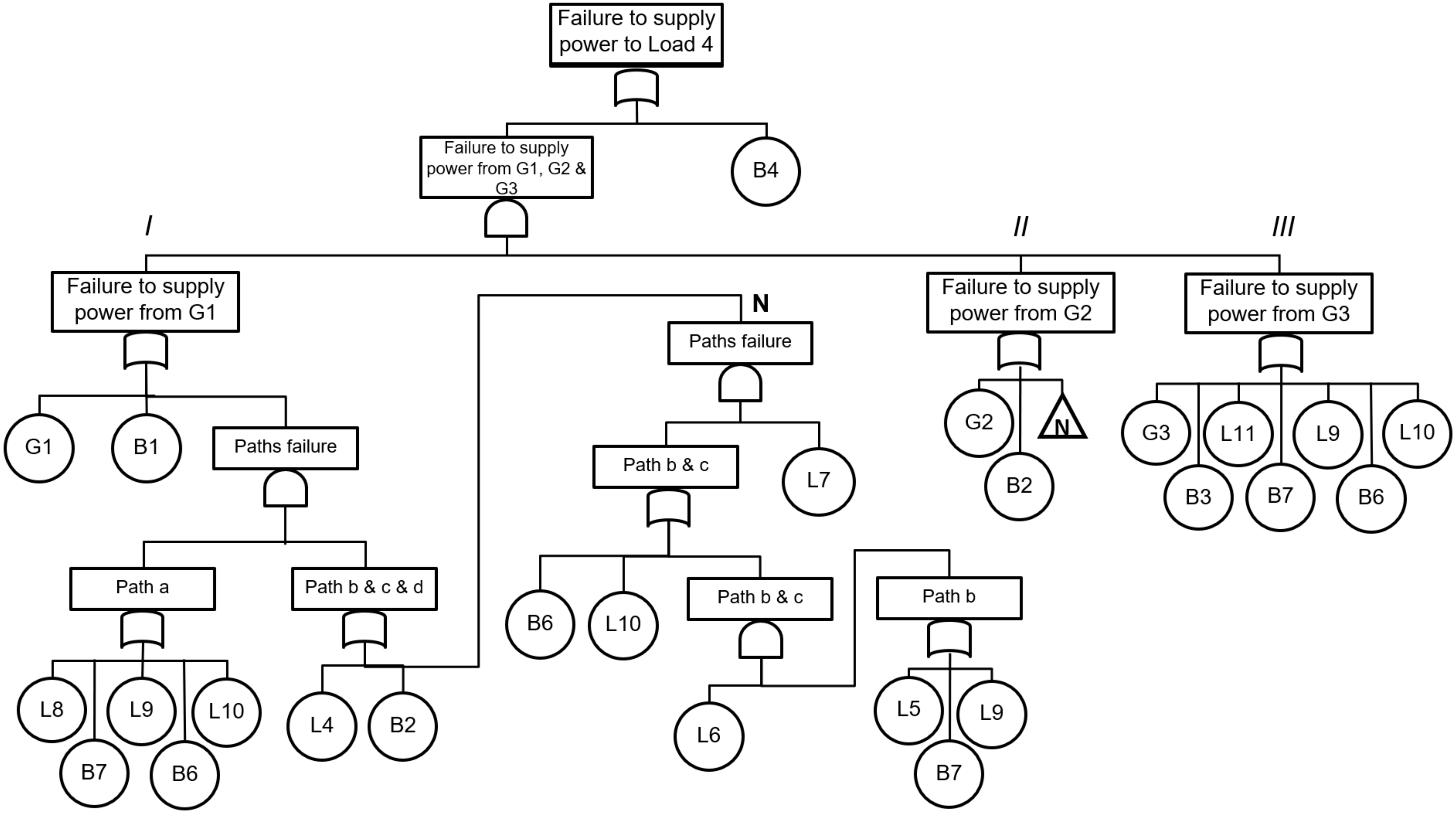
FT Example 4: IEEE14 Bus Power Distribution System

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 Load4”

FT Example 4: IEEE14 Bus Power Distribution System



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:***

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

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) $X + X = X$

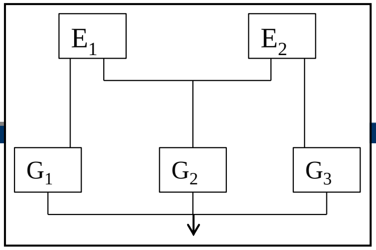
4) Absorption Law
   (a) $X(X + Y) = X$
   (b) $X + XY = X$

