CSED601
Dependable Computing
Lecture 13

Jong Kim

Dept. of CSE

POSTECH

Copyright, 2018 © JKim POSTECH HPC

Review of Previous Lecture

- Reliability Evaluation Techniques
  - Markov modeling
    - Discrete Parameter Markov Chain
    - Continuous Parameter Markov Chain

Fault Trees

- Concept
  - A dual of reliability block diagram
  - Logic failure diagram
  - Think in terms of logic where
    - O = operating, 1 = failed
- Diagram
  - AND gate
    - All inputs must fail for the gate to fail
  - OR gate
    - Any input failure causes the gate to fail
  - K-of-n gate
    - K or more input failures cause gate to fail

Fault Trees

- Example
  - Triplex Bus Guardian
    - Three serially connected pass transistor
    - Two failure states
      - Failed Active : signal pass but does not function as a guardian
      - Failed Passive : signal cut
  - Modeling
    - Active mode
      - If three switches are failed active, then the system fail → AND gate of Failed Active
    - Passive mode
      - Cut off with any single unit failure → OR gate

Fault Trees

- Example
  - Total failure of Bus guardian
    - Caused by either active or passive mode
    - Draw your diagram here
  - K-of-N

Petri Nets

- Refer the slide made by Dr. Axel Krings
  - http://www2.cs.uidaho.edu/~krings/CS449/Notes.S13/449-13-11.pdf

GSPN

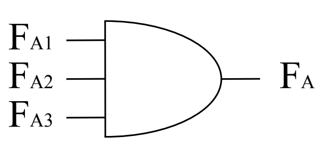
- General Stochastic Petri Net
- Refer the slide made by Dr. Axel Krings
  - http://www2.cs.uidaho.edu/~krings/CS449/Notes.S13/449-13-12.pdf

Fault Trees

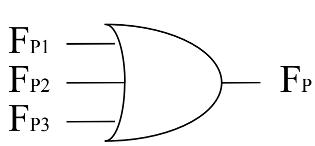
- Fault Trees
  - dual of Reliability Block Diagram
  - logic failure diagram
  - think in terms of logic where
    - 0 = operating, 1 = failed
- AND Gate
  - all inputs must fail for the gate to fail
- OR Gate
  - any input failure causes the gate to fail
- k-of-n Gate
  - k or more input failures cause gate to fail

e.g. Triplex Bus Guardian

- Active mode
  - M_1 and M_2 and M_3 fail =>
  - AND Gate

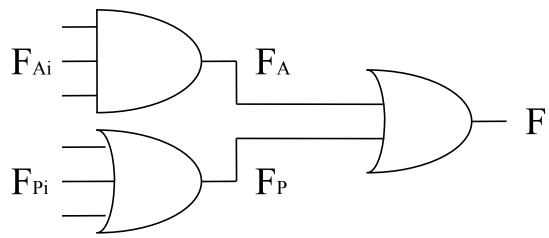


- Passive Mode
  - “cutoff” with any single unit failure =>
  - OR Gate



e.g. Triplex Bus Guardian

- Total Failure
  - caused by either active or passive mode



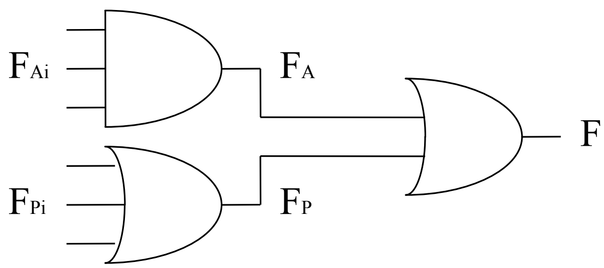
e.g. Triplex Bus Guardian

- How can one use the fault tree effectively to isolate those parts of the system that need reliability considerations?

e.g. Triplex Bus Guardian

- Combined fault model

$$Q(1000h) = 0.9851243 \cdot 10^{-6}$$



$$Q(1000h) = 0.295545 \cdot 10^{-1}$$

Examples

- Simple Passive TMR (no diagnosis)
  - RBD = (2 of 3): 2 operable => System operable
  - F-Tree = (2 of 3): 2 failed => System failed
- Simple TMR with *Benign* failures
  - RBD = (1 of 3): 1 operable => System operable
  - F-Tree = (3 of 3): 3 failed => System failed
- Summary
  - Parallel => AND
  - Series => OR
  - K-of-N => (n-k+1 of n)

