POLITECNICO DI MILANO

Logical Methods:
Project on system

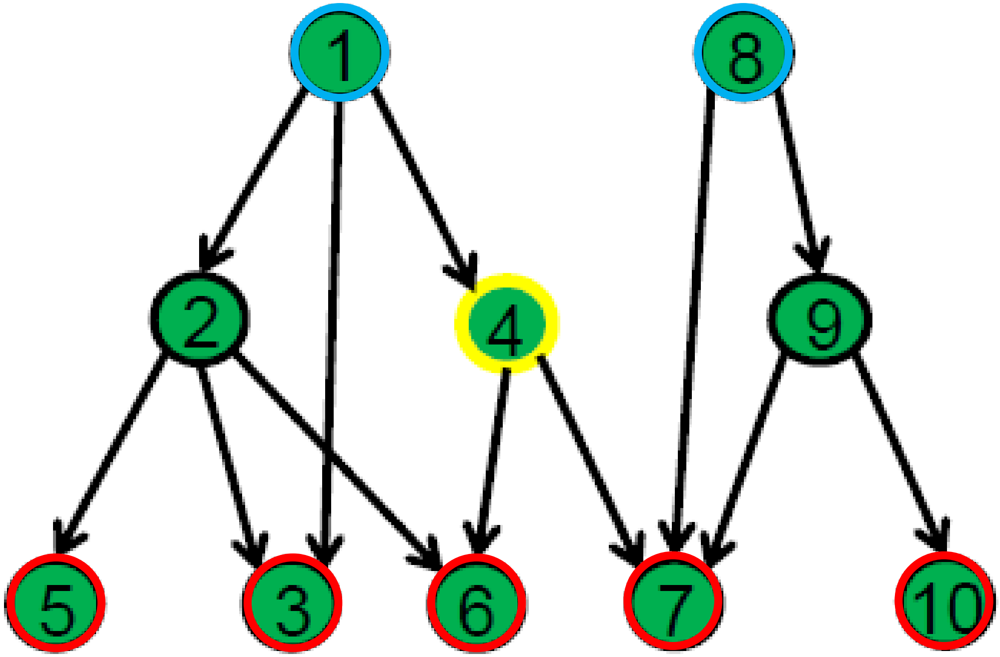
System: Electric Grid

○ Generators

○ Transformers

○ Redundancy (e.g. presence of diesel generators)

○ Consumers



A network with nodes and directed links:

- Each node has two states: safe vs failed
- The direction of links indicates the functional dependency
- Nodes having redundancy, yellow circle, will sustain disruptions coming from upper nodes.
- A node operates when all the nodes it depends on are functioning

Part 1

Generators in nodes 1 and 8 can be damaged by a landslide, if its magnitude is sufficiently large.
The return time of a landslide of such magnitude is 100y.
The failure probability of the generators, conditioned to such landslide occurrence is:

$$P(N1|L) = P(N8|L) = 4 \times 10^{-2}$$

Draw the Event Tree, with “landslide” as initiating event, and identify the success scenarios “consumers of node 7 are supplied with energy”.

- Consider the headings H_k

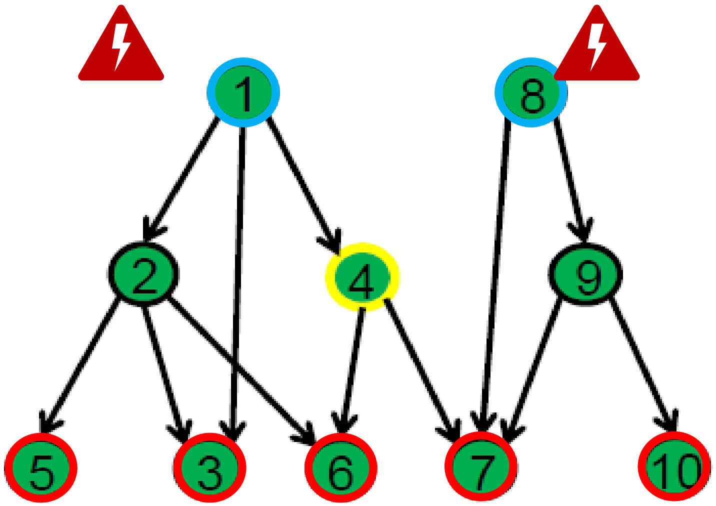
  H1: **“Node 8 out of service, due to the landslide”**

