Security Analysis of Safety Critical and Control Systems

Outline

- Introduction
- Security Modeling Process
- Petri nets
- A Case Study
- Using Petri net for security analysis
- Conclusions

Introduction

- Software has become an integral part of everyday system upon which the million of live depends.
- In early stage software into safety critical environment, were used to only expand the performance, flexibility and efficiency of systems. But now days it is major components consider for safety purpose.
- Problem of security and safety become important when these critical applications include software where consequence of failure of software are serious and may grave danger to human life and property.

Introduction

Safety critical system is a system where human safety is dependent upon the correct operation of system. If the failure of a system could lead to consequences that are determined to be unacceptable then the system is safety critical.

a) **Railway**

b) medical system

d) Airbag

c) Nuclear power plants

e) Airspace

Introduction

Digital technologies such as computers, control systems, and data networks currently play essential roles in modern nuclear power plants (NPPs). These digital technologies make the operation of NPPs more convenient and economical; however, they are inherently susceptible to cyber-attacks.

- In 2003, the enterprise and control networks of the Davis-Besse NPP in the US were shut down because of an infection by the Slammer worm.
- In 2006, the instrumentation and control (I&C) systems of the Browns Ferry NPP in the US state of Alabama were disabled because of a digital network problem; therefore, an operator shut down its operation manually.
- In addition, in 2010, a malicious code called Stuxnet damaged the Natanz nuclear power facility in Iran.

According to the Dr. Rajeswari Pillai Rajagoplam is senior Fellow at the Observer Research Foundation, New Delhi in her article “Nuclear Research in India”

One of the more probable threats to Indian nuclear facilities could come in the form of cyber attacks. The capacity of terrorist groups to use cyber tools to attack a nuclear installation is far higher as compared to other attacks. As more and more systems rely on computer networks, cyber attacks have grown to be a major threat to India's nuclear installations.

Thomas Franch is Senior Vice President of Reactors and Services for AREVA, Inc., North America

- Across the nation, nuclear plants are being licensed to operate for longer periods of time and are transitioning from analog to digital systems for increased safety and performance. While this transition to digital technology is increasing the capability, longevity, safety and reliability of America's nuclear plants, the need to integrate cybersecurity measures is a necessity.

- Protecting the U.S. nuclear power infrastructure from exploitation and cyberattacks perpetrated against critical system networks is an industry challenge.

