*Dedicated to my Family and Guruji…*

# Certificate

This is to certify that this thesis entitled "Some Observations on Modeling of Cyber-Physical Systems for Security" submitted by Dipty Tripathi (Roll No.: 17071001) for the award of the degree of doctor of philosophy to the Indian Institute of Technology (Banaras Hindu University), Varanasi, is a record of bona fide research works carried out by her under my direct supervision and guidance, and it has not been submitted elsewhere for a degree. It is further certified that the student has fulfilled all the requirements of Comprehensive Examination, Candidacy, and SOTA for the award of Ph.D. Degree.

Signature of Co-Supervisor
Amrita Chaturvedi
Assistant Professor
Computer Science and Engineering
Indian Institute of Technology (BHU)
Varanasi - 221005, India

Signature of Co-Supervisor
Lalit Kumar Singh
Scientific Officer/F
Nuclear Power Corporation of India Limited,
Department of Atomic Energy, India

Signature of Supervisor
Anil Kumar Tripathi
Professor
Computer Science and Engineering
Indian Institute of Technology (BHU)
Varanasi - 221005, India

# Declaration

I hereby declare that the work embodied in this thesis is my own bonafide work and carried out by me under the joint supervision of **Prof. Anil Kumar Tripathi, Dr. Amrita Chaturvedi, and Dr. Lalit Kumar Singh** from **July 2017** to **March 2022**, at the Computer Science and Engineering Department, Indian Institute of Technology (BHU), Varanasi. The matter embodied in this thesis has not been submitted for the award of any other degree/diploma. I declare that I have faithfully acknowledged and given credits to the research workers wherever their works have been cited in my work in this thesis. I further declare that I have not willfully copied any other's work, paragraphs, text, data, results, etc., reported in journals, books, magazines, reports dissertations, thesis, etc., or available at websites and have not included them in this thesis and have not cited as my own work.

Date:

Place: Varanasi

**Signature of Student**

**(Dipty Tripathi)**

# Certificate by the Supervisor

It is certified that the above statement made by the student is correct to the best of my/our knowledge.

**Signature of Supervisor**

**(Anil Kumar Tripathi)**

**Signature of Head of Department**

# Copyright Transfer Certificate

Title of the Thesis: **Some Observations on Modeling of Cyber-Physical Systems for Security**
Name of Student: **Dipty Tripathi**

# Copyright Transfer

The undersigned hereby assigns to the Indian Institute of Technology (Banaras Hindu University), Varanasi, all rights under copyright that may exist in and for the above thesis submitted for the award of the Doctor of Philosophy.

Date:
Place: Varanasi

**Signature of Student**
**(Dipty Tripathi)**

Note: However, the author may reproduce or authorize others to reproduce material extracted verbatim from the thesis or derivative of the thesis for author's personal use provided that the source and the Institute's copyright notice are indicated.

# Acknowledgments

*"No one who achieves success does so without acknowledging the help of others. The wise and confident acknowledge this help with gratitude." -Alfred North Whitehead*

Though only my name appears on the cover of this thesis, many people have contributed to produce it. I sincerely thank all the people who helped me to make this thesis possible.

Foremost, I would like to express my sincere gratitude to my supervisor, Prof. Anil Kumar Tripathi, co-supervisors Dr. Amrita Chaturvedi, and Dr. Lalit Kumar Singh for giving me the opportunity and continuous support to undertake my Ph.D. The availability of Dr. Lalit Kumar Singh as a co-supervisor was immensely useful in developing a clear understanding of nuclear power plants as a case study of cyber-physical systems. I am deeply grateful for their invaluable guidance, advice, mental and academic support, and motivation throughout my candidature. Their guidance helped me in all the time of research, conducting experiments, and writing of this thesis.
I would like to express my gratitude to the Research Program Evaluation Committee members Dr. Lakshmanan Kailasam, and Dr. Ashok Ji Gupta, for their insightful comments, encouragement, and suggestions, which helped me improve my research from various perspectives. I would like to convey my sincere gratitude to the other faculty members of the Department of Computer Science and Engineering, Prof. K.K Shukla, Prof. Rajeev Shrivastava, Dr. R.S Singh, Dr. Bhaskar Biswas, Dr. Sukomal Pal, Dr. Pratik Chattopadhyay, Dr. H.P Gupta, Dr. Ruchir Gupta, Dr. Amrita Chaturvedi, Dr. R.N. Chaudhary, Dr. A.K Singh, Dr. Tanima Dutta, Dr. Prasenjit Chanak and Dr. Vinayak Shrivastava for their guidance and support throughout this tenure.

