NOVA SCHOOL OF SCIENCE & TECHNOLOGY

DEPARTMENT OF
ELECTRICAL AND COMPUTER ENGINEERING

EVALUATING RESILIENCE OF CYBER-PHYSICAL-SOCIAL SYSTEMS

USING GRAPHICAL SECURITY MODELS AND TIMED COLOURED PETRI NETS

SHABNAM PASANDIDEH

Master in Information Technology Management

DOCTORATE IN ELECTRICAL AND COMPUTER ENGINEERING

NOVA University Lisbon
September, 2022

DEPARTMENT OF
ELECTRICAL AND COMPUTER ENGINEERING

EVALUATING RESILIENCE OF CYBER-PHYSICAL-SOCIAL SYSTEMS

USING GRAPHICAL SECURITY MODELS AND TIMED COLOURED PETRI NETS

SHABNAM PASANDIDEH

Master in Information Technology Management

Adviser: Luís Filipe dos Santos Gomes
Associate Professor with Habilitation, Universidade Nova de Lisboa

Co-adviser: Pedro Miguel Ribeiro Pereira
Assistant Professor, Universidade Nova de Lisboan

Examination Committee:

Chair: João Carlos da Palma Goes
Full Professor, Universidade Nova de Lisboa

Rapporteurs: Alberto Jorge Lebre Cardoso
Associate Professor, Universidade de Coimbra
Paulo Jorge Pinto Leitão
Full Professor, Instituto Politécnico de Bragança

Adviser: Luís Filipe dos Santos Gomes
Associated Professor with Habilitation, Universidade Nova de Lisboa

Members: João Paulo Mestre Pinheiro Ramos e Barros
Full Professor, Instituto Politécnico de Beja
João Carlos da Palma Goes
Full Professor, Universidade Nova de Lisboa
João Francisco Alves Martins
Associate Professor with Habilitation, Universidade Nova de Lisboa

DOCTORATE IN ELECTRICAL AND COMPUTER ENGINEERING

NOVA University Lisbon
September, 2022

Evaluating Resilience of Cyber-Physical-Social Systems

Acknowledgements

This Ph.D. accomplishment, which was initially meant to be a personal milestone, would not have been feasible without the help and dedication of a large number of individuals, some or all of whose names may not be stated here. I have the utmost respect for the contributions that they make. Obtaining this Ph.D. was not only a difficult but also a rewarding accomplishment that served as a turning point in my life.

First and foremost, I would like to express my profound gratitude to Professor Luis Gomes, my adviser, for his guidance, understanding, and support throughout this protracted process. I count myself quite fortunate to have been able to finish the dissertation with his critical remarks and insightful recommendations. I will never forget his thoughtfulness, words of support, nice manner, and pleasant disposition, all of which helped me to get through difficult times while working on my Ph.D.

I am also deeply grateful to my co-supervisor, Professor Pedro Pereira, for providing insightful criticism and suggestions during the process of developing this dissertation. Because of his intelligence and observations, this journey was able to advance and become more delightful. Also, I want to thank him for their unwavering support and for believing in me to keep going and conduct the dissertation when I needed it the most.

I would like to extend my sincere thanks to Professors João Martins and Joao Paulo Barros for all the support they have provided as well as their insightful and helpful suggestions. I would like to express my appreciation to FCT-NOVA and the Center for Technology and Systems (CTS) for giving me the opportunity to further my education with their respective facilities and resources available. We would like to express our gratitude to the Department of Electrical and Computer Engineering and the UNINOVA Research Institute, both of which have contributed to the success of this project by making financial support from their organizations.

I would like to offer my heartfelt thanks to my family, specifically my parents, Ebrahim Pasandideh and Shahnaz Samadi Alinia, as well as to my sister, Samira Pasandideh, for their unwavering support and encouragement throughout all of the steps that I have taken to pursue my goals. I can't express how much I value all of your hard work and how much I appreciate everything you've done for me.

Finally, I am deeply grateful to Armando Martires, who by his calmness and love was with me on this path and did his best to me in difficult moments to continue and work harder on making my dreams true.