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

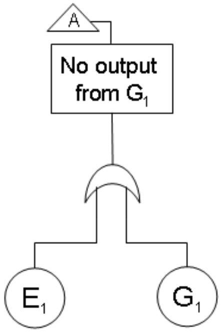
6) Complementation*
   (a) $X\overline{X} = \varnothing$
   (b) $X + \overline{X} = \Omega$
   (c) $\overline{\overline{X}} = X$

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

Structure function: Example 1

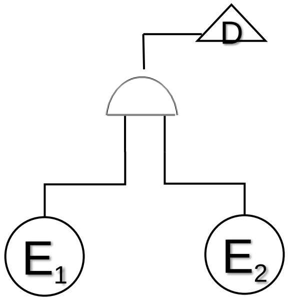


OR gate

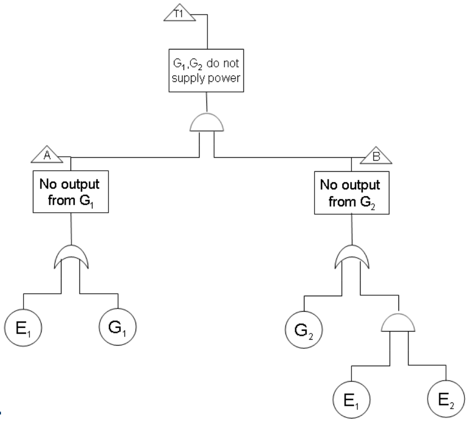


$$\mathbf{X_A = X_{E_1} + X_{G_1} - X_{E_1} X_{G_1} =}$$
$$= 1 - (1 - \mathbf{X_{E_1}})(1 - \mathbf{X_{G_1}})$$

AND gate



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



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

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.

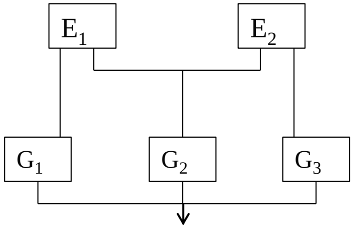
- **Reduce $\boldsymbol{\Phi}$ in terms of minimal cut sets (mcs)**
- **cut sets =** logic combinations of primary events which render true the top event
- **minimal cut sets =** cut sets such that if one of the events is not verified, the top event is not verified

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



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

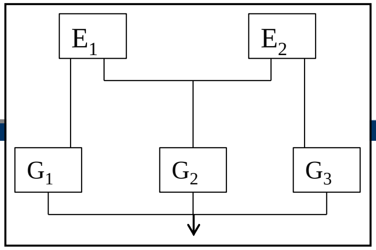
$$= (X_{E_1} + X_{G_1} - X_{E_1}X_{G_1})(X_{G_2} + X_{E_1}X_{E_2} - X_{E_1}X_{E_2}X_{G_2}) =$$

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

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

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

mcs: Example 1



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

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

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

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

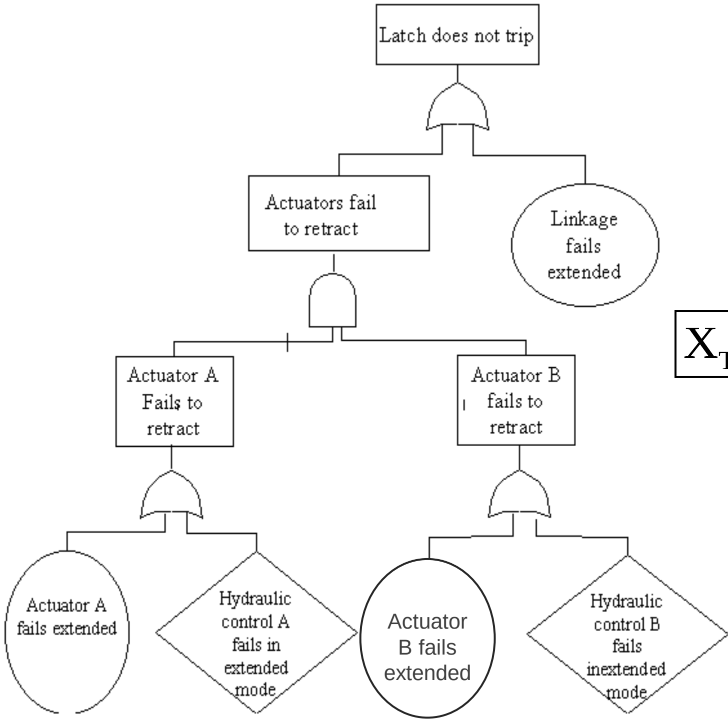
$$= 1 - [1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2} - X_{E_1}X_{G_2}(1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2})] =$$