I want to thank my seniors and colleagues Dr. Ashish Kumar Maurya, Dr. Vinay Kumar, Dr. Sushant Kumar Pandey, Mr. Amit Biswas, Ms. Manisha Singh, Ms. Shruti Bajpai, Ms. Pragya Shukla, Ms. Sneha Mishra, Ms. Deeksha Gupta, Dr. Pratishta Verma, Mr. Ankit Jaiswal, and Ms. Naina Yadav for their motivation and valuable comments. I also extend my thanks to other colleagues, members of our department of computer science and engineering department, and different departmental colleagues. This thesis would not have been possible without their invaluable remarks and persistent help. I extend special thanks to the non-teaching and technical staff in the department, particularly Mr. Ravi Kumar Bharti, Mr. Shubham Pandey, Mr. Prakhar Kumar, Mr. Akhilesh Kumar Pal,

Mr. Biplab Biswas.
Finally, I would like to thank my family for their love, encouragement, and moral and emotional support to achieve this great goal. It would not have been possible without their help and support. To them, I am eternally grateful.

Dipty Tripathi

# Preface

The physical infrastructure, equipment, and facilities are gradually instrumented, controlled, automated, and administered through computerization and possibly internetworking. Such an arrangement is known in the literature as a Cyber-Physical System (CPS). The emerging CPS may range from small-scale industries to large-scale connected systems of diverse areas such as transportation, avionics, defense, entertainment, industrial control system, safety-critical systems, healthcare, *etc.* The cyber components monitor and control the real-world physical devices and infrastructures to improve the quality of services, including reliability and resource utilization.

However, the automation and connectivity of all the networked computing devices increase the security risks and leverage the opportunity to perform successful attacks to compromise system safety with catastrophic effects on human lives and the environment. The attackers compromise the system by exploiting existing vulnerabilities that arise due to inappropriate policies, facilitation to external entities, inefficient and inaccurate protection mechanisms and procedures. Several powerful attacks have been launched on critical infrastructures in recent years, resulting in substantial financial losses, productivity losses, and physical injuries. Protecting Industrial control systems (ICS) from cyber attacks is critical to a country's economic development and social stability. This is an emergent need that security is also considered in the modeling of CPS in general and safety-critical systems in particular. Through a detailed literature survey of existing modeling, analysis, and system organization methods, we find some significant issues and challenges. During development, functionality often takes priority over security. Security measures were implemented late as an add-on resulting in brittle designs that lack proper integration. Further, several techniques are proposed to perform the security analysis in early phases of the system development life cycle. However, most of these present the qualitative assessment rather than quantitative assessment.

This thesis presents the security modeling and arrangement approaches to overcome these research gaps in the early phases. The first chapter proposes a design-time methodology to map and analyze the system security using Stochastic Petri Nets (SPN) and their fundamental properties. The presented theoretical framework exploits the power of SPN to model the stochastic nature of the system in the presence of external threats. It provides the mathematical support for structural and behavioral analysis to validate the effect of responsive mitigations against security vulnerabilities qualitatively and quantitatively. The effectiveness of the proposed methodology is shown through a case study of Nuclear Power Plant (NPP).

Deploying preventive or responsive measures alone may not be enough to detect, prevent and respond to intrusion attempts and subsequent sophisticated attacks. In the second chapter, we have extended the earlier work, where multiple intrusion prevention and response techniques are applied in place of responsive measures only, and their combined effect on system security and availability are analyzed quantitatively using Generalized Stochastic Petri Nets (GSPN). As SPN suffers from a state explosion problem, GSPN is used to deal with the problem. Moreover, the proposed model helps to prioritize the available security measures.

As CPSs are mostly distributed systems, it is interesting to consider a possible approach for the separation of functionality and security concerns for CPS that are usually organized and created in a distributed manner. In the third chapter, we propose a distributed multi-tier architectural model of CPS and its management as per aspect orientation and leader election as observable in distributed computing systems to improve the CPS performance, security, and functionality management.