Security Modeling Process

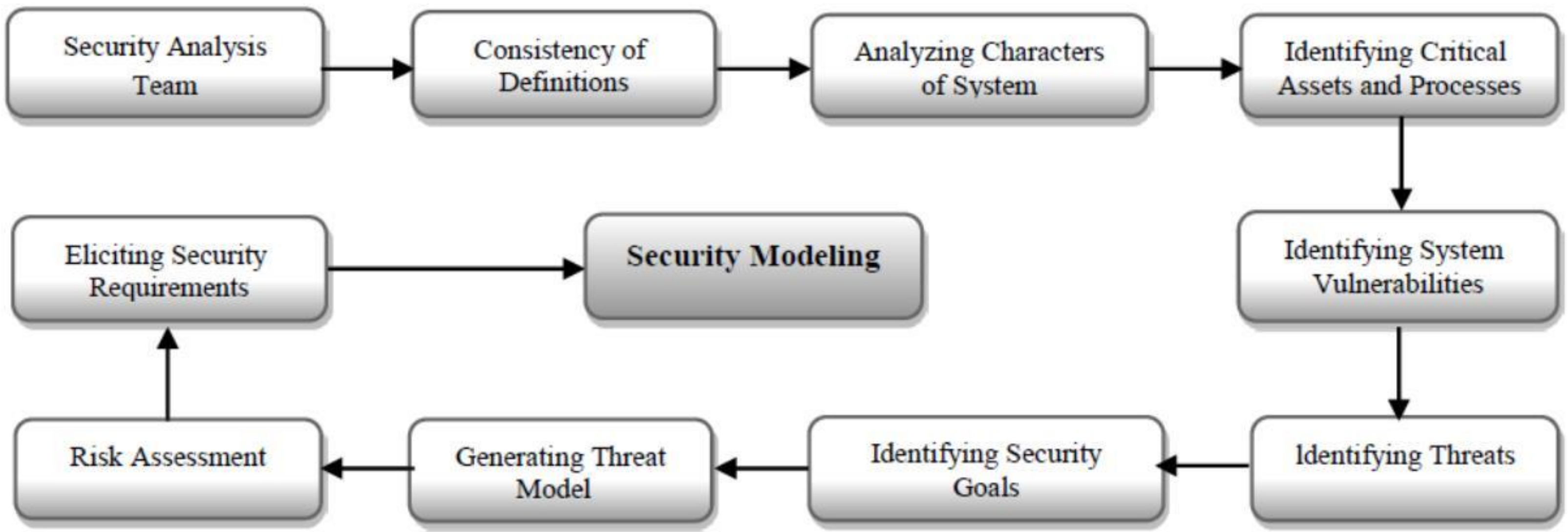


Figure 1. Security Modeling Process

Petri nets

- concurrent, asynchronous, distributed, parallel, nondeterministic and/or stochastic systems
- graphical tool

  -visual communication aid
- mathematical tool

  -state equations, algebraic equations, etc
- communication between theoreticians and practitioners

Petri nets History

- **1962**: C.A. Petri’s dissertation (U. Darmstadt, W. Germany)
- **1970**: Project MAC Conf. on Concurrent Systems and Parallel Computation (MIT, USA)
- **1975**: Conf. on Petri Nets and related Methods (MIT, USA)
- **1979**: Course on General Net Theory of Processes and Systems (Hamburg, W. Germany)
- **1980**: First European Workshop on Applications and Theory of Petri Nets (Strasbourg, France)
- **1985**: First International Workshop on Timed Petri Nets (Torino, Italy)

Petri nets Applications

- **performance evaluation**
- **communication protocols**
- distributed-software systems
- distributed-database systems
- concurrent and parallel programs
- industrial control systems
- discrete-events systems
- multiprocessor memory systems
- dataflow-computing systems
- fault-tolerant systems
- etc, etc, etc

Petri nets Definition

- Directed, weighted, bipartite graph
  - places
  - transitions
  - arcs (places to transitions or transitions to places)
  - weights associated with each arc

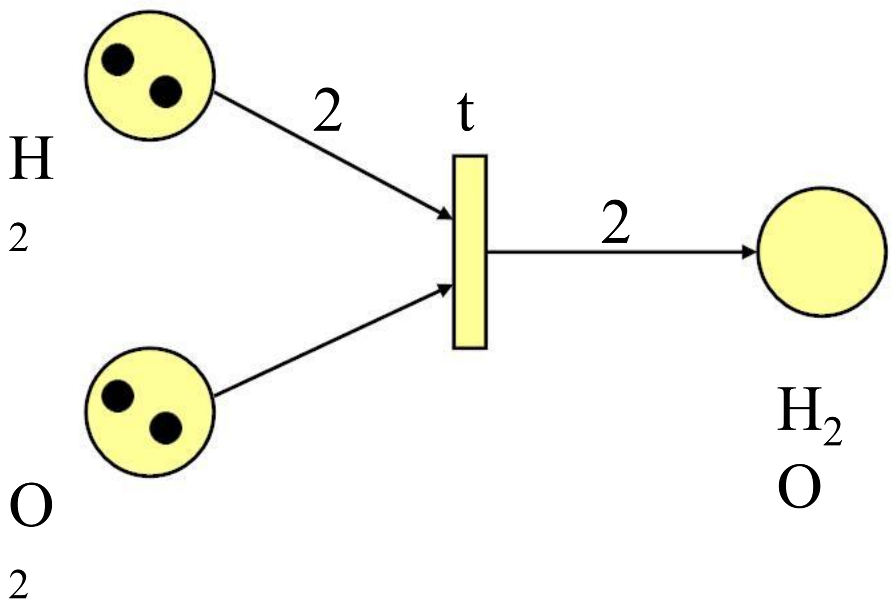
- Initial marking
  - assigns a non-negative integer to each place