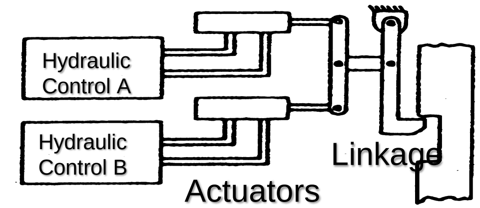
$$= 1 - [(1 - X_{E_1}X_{G_2})(1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2})] =$$

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

$$\text{3 minimal cut sets: } \begin{cases} M_1 = \{E_1G_2\} \\ M_2 = \{E_1E_2\} \\ M_3 = \{G_1G_2\} \end{cases}$$

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:

$M_1 = X_L$

$M_2 = X_A X_B$

$M_3 = X_A X_{HB}$

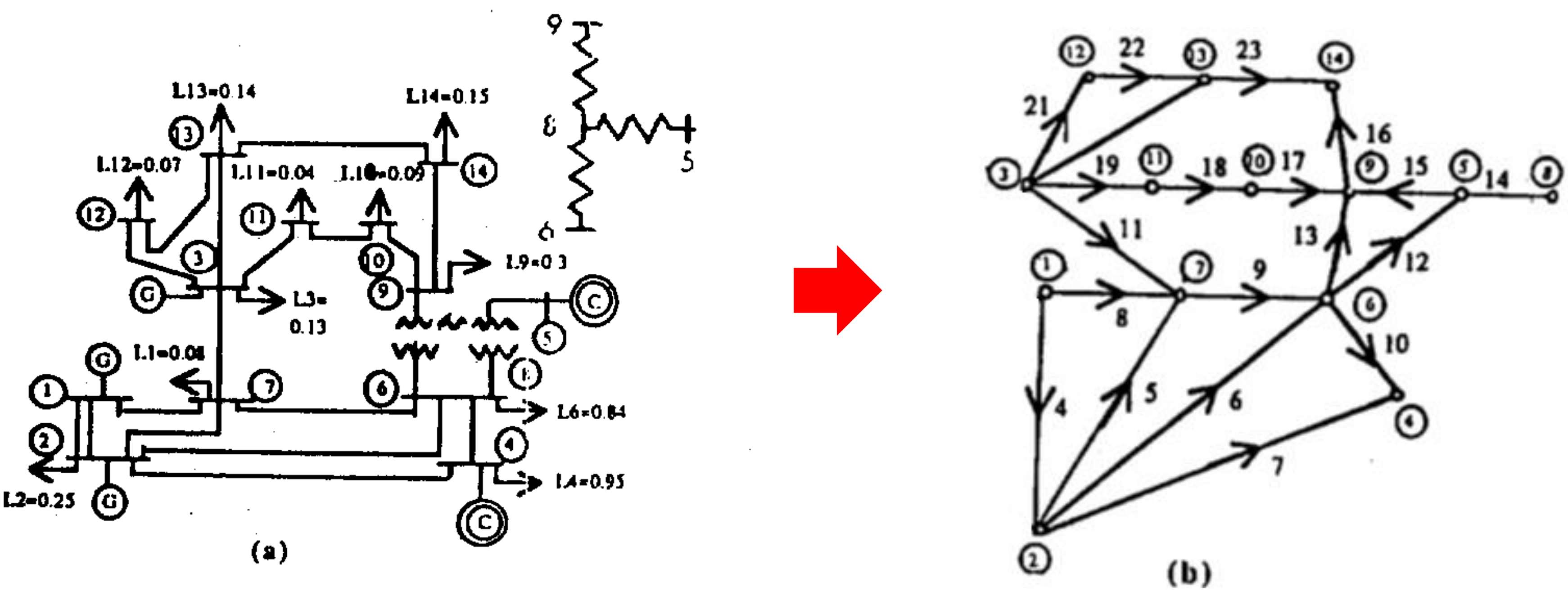
$M_4 = X_{HA} X_B$

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

FT qualitative analysis: results

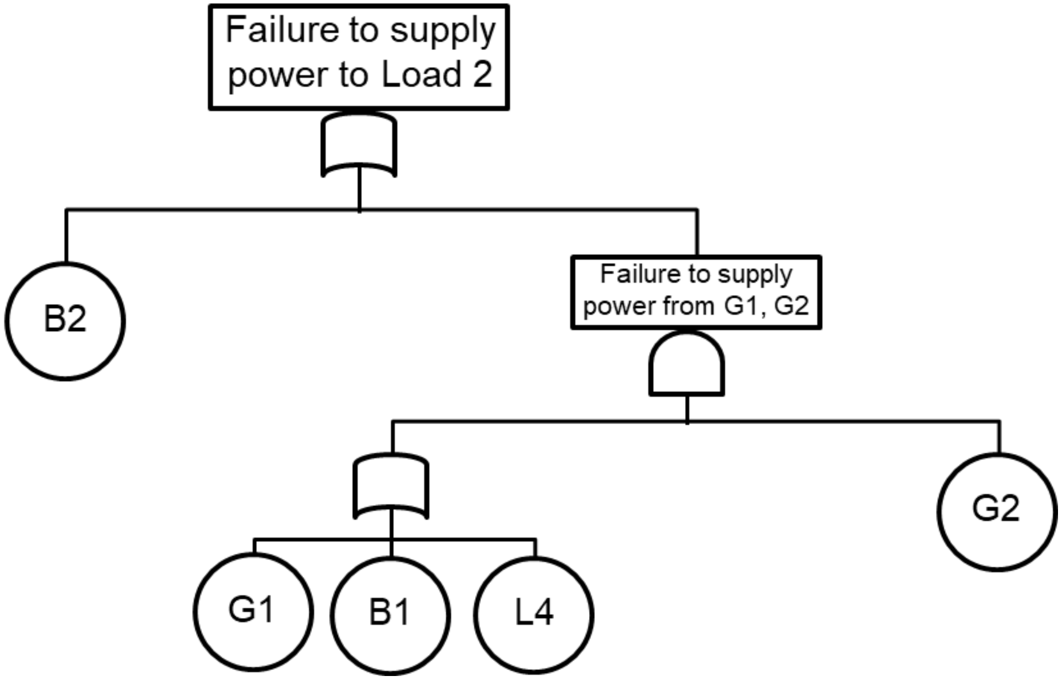
1. mcs identify the component basic failure events which contribute to system failure
2. qualitative component criticality: those components appearing in low order mcs or in many mcs are most critical

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”