Petri Nets

- Part of this discussion is based on the paper
  - *Petri Nets: Properties, Analysis and Applications*
  - by Tadoa Murata, Proc. IEEE, Vol. 77, No. 4, April 1989.
- Petri Nets
  - graphical and mathematical modeling tool
  - tool for describing systems characterized as being:
    - concurrent, asynchronous, distributed, parallel, nondeterministic and/or stochastic

Petri Nets

- History
  - **1962:** Carl Adam Petri's submitted his dissertation at the Uni. Darmstadt, Germany
  - **1970:** early development was published by A.W. Host and in the records of the 1970 Project MAC Conference on Concurrent Systems and Parallel Computation
  - **1970-75:** Computation Structure Group and MIT was most active
  - **1975:** conference on Petri Nets and Related Methods at MIT
  - **1979:** 135 researchers assembled in Hamburg, Germany, for 2-week advanced course on General Net Theory of Processes and Systems
  - **1980:** first European Workshop on Applications and Theory of Petri Nets, Strasbourg, France.
  - check out Murata's paper for the extensive literature discussion

Petri Nets

- General:
  - directed, weighted, bipartite graph
  - two kinds of notes (Places P, Transitions T)
  - arcs from P to T or from T to P
  - arcs have integer weights
  - non-negative Place weights are called tokens

Petri Nets

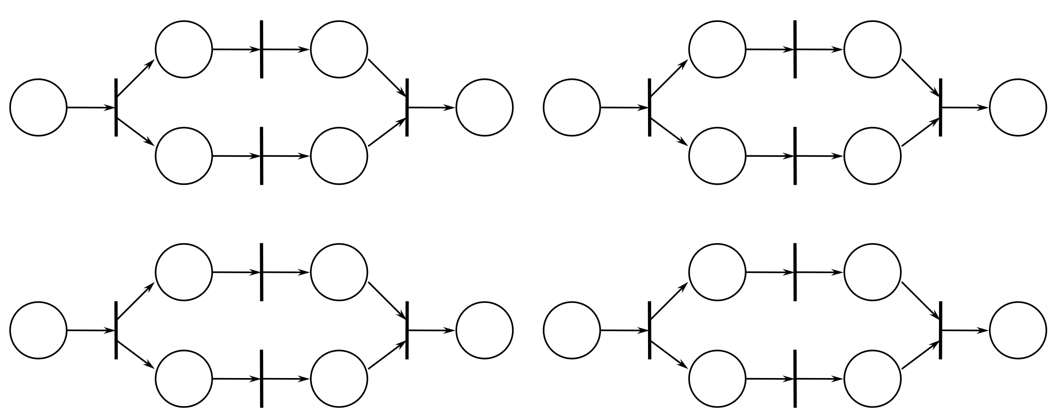
- A Petri Net is a 5-touple PN={P,T,A,W,M0}
- Place Set P = $\{p_1, p_2, \ldots, p_m\}$
  - finite set of places
  - condition = place
  - one condition or set of atomic conditions
  - symbol ◯
- Transition Set T = $\{t_1, t_2, \ldots, t_n\}$
  - finite set of transitions
  - action = transition
  - one action or set of atomic transitions
  - symbol —

Petri Nets

- Arc Set $A \subseteq (P \times T) \cup (T \times P)$
  - set of directed arcs
  - edge of graph = arc
  - symbol $\longrightarrow$
- Weight Function $W = A \rightarrow \{1,2,3,\ldots\}$
  - weights are associated with arcs
- Initial Marking $M_0 = P \rightarrow \{0,1,2,\ldots\}$
  - the initial assignment of tokens to places