Petri nets Definition

- A transition t is enabled if each input place p has at least w(p,t) tokens
- An enabled transition may or may not fire
- A firing on an enabled transition t removes w(p,t) from each input place p, and adds w(t,p') to each output place p'

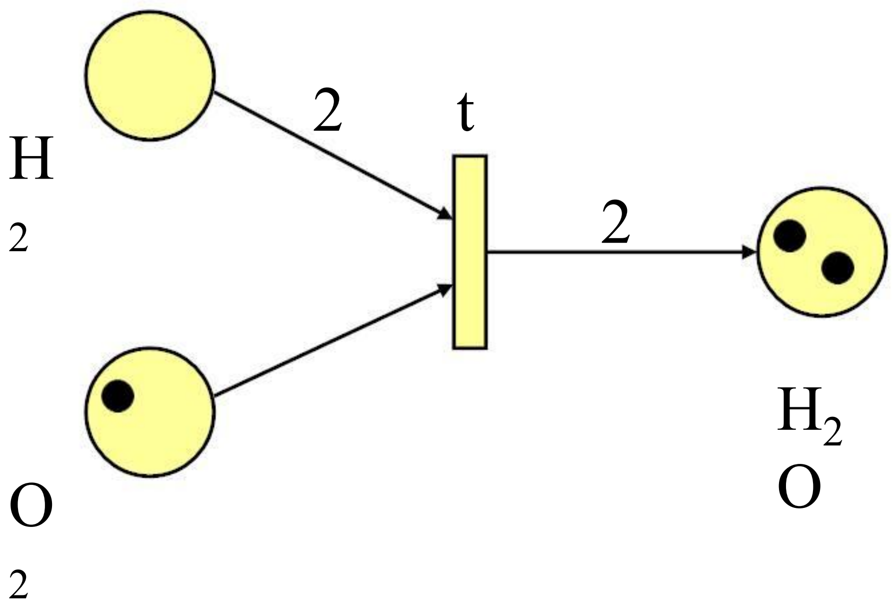
Petri nets Firing example

$2H_2 + O_2 \rightarrow 2H_2O$

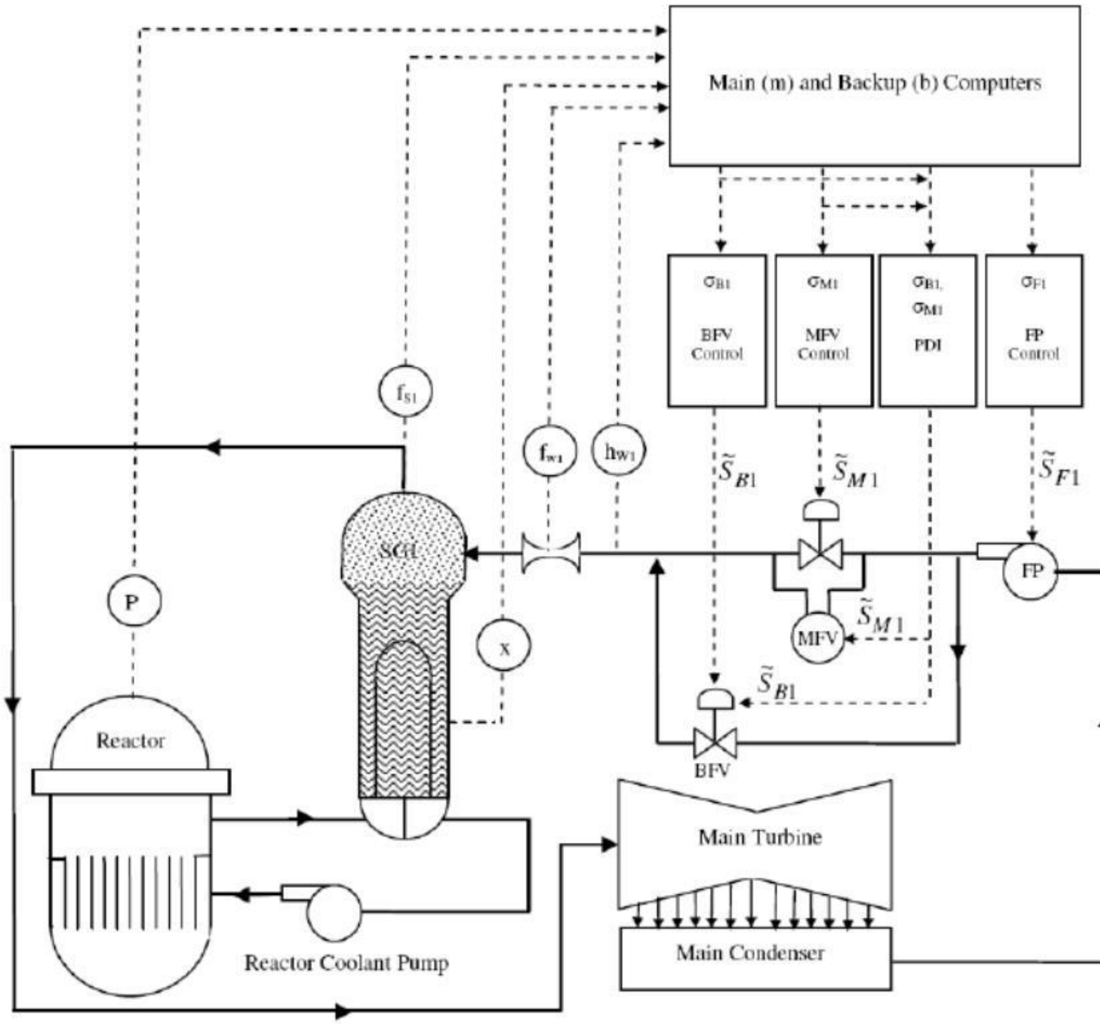