# List of Publications

1. **Dipty Tripathi**, Lalit Kumar Singh, Anil Kumar Tripathi and Amrita Chaturvedi, "Model based security verification of Cyber-Physical System based on Petrinet: A case study of Nuclear power plant", Annals of Nuclear Energy, 2021, 159, pp.108306. DOI: https://doi.org/10.1016/j.anucene.2021.108306, (SCI indexed, Publisher: Elsevier, Impact Factor: 1.77)

2. **Dipty Tripathi**, Anil Kumar Tripathi, Lalit Kumar Singh and Amrita Chaturvedi, "Towards analyzing the impact of intrusion prevention and response on cyber-physical system availability: A case study of NPP", Annals of Nuclear Energy, 2021, pp.108863. DOI: https://doi.org/10.1016/j.anucene.2021.108863, (SCI indexed, Publisher: Elsevier, Impact Factor: 1.77)

3. **Dipty Tripathi**, Amit Biswas, Anil Kumar Tripathi, Lalit Kumar Singh and Amrita Chaturvedi, "An Integrated Approach of Designing Functionality with Security for Distributed Cyber-Physical System", The Journal of Supercomputing, (SCI indexed, Publisher: Springer, Impact Factor: 2.474) (Accepted)

4. **Dipty Tripathi**, Ashish Kumar Maurya, Anil Kumar Tripathi, and Amrita Chaturvedi "A Study of Security Modeling Techniques for Smart Systems", 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), India, February 14-16, 2019, pp. 87-92 (SCOPUS indexed, Publisher: IEEE)

# Contents

# List of Figures

# List of Tables

# Abbreviations

| | |
|---|---|
| **AS** | **A**ttack **S**cenarios |
| **BC** | **B**ackup **C**omputer |
| **BN** | **B**ayesian **N**etworks |
| **BFV** | **B**ypass **F**eedwater **V**alve |
| **CC** | **C**ontrol **C**enter |
| **CPS** | **C**yber **P**hysical **S**ystem |
| **DFWCS** | **D**igital **F**eed **W**ater **C**ontrol **S**ystem |
| **DoS** | **D**enial **o**f **S**ervice |
| **EMC** | **E**mbedded **M**arkov **C**hain |
| **FP** | **F**eedwater **P**ump |
| **FM** | **F**unctional **M**odel |
| **FMDT** | **F**unctional **M**odel under **D**oS **T**hreat |
| **FMIT** | **F**unctional **M**odel under **I**ntegrity **T**hreat |
| **FMM** | **F**unctional **M**itigation **M**odel |
| **FNR** | **F**alse **N**egative **R**ate |
| **FPR** | **F**alse **P**ositive **R**ate |
| **GSPN** | **G**eneralized **S**tochastic **P**etri **N**et |
| **ICS-CERT** | **I**ndustrial **C**ontrol **S**ystems **C**omputer **E**mergency **R**esponse **T**eam |
| **ICT** | **I**nformation and **C**ommunications **T**echnology |
| **IDS** | **I**ntrusion **D**etection **S**ystem |
| **IDRL** | **I**ntrusion **D**etection and **R**esponse textbfLayer |
| **IoT** | **I**nternet **o**f **T**hings |

| | |
|---|---|
| **I&C** | **I**nstrumentation and **C**ontrol |
| **MBSE** | **M**odel **B**ased **S**ystem **E**ngineering |
| **MC** | **M**ain **C**omputer |
| **MFV** | **M**ain **F**eedwater **V**alve |
| **MTTD** | **M**ean **T**ime **T**o **D**isrupt |
| **NIDRS** | **N**etwork **I**ntrusion **D**etection and **R**esponse **S**ystem |
| **NPP** | **N**uclear **P**ower **P**lant |
| **PDI** | **P**ressure **D**ifferential **I**ndicator |
| **PN** | **P**etri **N**et |
| **RCP** | **R**eactor **C**oolent **P**ump |
| **RG** | **R**eachability **G**raph |
| **RQ** | **R**esearch **Q**uestion |
| **REMC** | **R**educed **E**mbedded **M**arkov **C**hain |
| **RCICS** | **R**eactor **C**ore **I**solation **C**ooling **S**ystem |
| **SCADA** | **S**upervisory **C**ontrol and **C**yber **P**hysical **S**ystem |
| **SC-CPS** | **S**afety **C**ritical **D**ata **A**cquisition **S**ystem |
| **SDN** | **S**oftware **D**efined **N**etworking |
| **SG** | **S**team **D**enerators |
| **SPN** | **S**tochastic **P**etri **N**et |
| **SSP** | **S**teady **S**tate **P**robability |
| **STRIDE** | **S**poofing **T**ampering **R**epudiation **I**nformation disclosure **D**enial of service **E**levation of privilege |
| **UML** | **U**nified **M**odeling **L**anguage |