Petri Nets

- example



Petri Nets

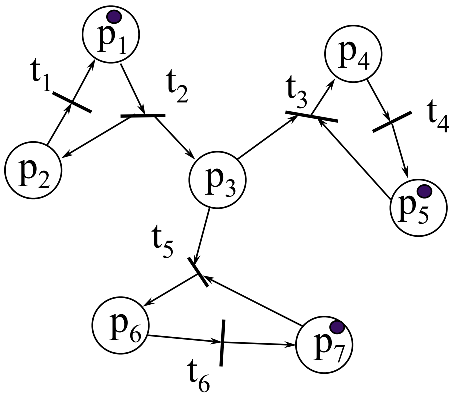
- Dynamic Behavior
  - during simulation of a petri net the state of the net may change
  - change of state:
    - transitions can be enabled
    - enabled transitions may fire
    - firing transition changes the marking of the net
    - the marking is the "snap-shot" of all the tokens

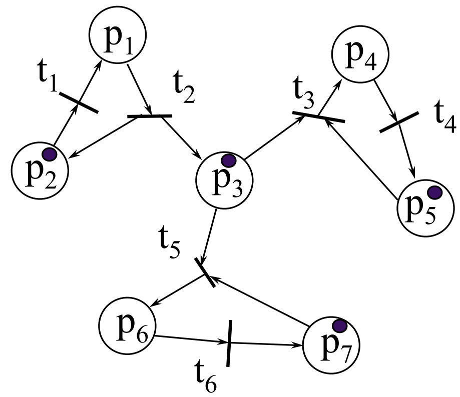
Petri Nets

- Firing rules
  - A transition T is said to be *enabled* if each input place P is marked with at least $W(P,T)$ tokens
    - $W(P,T)$ is the weight of the arc from P to T
  - An enabled transition may or may not fire (depending on whether or not the event actually takes place).
  - A *firing* of an enabled transition T removes $W(P,T)$ tokens from each input place P of T, and adds $W(T,P)$ tokens to each output place P of T
    - $W(T,P)$ is the weight of the arc from T to P
  - Common misconception: When a transition fires, it does **not** *move* tokens
    - i.e. the number of tokens in the system is not necessarily constant

Petri Nets

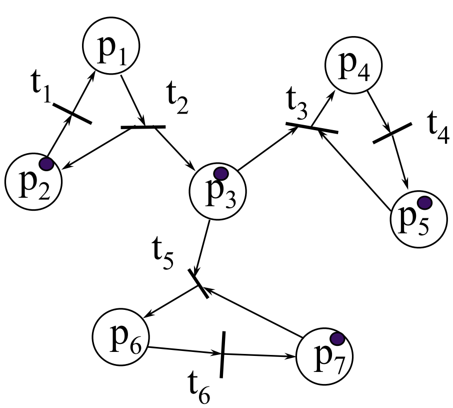
- Example: assume the following initial marking
  - Only one transition is enabled, i.e. t_2