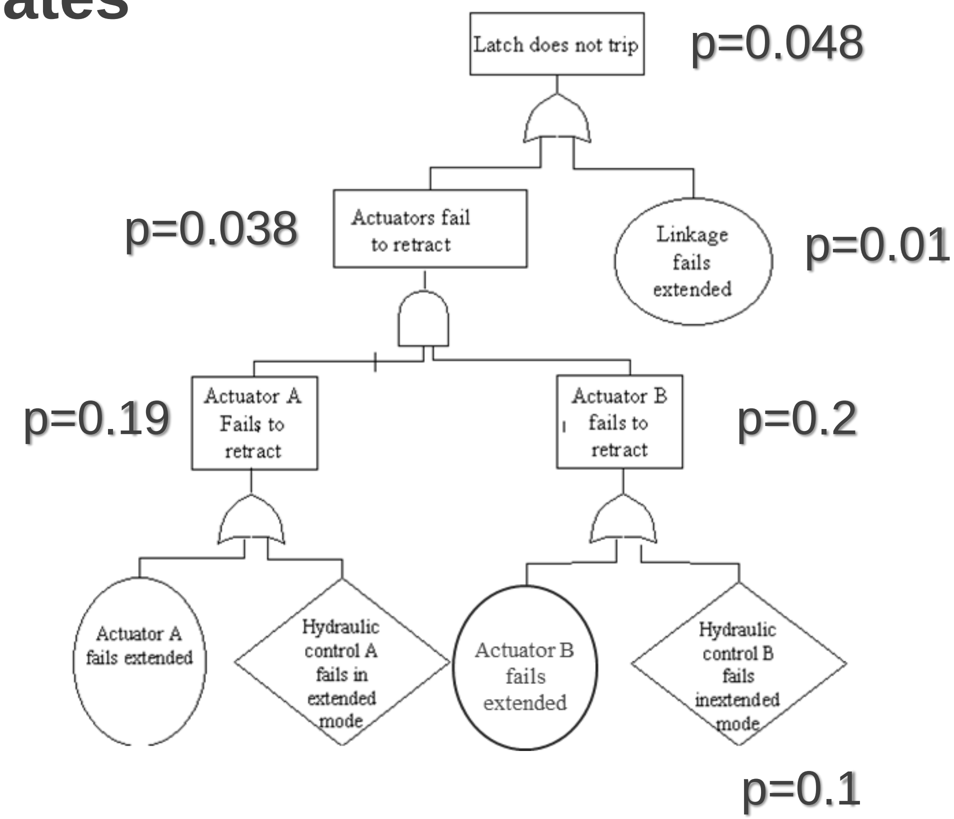


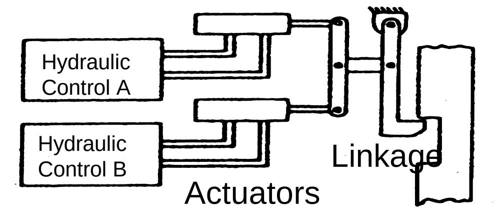
FT quantitative analysis

FT quantitative analysis

Compute system failure