Abstract

Nowadays, protecting the network is not the only security concern. Still, in cyber security, websites and servers are becoming more popular as targets due to the ease with which they can be accessed when compared to communication networks. Another threat in cyber physical social systems with human interactions is that they can be attacked and manipulated not only by technical hacking through networks, but also by manipulating people and stealing users' credentials. Therefore, systems should be evaluated beyond cyber security, which means measuring their resilience as a piece of evidence that a system works properly under cyber-attacks or incidents. In that way, cyber resilience is increasingly discussed and described as the capacity of a system to maintain state awareness for detecting cyber-attacks. All the tasks for making a system resilient should proactively maintain a safe level of operational normalcy through rapid system reconfiguration to detect attacks that would impact system performance. In this work, we broadly studied a new paradigm of cyber physical social systems and defined a uniform definition of it. To overcome the complexity of evaluating cyber resilience, especially in these inhomogeneous systems, we proposed a framework including applying Attack Tree refinements and Hierarchical Timed Coloured Petri Nets to model intruder and defender behaviors and evaluate the impact of each action on the behavior and performance of the system.

Keywords: Cyber Physical Social Systems, Cyber Resilience, Cyber Security, Coloured Petri Nets, Evaluate Cyber Resilience, Cyber Physical Social Systems Taxonomy, Cyber Resilience Taxonomy.

Resumo

Hoje em dia, proteger a rede não é a única preocupação de segurança. Ainda assim, na segurança cibernética, sites e servidores estão se tornando mais populares como alvos devido à facilidade com que podem ser acessados quando comparados às redes de comunicação. Outra ameaça em sistemas sociais ciberfisicos com interações humanas é que eles podem ser atacados e manipulados não apenas por hackers técnicos através de redes, mas também pela manipulação de pessoas e roubo de credenciais de utilizadores. Portanto, os sistemas devem ser avaliados para além da segurança cibernética, o que significa medir sua resiliência como uma evidência de que um sistema funciona adequadamente sob ataques ou incidentes cibernéticos. Dessa forma, a resiliência cibernética é cada vez mais discutida e descrita como a capacidade de um sistema manter a consciência do estado para detectar ataques cibernéticos. Todas as tarefas para tornar um sistema resiliente devem manter proativamente um nível seguro de normalidade operacional por meio da reconfiguração rápida do sistema para detectar ataques que afetariam o desempenho do sistema. Neste trabalho, um novo paradigma de sistemas sociais ciberfisicos é amplamente estudado e uma definição uniforme é proposta. Para superar a complexidade de avaliar a resiliência cibernética, especialmente nesses sistemas não homogéneos, é proposta uma estrutura que inclui a aplicação de refinamentos de Árvores de Ataque e Redes de Petri Coloridas Temporizadas Hierárquicas para modelar comportamentos de invasores e defensores e avaliar o impacto de cada ação no comportamento e desempenho do sistema.

Palavras-chave: Sistemas Sociais Ciberfísicos, Resiliência Cibernética, Segurança Cibernética, Redes de Petri Coloridas, Avaliar Resiliência Cibernética, Taxonomia Sistemas Sociais Ciberfisicos, Taxonomia Ciberresiliência.

Contents

List of Figures

List of Tables

Acronyms

ACP	Artificial, Computational, Parallel 16, 17, 59
ACT	Attack Countermeasure Tree 30, 33
ADT	Attack Defense Tree 8, 33, 66, 67, 72, 94
AFT	Attack Fault Tree 33
AG	Attack Graph 4
AI	Artificial Intelligence 16
AT	Attack Tree 4, 15, 30, 67
CIA	Confidentially, Integrity, Availability 112, 114
CPN	Coloured Petri Nets 15, 36, 38
CPS	Cyber Physical System 1, 2, 4, 8, 9, 56
CPSS	Cyber Physical Social System 1, 5, 6, 7, 8, 9, 10, 12, 15, 107
CPST	Cyber Physical Social Thinking 49
DDoS	Distributed Denial of Service 22
DoS	Denial of Service 2, 10, 19, 85, 97, 103, 106, 111, 114
DT	Defense Tree 32
DVFS	Dynamic Voltage and Frequency Scaling 16
GrSMs	Graphical Security Models 30, 31, 33, 66
GSPN	Generalized Stochastic Petri Nets 41, 66, 67, 72, 73
I4.0	Industry 4.0 1, 37, 45, 55, 59
I5.0	Industry 5.0 1, 54, 55
ICMP	Internet Control Message Protocol 90
ICT	Information Communication Technology 47, 62
IDS	Intrusion Detection System 7, 84, 88, 97, 110, 112
IoP	Internet of People 49