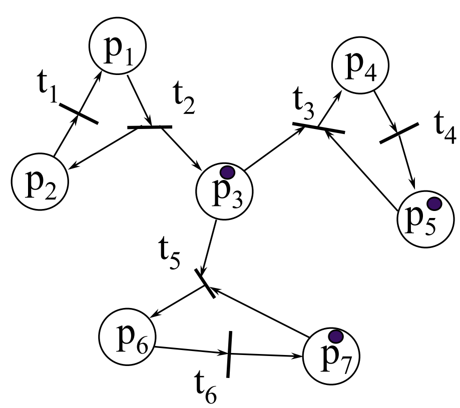




Petri Nets

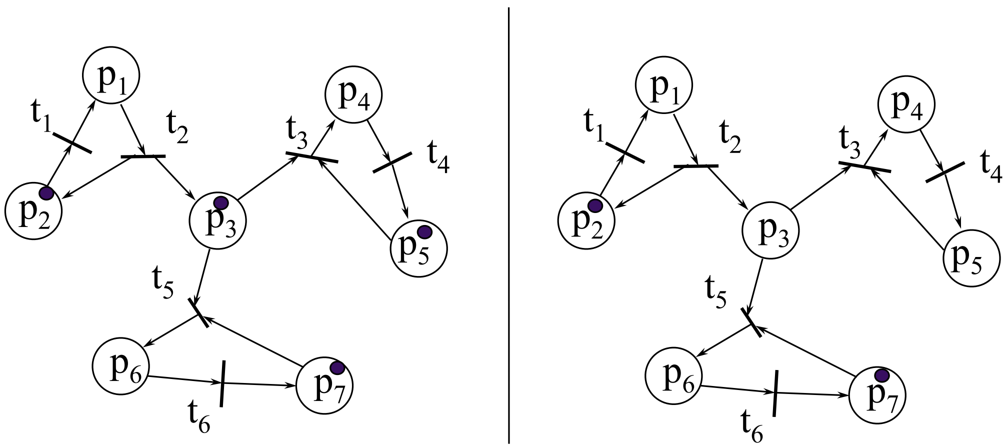
- Now several transitions are enabled, i.e. t_1 t_3 and t_5
- if t_1 fires first





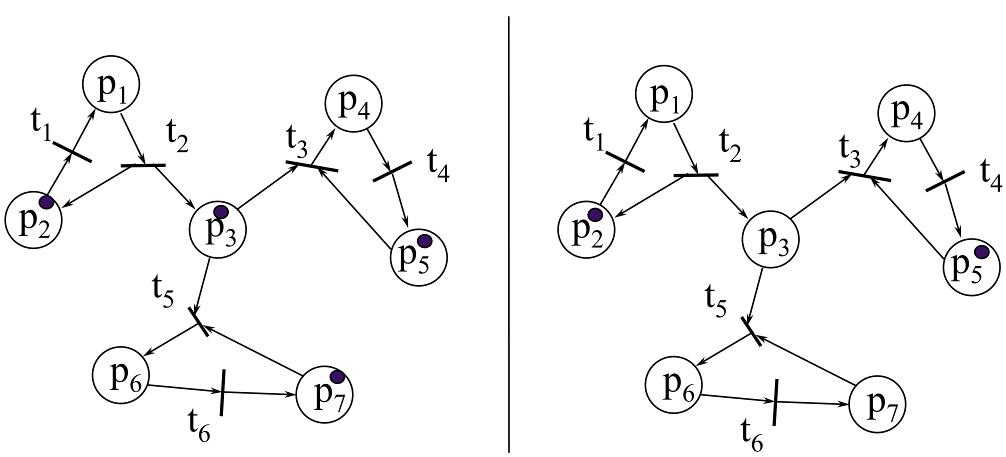
Petri Nets

- if t_3 fires first



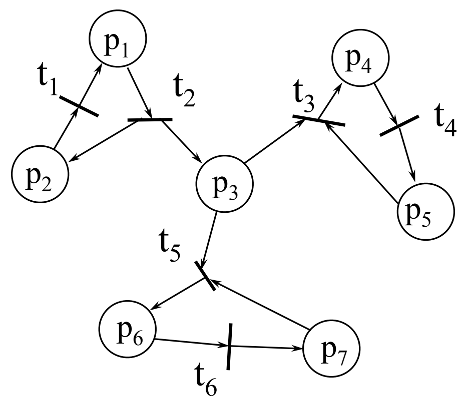
Petri Nets

- if t_5 fires first
- t_3 and t_5 are said to be in conflict



Petri Nets

– what could this Petri net represent?



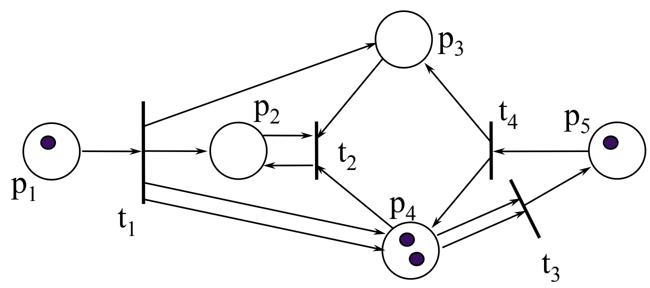
Petri Nets

- Marking: Number and placement of tokens
  - let m_i = # of tokens in place p_i
  - then marking