probability from primary events probabilities by:

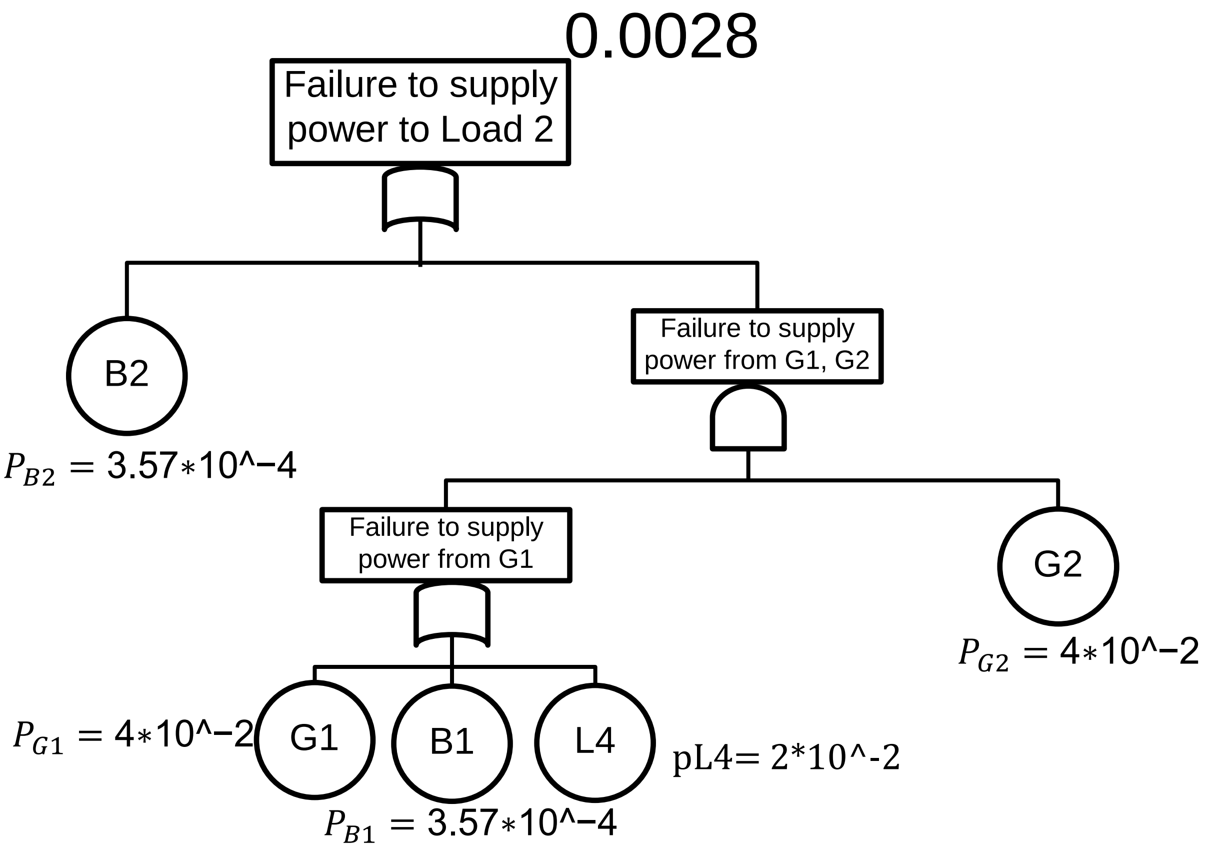
1. **using the laws of probability theory at the fault tree gates**