  H2: **“Node 1 out of service, due to the landslide”**

- Assume the following conditional probabilities

$$\boldsymbol{P(N8|L) = 4 \times 10^{-2}}$$

$$\boldsymbol{P(N1|L) = 4 \times 10^{-2}}$$



Part 2

Generators in nodes 1 and 8 can be damaged by a landslide, if its magnitude is sufficiently large. The return time of a landslide of such magnitude is 100y.
The failure probability of the generators, conditioned to such landslide occurrence is:

$$P(N1|L) = P(N8|L) = 4 \times 10^{-2}$$

Draw the Event Tree, with "landslide" as initiating event, and identify the success scenarios "consumers of node 7 are supplied with energy".

- Consider the headings H_k

  H1: **"Node 8 out of service, due to the landslide"**

  H2: **"Node 1 out of service, due to the landslide"**

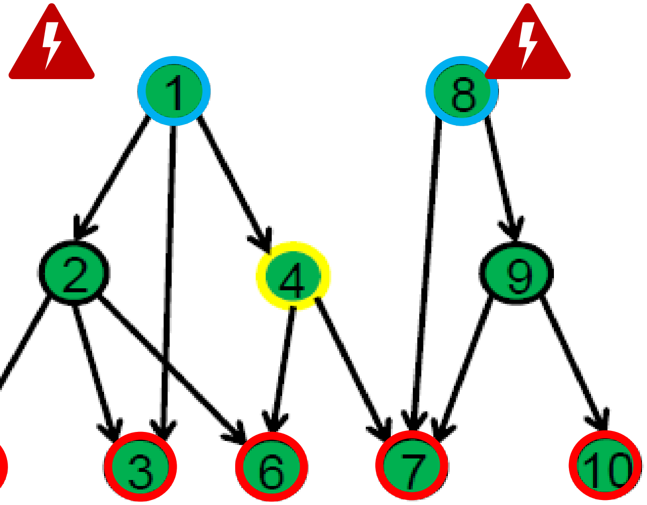
- Assume the following conditional probabilities

$$\boldsymbol{P(N8|L) = 4 \times 10^{-2}}$$

$$\boldsymbol{P(N1|L) = 4 \times 10^{-2}}$$

Consider the hypothesis:
"A node operates when at least one of the nodes it depends on is functioning well"

~~"A node operates when all the nodes it depends on are functioning well"~~



Part 3

Generators in nodes 1 and 8 can be damaged by a landslide, if its magnitude is sufficiently large. The return time of a landslide of such magnitude is 100y.
The failure probability of the generators, conditioned to such landslide occurrence is:

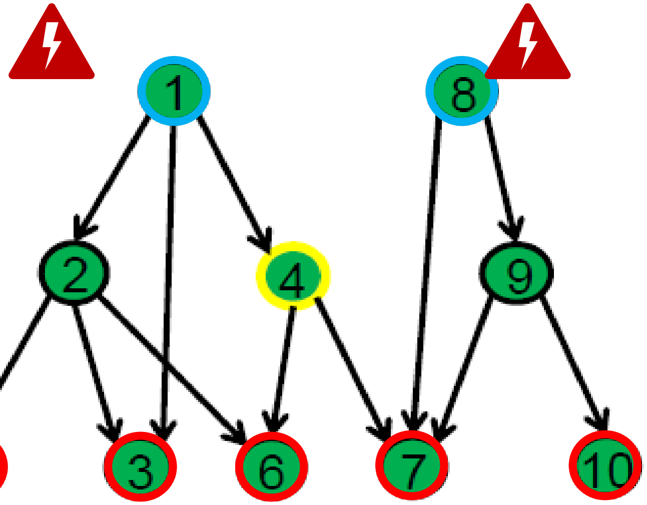
$$P(N1|L) = P(N8|L) = 4 \times 10^{-2}$$