Petri nets Definition

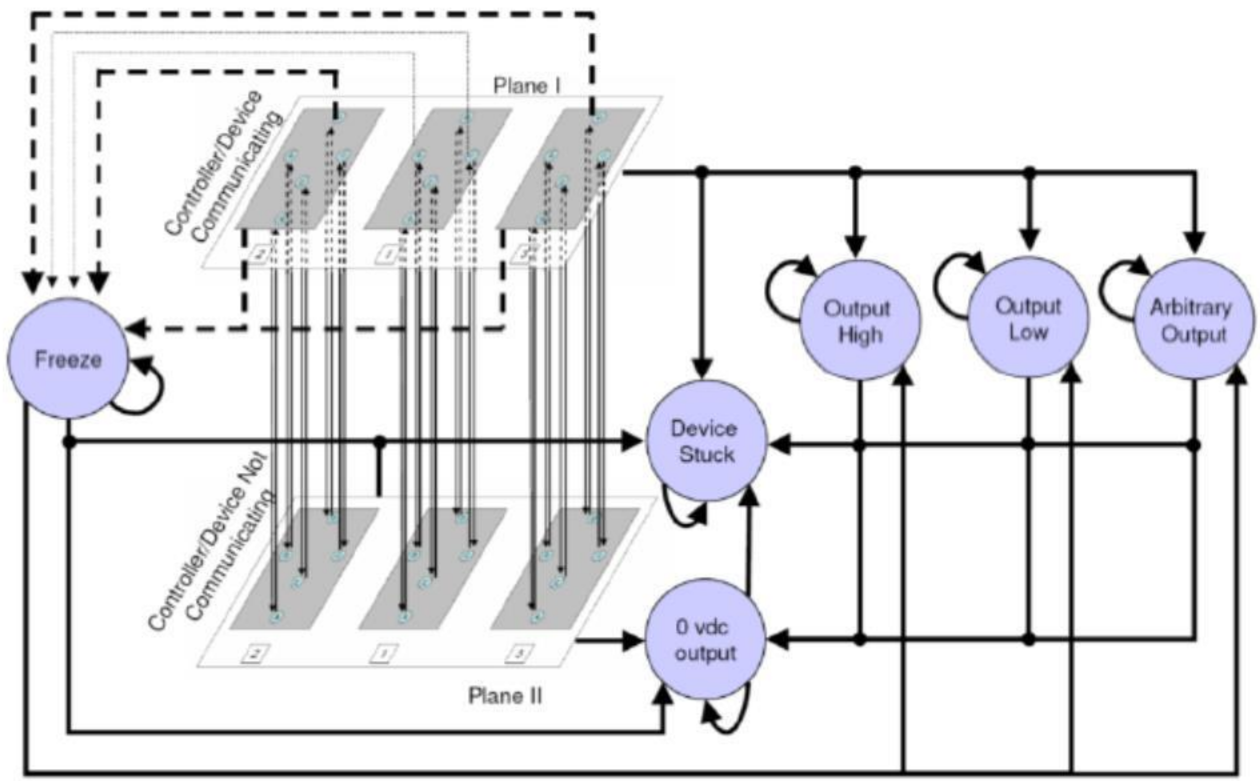
- $2H_2 + O_2 \rightarrow 2H_2O$



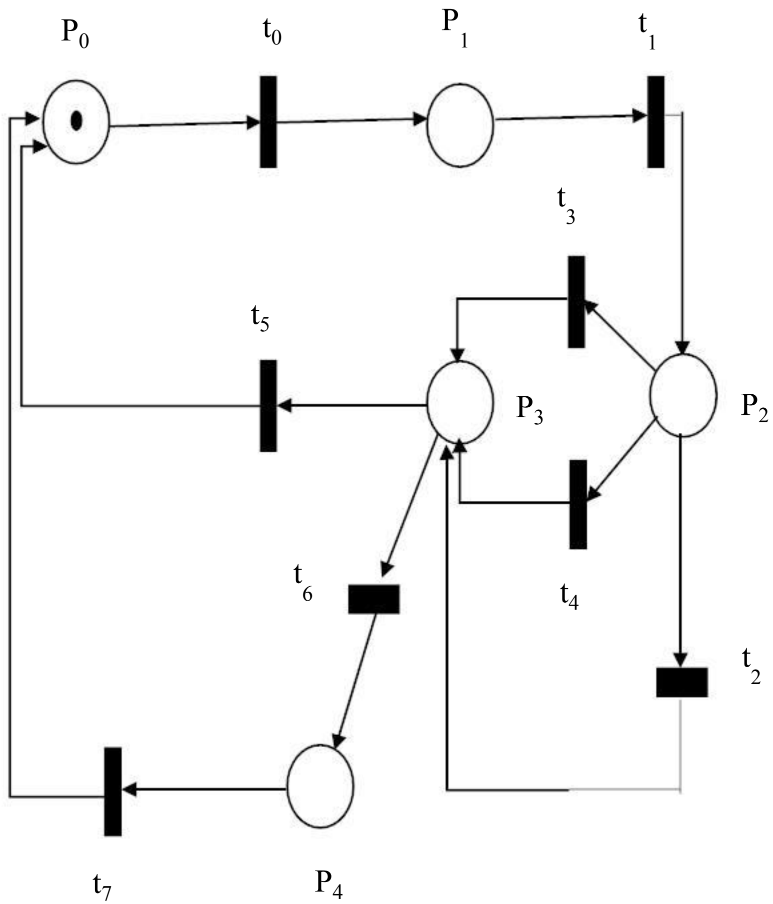
A Case Study: Digital Feed Water Control System