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:

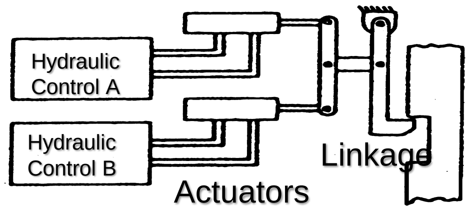
1. using the laws of probability theory at the fault tree gates
2. **using the mcs found from the qualitative analysis**

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

It can be shown that:

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

FT quantitative analysis: Example 2



5 mcs:

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

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

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

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

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

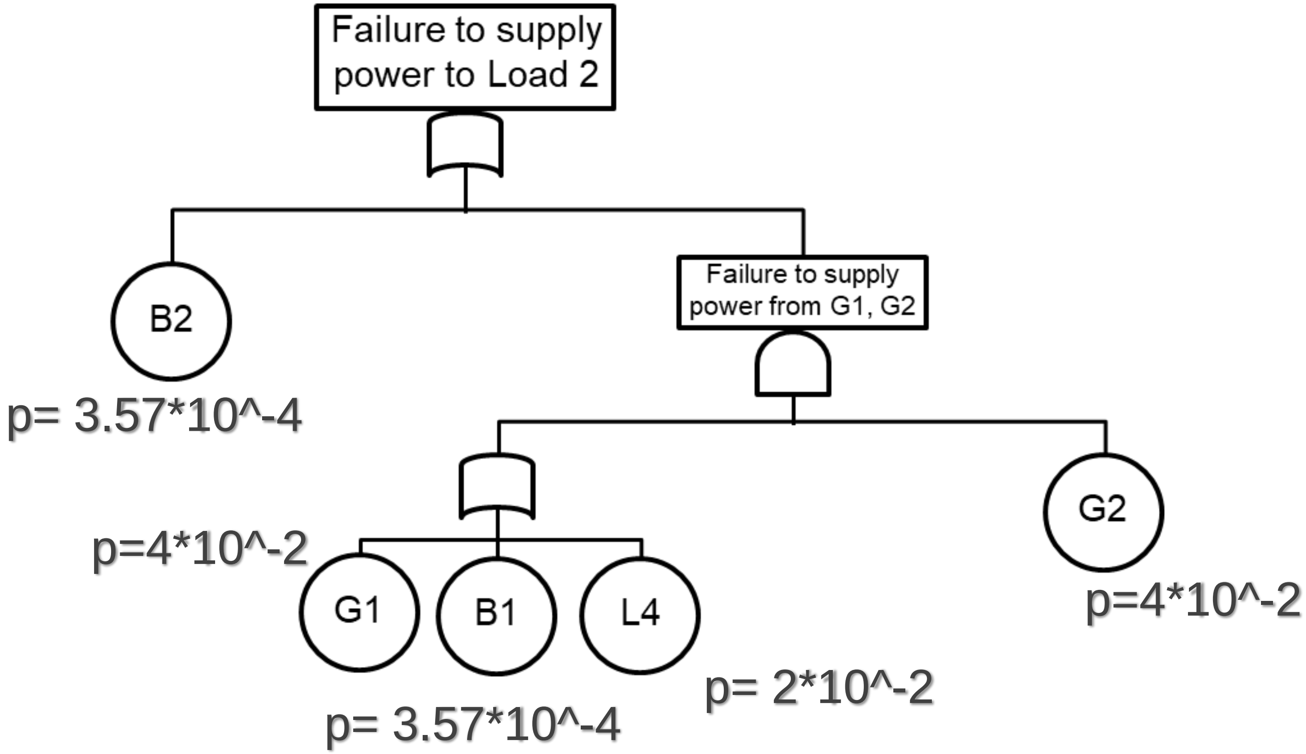
$\Downarrow$

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

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

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).