    $M = \{m_1, m_2, ..., m_n\}$
  - marking -- system state
  - Advantage: economy of model
    - e.g. assume net with 6 places
      - we limit each place to maximal 1 token
      - then there are 2^6 possible markings
      - => 64 states
      - thus Petri Nets are a lot smaller than state diagrams, i.e. Markov chains

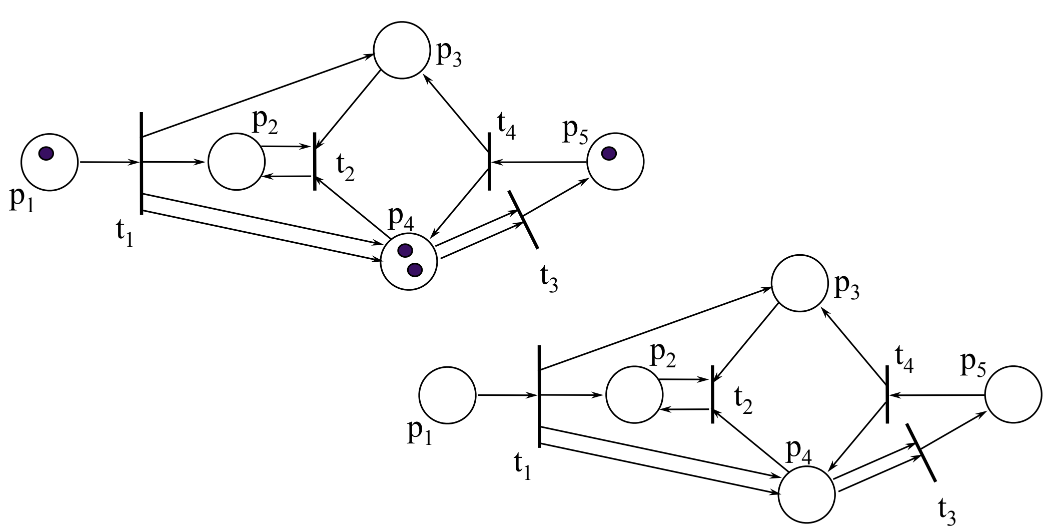
Petri Nets

- Firing rules
  - transition 1,3 and 4 are enabled



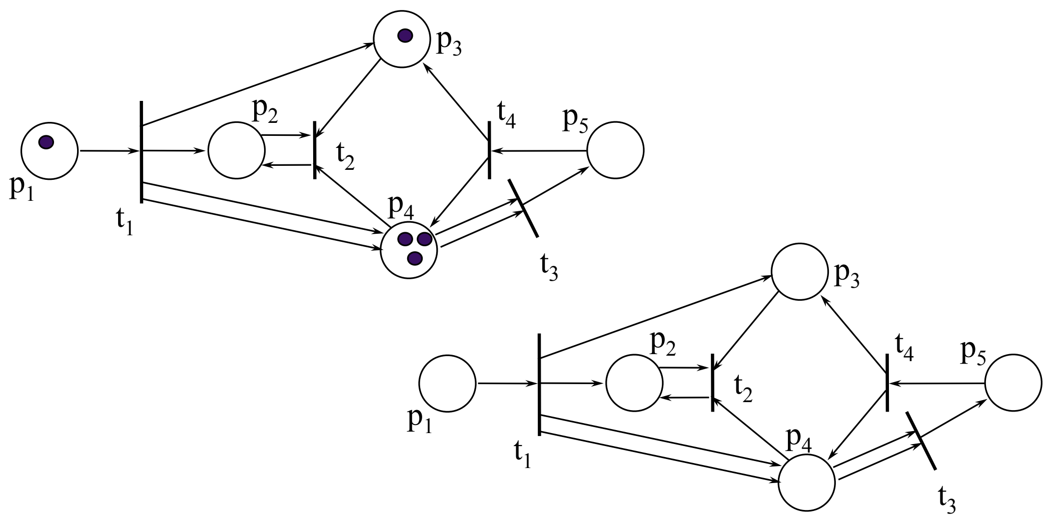
Petri Nets

- Firing rules
  - transition 4 fires



Petri Nets

- Firing rules
  - transition 1 fires



Petri Nets

- Firing rules
  - transition 3 fires