# Symbols

| | |
|---|---|
| $A$ | set of attributes |
| $AR$ | set of actuators |
| $as$ | attack surface |
| $atk_i$ | attack $i$ |
| $av$ | attack vector |
| $Avl$ | availability |
| $C$ | set of controllers |
| $c\_ack\_id$ | *ack* message creator Id |
| $c_j$ | $j^{th}$ cluster |
| $c_x(t)$ | output of controller $x$ at time $t$ |
| $CN$ | set of computing nodes |
| $D$ | set of threat mitigations |
| $d_i$ | firing delay of transition $t_i$ |
| $d_{max}$ | is the maximum diameter of the clusters |
| $D_p$ | preventive defense sequence |
| $D_r$ | responsive defense measures |
| $Dia$ | diameter of graph $G$ |
| $DSC$ | decision support cluster |
| $eini\_id$ | election initiator Id |
| $f_{Dj}$ | failure probability of each defence measure $Dj$ against $atk_i$ |
| $failed\_leader\_id$ | failed leader id |
| $FC$ | set of monitoring and field controller nodes |

| | |
|---|---|
| $flc\_list_i$ | a node $i$ stores the list of functionality leader capable nodes in it |
| $fun\_leader_i$ | functionality leader Id stored by a node $i$ |
| $FN$ | set of functionality nodes |
| $FS$ | set of failed states |
| $G = (CN, L)$ | Graph with computing nodes $CN$ and set of links $L$ |
| $L$ | total possible loss due to cyber attack |
| $l\_id$ | newly elected leader Id |
| $l\_child_i$ | list of child nodes of a node $i$ |
| $leader_i$ | a node $i$ stores the system leader Id in it |
| $M_0$ | initial marking |
| $M(P)$ | set of markings |
| $P$ | set of places |
| $parent_i$ | parent node of a node $i$ |
| $p_i$ | frequency of successful attack $a_i$ |
| $Q$ | transition rate matrix |
| $R$ | radius of graph $G$ |
| $RI$ | cyber risk impact |
| $r\_list$ | a 2D list with two fields. First field contains node Id and second field contains rank of a node |
| $S$ | set of sensors |
| $S_{Dj}$ | strength of defence measure $Dj$ |
| $s\_em\_id$ | sender of the election message |
| $sd_{ij}$ | synchronic distance between transitions $t_i$ and $t_j$ |
| $sec\_leader_i$ | security leader Id stored by a node $i$ |
| $s_{ta}$ | targeted system attribute or functionality |
| $s_x(t)$ | measurement of sensor $x$ at time $t$ |
| $slc\_list_i$ | a node $i$ stores the list of security leader capable nodes in it |
| $sm_x(t)$ | operational state of system at time $t$ |
| $s_\gamma(v, t)$ | threat strength |
| $SN$ | set of security nodes |

| | |
|---|---|
| $T$ | set of transitions |
| $t\_list$ | list of transient leader |
| $ta$ | target security attribute |
| $Tf$ | set of functionality tasks |
| $toe$ | type of election, if the election is initiate to elect the functionality leader then $toe = 1$, if the election is initiate to elect security leader then $toe = 0$ |
| $tol$ | type of leader, $tol$=1 functionality leader, $tol$=0 security leader |
| $ton_i$ | type of node, if node $i$ is a functionality node then $ton_i = 1$, if node $i$ is a security node then $ton_i = 0$ |
| $Ts$ | set of security tasks |
| $v$ | existing vulnerability |
| $\alpha'$ | deviation in intended functionality |
| $\beta_\alpha(t)$ | security goals at time $t$ |
| $\delta t$ | threat duration |
| $\gamma$ | an active threat |
| $\lambda_{ij}$ | transition rate of state $i$ to state $j$ |
| $\omega_i(t)$ | attack impact per unit time |
| $\pi$ | probability distribution |
| $\pi_i$ | the steady-state probability of being in state $M_i$ |
| $p\{t_{k\gamma}\|M_j\}$ | probability of firing a malicious transition $t_{k\gamma}$ |
| $\sigma(t)$ | disturbance factor for sensor values |