Computer-controller-actuated devices interaction in DFWCS



Generate model

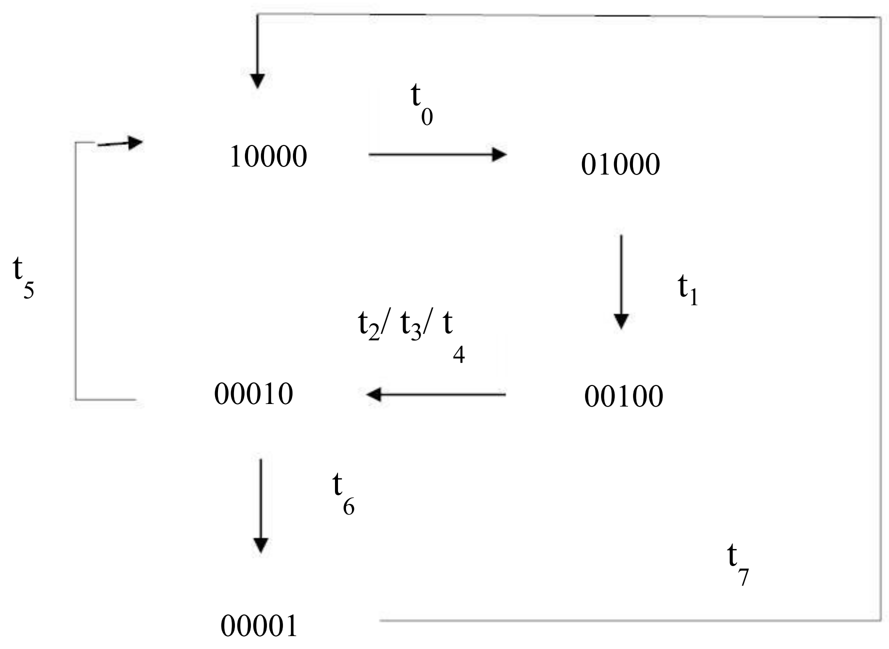


Places	Description
P_0	FWS is in ready state
P_1	Computer (MC or BC) receive deviated value
P_2	Controller receive error signal(deviated value)
P_3	Actuator operates(according to the input)
P_4	Actuator in stuck state

Transitions	Description
t_0	SG level deviated from normal limit
t_1	Error signal(deviated value) send to the controller
t_2	Trigger normal open to actuator
t_3	Controller recognized failure of computer and send previous correct (freeze)value to the actuator device
t_4	Controller does not recognized failure of MC/BC and send false value (high /low/ arbitrary) to the actuator device
t_5	System reset
t_6	Actuator stuck
T_7	Repair

Behavioral and Structural analysis

Behavioral properties: Behavioral properties depend on the initial marking of the net. In this phase the behavioral properties for the created PN is validated with respect to the three basic properties: **reachability, boundedness and liveness from the reachability graph.**



Structure properties are depending on the topological structure of the net, namely **p-invariant and siphons.** P-invariant is corresponds to a set of places whose weighted token count is a constant for any reachable marking.

P-invariant

- Calculate incidence matrix

$$A = D^{-} - D^{+}$$

$$D^{-} = \begin{bmatrix} & t_0 & t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 \\ p_0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ p_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_3 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ p_4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$D^{+} = \begin{bmatrix} & t_0 & t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 \\ p_0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_2 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ p_3 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ p_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

P-invariant

- Calculate incidence matrix

$$A = D^{-} - D^{+}$$

$$A = \begin{bmatrix} & t_0 & t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 \\ p_0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ p_1 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_2 & 0 & 1 & -1 & -1 & -1 & 0 & 0 & 0 \\ p_3 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & 0 \\ p_4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

P-invariant calculation

The order of places in the matrix is row based $P = \{P_0, P_1, P_2, P_3, P_4\}$ and the order of transitions is column based $T = \{t_0, t_1, t_2, t_3, t_4, t_5, t_6, t_7\}$.

o

$$\begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

2 Step

$$\left[\begin{array}{cccccccc|ccccc} -1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

3rd Step

$$\left[\begin{array}{cccccccc|ccccc} 0 & -1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