IoT	Internet of Things 56
IRM	Intermediate Representation Model 16
KNN	k-nearest neighborhood 18
KPI	Key Performance Indicator 22
LAN	Local Area Network 83
MAN	Metropolitan Area Network 83
MOCOP	Multi-Objective Combination Optimization Problem 16
NAS	National Academy of Science 20, 24, 26
NSF	National Science Foundation 1
PAN	Personal Area Network 83
PN	Petri Nets 68
PT	Protection Tree 31
RG	Reachability Graph 37, 118
RoA	Return of Attack 33
RoI	Return of Investment 30, 31, 33
SA	Situation Awareness 63, 64, 91, 107
SCADA	Supervisory Control and Data Acquisition 30, 33
SE	Social Engineering 97, 107, 108, 115
SG	Smart Grids 56
SIEM	Security Information and Event Management 85, 104, 111
SIoT	Social Internet of Things 50, 126
SoS	System of System 51
SSL	Secure Sockets Layer 103
STRIDE	spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege 37
TCP	Transmission Control Protocol 90, 112
TCPN	Timed Coloured Petri Nets 5, 8, 38, 84, 89, 97
TLS	Transport Layer Security 103
TOCTOU	Time Of Check to Time Of Use 38
TRBAC	Temporal Role Based Access Control 38
UDP	User Datagram Protocol 90

VHDL	Very High-Speed Integrated Circuit Hardware Description Language 86
VM	Virtual Machine 111
WAN	Wide Area Network 83

1

Introduction

I find it fascinating that you can look at the same problem from different perspectives and approach it using different methods.

Maryam Mirzakhani (1977–2017)

1.1 Motivation

The motivation for this work was inspired by the DEFENDER project that was previously undertaken in the cyber security analysis aided by graphical analysis models. The success and impact of that project served as a catalyst for my interest in pursuing similar research. As a result, I have attempted to build on the foundation established by that project in order to contribute new insights and advancements to the field.

Developments in ubiquitous computing technology, integration of computation, and physical processes have led to a definition of systems called Cyber Physical System (CPS) [1]. The CPS technologies drive competitiveness and intelligence in a range of application domains, including agriculture, hospitality and tourism, civil infrastructure, energy, healthcare, environmental management, transportation, and manufacturing [2]. The US National Science Foundation (NSF) [2] has identified advances in CPS as one of their core research aims to expand the horizons of these domains through smart CPS technologies and innovations. In consonance with the NSF´s program, the European Commission has supported research and improvement in CPS since 2014; hence, they have reckoned that CPS is a key infrastructure for the futuristic world I live in. They believe that CPS brings a superior quality of life to people and European industries [3], which means leading the European industry to digitization, which the German initiative "Industry 4.0 (I4.0)" is an example. During COVID-19, which started in 2020, the EU introduced Industry 5.0 (I5.0) to complement I4.0 with the aim of "putting research and innovation at the service of the transition to a sustainable, human-centric, and resilient European industry" [3].

The recent attention of system designers has been on human and social integration in CPS which has brought about a novel paradigm called Cyber Physical Social System

(CPSS) [4]. Human and social interactions have a noticeable impact on managing the security of the systems. In fact, in the CPSS, humans, and society are not considered external components, but they represent social systems and are full members of the entire system [5].

The cyber layer in a CPSS (the same as a CPS) corresponds to the computation and communication of other components in a CPSS (sensors, actuators, humans, applications, etc). Companies and big industries can lose their customers' trust as a result of their poor cyber-security. Also, the number of sophisticated hackers is increasing, which means they can disrupt the systems by gaining unauthorized access to the websites of companies and manipulating their servers. In a formal report released by the White House in February 2018, they estimated the impact of malicious cyber activities on the US economy was between $57 billion and $109 billion in 2016 [6]. These activities directed at private and public entities manifest as Denial of Service (DoS) attacks, data and property destruction, business disruption, and theft of proprietary data, intellectual property, and sensitive financial and strategic information.