Each node (also the redundant ones) is subject to random failures described by exponential distributions with parameter λ= $3 \times 10^{-4}\, Y^{-1}$. Given a mission time of 10 years:

a) Draw a Fault Tree and identify the Minimal Cutsets of the top event: “Consumers of node 7 are not supplied with energy”
b) Draw the Goal Tree Success Tree for the success scenario “Consumers of node 7 are supplied with energy”

~~“A node operates when at least one of the nodes it depends on is functioning well”~~

Consider the hypothesis:
“A node operates when all the nodes it depends on are functioning well”



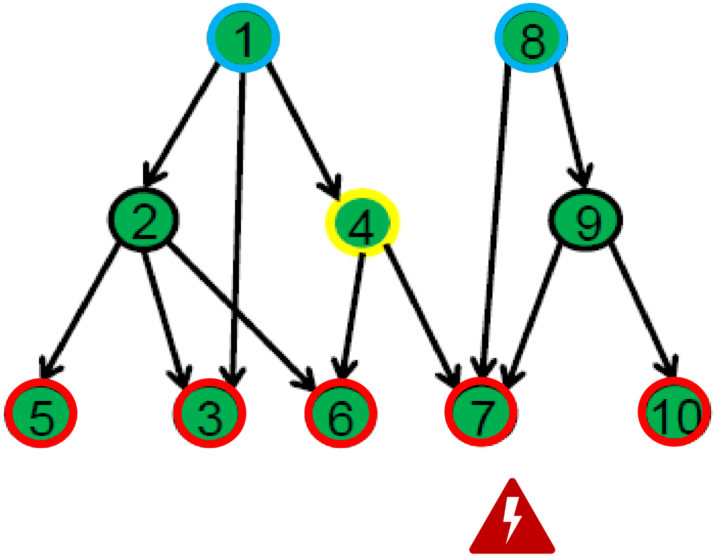
Fault Tree: Top event and subevents identification.

- Define the top event:

"Consumers of node 7 are not supplied with energy"

- Decompose the top event by identifying the subevents that can cause it:

"Node 9 fails in next 10y"
"Node 7 fails in next 10y"
"Generator 1 fails in next 10y"
"Generator 8 fails in next 10y"



- Decompose each sub-event by identifying more elementary subevents that can cause it until the basic events are identified:

- Build the fault tree

Appendix on geometric distribution

Given p the yearly probability of occurrence per year (i.e $p = \frac{1}{Return\,Time}$) of an event Y, the probability of the occurrence of Y at exactly the k-th year is equal to:

$$P(Y = k) = (1 - p)^{k-1} * p$$

Thus, the probability of the occurrence of Y in the next T years is equal to the sum of all the possible occurrences in between 1 and T:

$$P(Y < K) = \sum_{k=1}^{T} (1 - p)^{k-1} * p$$

If p=1/100 and T is equal to 10:

$P(Y < 10) = 0.0956$

Part 4:

Consider a chemical plant supplied by the energy station in node 7.
The plant has 3 safety levels against a possible “Loss of Primary Containment” (LOPC).
When a LOPC happens the plant can overheat, and cause severe damage, several ways to interrupt the accident sequence exist.

1. An automatic mechanical **valve** that is expected to stop the injection of reagents.

   Valve switch on failure probability → P$_v = 5 \times 10^{-2}$
2. A **reservoir** containing water to cool the plant, it must be activated by an operator.

   Human error probability→ $P_r = 2 \times 10^{-2}$
3. A **pump** that take water from underground to cool the plant, the pump is electrical and **supplied by node 7** of the grid.

   Pump switch on failure probability → P$_p = 10^{-2}$

   The pump is expected to supply water for one month in order to restore a safe condition. Note that the pump must be supplied with energy in order to work

Calculate the probability that the LOPC ends in overheating

→ (FT/ET link).