4th step

$$\left[\begin{array}{cccccccc|ccccc} 0 & 0 & -1 & -1 & -1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

5th step

$$\left[\begin{array}{cccccccc|ccccc} 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

6th step

$$[0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0] \quad 1 \quad 1 \quad 1 \quad 1 \quad 1$$

P-invariant is $x = [1\ 1\ 1\ 1\ 1]$

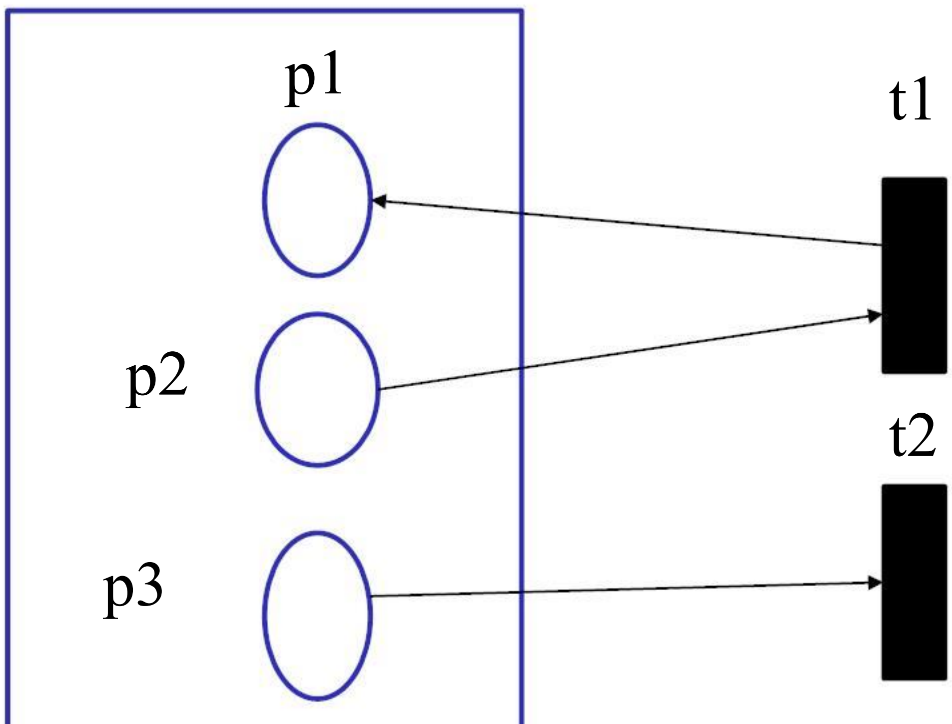
T-invariant

- T-invariant
- $$\left[\begin{array}{ccccc|cccccccc} -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$
- 2step $$\left[\begin{array}{ccccc|cccccccc} 0 & 1 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$
- 3^{rd} step $$\left[\begin{array}{ccccc|cccccccc} 0 & 0 & 1 & -1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{array}\right]$$
- 4^{th} step $$\left[\begin{array}{ccccc|cccccccc} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right]$$
- 5^{th} step $$\left[\begin{array}{ccccc|cccccccc} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right]$$

T-invariants $y1$ =[11100100], y2=[11010011], y3= [11100011], $y4 =$ [11010100], $y5 =$ [11001100]

SIPHON

The siphon is used for the structural analysis of PN. A non-empty sub-set of places $S \subseteq P$ is a called siphon if $^{\cdot}S \subseteq S^{\cdot}$ i.e, a set of transition having an output place in S has an input place in S. A siphon is called to be minimal if it does not contain any other siphon as a proper subset. A minimal siphon that does not comprise the support of any P-invariant is called a strict minimal siphon. A siphon S which is controlled by P-invariants can never be emptied. It is called to be invariant-controlled by P-invariant I under M_0 if $I^T \bullet M_0 > 0$ and $||I||^+ \subseteq S$. The emptiness of minimal siphon leads to the deadlock of the net.



