Contents

Certificate **ii**

Acknowledgments **v**

Preface **vii**

List of Publications **ix**

Contents **x**

List of Figures **xiii**

List of Tables **xv**

Abbreviations **xvi**

Symbols **xviii**

1 Introduction **1**
- 1.1 Research Goal and Problem Statement 6
- 1.2 Motivation 7
- 1.3 Contribution 10
- 1.4 Scope of Research 11
- 1.5 Thesis Outline 11

2 Preliminaries and Literature Review **14**
- 2.1 Preliminaries 14
  - 2.1.1 System Requirements 14
  - 2.1.2 Security Related Concepts 15
  - 2.1.3 Model Based System Engineering (MBSE) 16
  - 2.1.4 Threat modeling 17
    - 2.1.4.1 Markov Model 17

2.1.4.2 Petri Net 22
2.1.4.3 Stochastic Petri Net 23
2.1.4.4 GSPN 24
2.2 Literature Review 26
2.2.1 Modeling and Analysis Methods for CPS Security 26
2.2.1.1 Organization and Management of Distributed Secure CPS 32

3 Model based Security Verification of Cyber-Physical System Based on Petrinet: A Case Study of Nuclear Power Plant 38
3.1 Formal Description of CPS 39
3.2 Proposed Methodology 40
3.2.1 Requirement Analysis 40
3.2.2 Functional Model Generation 40
3.2.3 Threat Model Generation 40
3.2.4 Mitigation Model Generation 42
3.2.5 Security Validation 42
3.2.5.1 Qualitative Analysis 43
3.2.5.2 Quantitative Analysis 45
3.3 Case study 46
3.3.1 Requirement identification and analysis: 47
3.3.2 Functional Model Generation 49
3.3.3 Threat Model Generation 52
3.3.4 Mitigation Model Generation 55
3.3.5 Security Metrics Validation 56
3.3.5.1 Qualitative Analysis 56
3.3.5.2 Quantitative Analysis 58
3.4 Discussion 61
3.5 Summary 61

4 Towards Analyzing the Impact of Intrusion Prevention and Response on Cyber-Physical System Availability: A case study of NPP 62
4.1 A roadmap to research solution 63
4.1.1 Intrusion-Disruption Model 64
4.1.2 Security Measures 66
4.2 Formal Specification of Applied Security Measures 67
4.2.1 Preventive Measures 67
4.2.1.1 Perimeter Protection Layers 68
4.2.1.2 Authentication Layer 69
4.2.1.3 Access Control Layer 70
4.2.2 Responsive Measures 71
4.2.2.1 Intrusion Detection and Response Layer 71

4.3 Proof of Concept . . . 72
4.3.1 DFWCS Security Modeling . . . 74
4.3.2 Quantitative Evaluation . . . 78
4.3.3 Comparative Evaluation . . . 92
4.4 Summary . . . 92

5 An Integrated Approach to Design Functionality with Security for Cyber-Physical Systems 93
5.1 Attack scenarios . . . 95
5.2 The proposed architectural model . . . 96
5.2.1 Formal description . . . 96
5.2.2 Layers responsibilities . . . 96
5.2.3 Role of functionality and security leaders . . . 99
5.2.4 The proposed leader election algorithm . . . 101
5.2.4.1 Message type . . . 103
5.2.4.2 Leader election method . . . 103
5.2.4.3 Complexity analysis . . . 107
5.2.5 Resilience against cyber attacks . . . 109
5.3 Performance evaluation of the proposed architectural model . . . 110
5.3.1 Case study . . . 110
5.3.2 Performance evaluation . . . 112
5.4 Summary . . . 118

6 Conclusion and Future Direction 120
6.1 Conclusion . . . 120
6.2 Future Research Directions . . . 123

Bibliography 125

List of Figures

1.1 Holistic view of a CPS 2
1.2 Major responsibilities of CPS architecture layers [78] 2
1.3 Thesis Structure 12

2.1 Security ontology 15
2.2 Simplex system model example 21
2.3 Elementary SPN models 24
2.4 Transformation of SPN model 24
2.5 GSPN model and its reachability graph 25

3.1 Proposed security modeling and analysis methodology 40
3.2 Architectural view of feed water controller [4] 47
3.3 Functional model of DFWCS (FMA) 48
3.4 Integrity attack on sensor data (FMIT) 48
3.5 DoS attack on communication channel (FMDT) 48
3.6 Functional model of DFWCS with security measure (FMM) 49
3.7 Reachability graph of FMA 49
3.8 Reachability graph of FMIT 50
3.9 Reachability graph of FMDT 50
3.10 Reachability Graph of FMM 51
3.11 Markov chain corresponding to FMM reachability graph 51
3.12 Transition rate matrix corresponding to FMM 52
3.13 Effect of readjustment of mitigation strategy 53

4.1 General underline framework of CPS security 68
4.2 Applied preventive and responsive defense measures on DFWCS . . . 73
4.3 GSPN model of DFWCS functionality 74
4.4 GSPN model of DFWCS under attack and defense 74
4.5 Reachability graph of FIGURE 4.4 77
4.6 EMC generated from reachability graph of FIGURE 4.4 77
4.7 Integrity Attack (IA) on level sensor 79
4.8 DoS Attack on level sensor 80
4.9 Impact of adjusting defense strength on security evaluation metrics . 84

5.1 Layered representation of CPS architecture 97

5.2 Clustered view of the proposed distributed CPS architectural model . 97
5.3 Clustered view of cyber layer and decision support layer of the proposed distributed CPS architectural model with functionality and security leaders 97
5.4 Cluster arrangement of a distributed hospital network with functionality and security leaders 111
5.5 Comparison of the proposed system management manner with other possible system management manners based on the number of exchanged messages to complete the task. 114
5.6 Comparison of the proposed system management manner with other possible system management manners based on the time required to complete the task. 115
5.7 Comparison of the proposed system management manner with the distributed manner with a single leader based on the average response time of the task. 116
5.8 Comparison of the proposed system management manner with the distributed manner with a single leader based on the success ratio of real time tasks completion within deadline 117
5.9 Quantile-Quantile plot (Q-Q plot) on the average response time of the tasks getting through the proposed system management manner. 117
5.10 Quantile-Quantile plot (Q-Q plot) on the completion ratio of real-time tasks getting through the proposed system management manner. . . . 118

List of Tables

1.1 Cyber Attacks on cyber physical systems 8

2.1 Related work 31
2.2 Comparative analysis with existing works 36

3.1 Operational mode of DFWCS 47
3.2 Place Description of FMA 52
3.3 Transition Description of FMA 52
3.4 Security metrics evaluation table of FMA, FMIT, FMDT 57
3.5 Effect of readjustment of mitigation strength on steady-state probabilities λ_9 60

4.1 IDRS responses 72
4.2 Place Description of Figure 4.3 73
4.3 Transition Description of Figure 4.3 73
4.4 Place Description of Figure 4.4 75
4.5 Transition Description of Figure 4.4 76
4.6 Impact of attack 78
4.7 Effect of readjustment of mitigation strength on performance metrics 85
4.8 Effect of readjustment of mitigation strength on performance metrics 86
4.9 Comparative study 87

5.1 Details of the networks considered for the experiments 112