$^{\cdot}S \subseteq S^{\cdot}$

$^{\cdot}S = \{t1\}, S^{\cdot} = \{t1, t2\}$

Conclusions

- Software security is a key part in software quality
- Software security improvement is hard
- There are no generic models
- Measurement is very important for finding the correct model
- Using PN for security analysis

Bibliography

1. Lalit Singh, Hitesh Rajput, “Dependability analysis of Safety Critical Real-Time Systems by using Petri nets” in IEEE Transactions on Control Systems Technology, vol.PP, no.99, pp.1-12 doi: 10.1109/TCST.2017.2669147.
2. Lalit Singh, Gopika Vinod, A.K. Tripathi, "Design verification of Instrumentation and Control systems of Nuclear Power Plants," in IEEE Transactions on Nuclear Science, Vol.61(2), March 2014, pp.921-930.
3. Vinay Kumar, Lalit Singh, Pooja Singh, K.V. Singh, A.K. Maurya, A.K. Tripathi, “Parameter Estimation for Quantitative Dependability Analysis of Safety-Critical and Control Systems of NPP,” in IEEE Transactions on Nuclear Science, (Accepted for Publication).
4. Lalit Singh, Gopika Vinod, A.K. Tripathi, “Early Prediction of Software Reliability: A Case Study with a Nuclear Power Plant System”, in IEEE Computer, Vol.49 (1), Jan 2016, pp.52-58.
5. Vinay Kumar, Lalit Singh, A.K. Tripathi, Pooja Singh “Safety Analysis of safety critical systems using state space models”, in IEEE Software, Vol. 34(4), July 2017, pp.38-47.

Bibliography (cont.)

6. Raj Kamal, Lalit Singh, Babita Pandey, “A Review of Security Analysis for Electronic Power Systems,” in IEEE Consumer Electronics Magazine, (under production).
7. Lalit Singh, Hitesh Rajput, “Ensuring Safety in Design of Safety Critical Computer Based Systems,” in Annals of Nuclear Energy, Elsevier Vol.92, June 2016, pp.289-294.
8. Raj Kamal, Lalit Singh, Babita Pandey, “Dependability Analysis of Safety Critical Systems: Issues and Challenges,” in Annals of Nuclear Energy, Elsevier, Vol.105, July 2017, pp.133-143 (Accepted for Publication).
9. Vinay Kumar, Lalit Singh, A.K. Tripathi, “Reliability Analysis of safety-critical systems: A state-of-the-art review”, in IET Software, 2017, DOI: 10.1049/iet-sen.2017.0053 IET Digital Library, http://digital-library.theiet.org/content/journals/10.1049/iet-sen.2017.0053.
10. Pramod Kumar, Lalit Singh, Chiranjeev Kumar, “Suitability Analysis of Software Reliability Models for its Applicability on NPP Systems,” in Quality and Reliability Engineering International, (Accepted for Publication).

Bibliography (cont.)

11. Pramod Kumar, Lalit Singh, Chiranjeev Kumar, "An Optimized Technique for Reliability Analysis of Safety Critical Systems: A case study of Nuclear Power Plant," in Quality and Reliability Engineering International, (Accepted for Publication).
12. Raj Kamal, Lalit Singh, Babita Pandey, "Security Analysis of Safety Critical and Control Systems: A Case Study of Nuclear Power Plant System," in Nuclear Technology, American Nuclear Society, Vol.197(3), Feb 2017, pp.296-307.
13. Lalit Singh, Gopika Vinod, A.K. Tripathi, "Reliability Prediction through System Modeling", in ACM SIGSOFT Soft. Engineering Notes, vol. 38, Nov, 2013, pp.1-10.
14. Lalit Singh, Gopika Vinod, A.K. Tripathi, "Impact of Change in Component Reliabilities on System Reliability Estimation," in ACM SIGSOFT Software Engineering Notes, June, 2014, pp.1-6.

Thank You!

lalit.singh.poo(at)gmail.com