In this research, the cyber-resilience of the system as a property of systems will be investigated, focusing on the application layer of CPSS and restricting it to three kinds of attacks: buffer overflow (TCP SYN flood attacks), Social Engineering, and DoS.

This study is conducted to meet this requirement in CPSS in terms of graphical modeling. The rest of this chapter completes the motivations for this work and provides an overview of the proposed solution. At first, in (Section 1.2) I give an overview of this research motivation and the importance of research on cyber resilient, and in (Section 1.3) I provide this research scope, then I elaborate on the problem that this work aims to address by deliberating the hypotheses and research questions (i.e., the problem space in Section 1.4). Afterward, the basic elements of the proposed solution and the specific contribution of this thesis are discussed, (i.e., the solution space under the thesis vision (Section 1.5). The details of the research methodology that I have followed throughout this work are then presented (Section 1.6). Finally, the structure of the remainder of this document, explaining each chapter's relevance to the stated thesis, is presented (Section 1.7).

1.2 Research Motivation

The evolution of isolated devices into homogeneous control systems that operate within dedicated networks is evident in the proliferation of smart and IoT devices, which are now more interconnected than ever before and utilized in various settings such as residential homes, factories, and critical infrastructure. These cutting-edge tools can enhance efficiency and hasten the execution of tasks while also facilitating better oversight and accessibility. However, the possibility of cyber, social, and physical attacks, programmatic and human errors, as well as environmental uncertainties, presents significant challenges that must be addressed [7].

Traditional security analysis focuses on the threat, and vulnerability analysis, and following that, risk assessment is limited to the cyber security scope [8]. Therefore, in the research context, developing methods and techniques to calculate consequences for incidents and avoid unwanted exposures were the central themes for a long time when the usage and application of the Internet and cyber systems were not expanded to people´s daily lives.

However, existing security and privacy approaches aim to address the security of embedded systems, which becomes prohibitively difficult to adapt to those in highly complex and interconnected systems such as CPSS. As a digital transformation, hyper-convergence creates unintended getaways to vulnerability and attacks. In CPSS, considering human characteristics and stochastic behavior, designing secure systems is a complex task. Human behavior has a high impact on the behavior of the system either in non-autonomous systems or autonomous ones. For instance, social engineering, such as email phishing, is one of the threats in CPSS that can trigger data sets and lead to enclosing sensitive information, or disruption in the system's performance.

The upcoming iteration of CPSS needs to be created with the capacity to operate effectively in ambiguous and unforeseeable conditions, and in the long run, it should possess the ability to bounce back from incidents and interruptions. The application of cyber resilience strategies is necessary to enable systems to withstand and recover from disruptive cyber incidents. This underscores the significance of assessing the resilience of cyber systems, particularly CPSS, as a critical property. Although research has extensively examined the security analysis needs of CPSS, few studies have offered solutions for cyber resilience. Thus, it is crucial to comprehend the different attack types and detection systems in order to develop appropriate defense and recovery plans for the system.

Another challenging issue for making CPSS resilient is the augmentation of the social system, which makes these systems more vulnerable and increases the risk of cyber-attacks. In this sense, an initial step is studying and understanding human behavior and its interaction with other people in the context of social and even cyber-social systems. It is hard, but to some degree, it is possible to find out the attack patterns by tracing and learning from past and current events. Therefore, identifying each component of CPSS and their interactions, besides cyber security analysis methodologies, provides strong knowledge for designing cyber-resilient systems.

All the sources of resilience mentioned above can undermine the certainty with which decisions are made during the defense and recovery phases. Given that the scope of a resilience analysis can be quite extensive, this study focuses on discussing resilience in the context of cyber security and how it can be adapted to the definition of cyber resilience.

I propose a framework for modeling and assessing the resilience of the CPSS based on the phases defined in the NIST and MITRE report [9, 10]. The framework is used to construct a graphical security model and security evaluator to automate the security analysis of the CPSS. More specifically, the graphical security model is based on two representations; an attack-defense tree to capture potential paths and mitigation, and the second one is Petri nets for performance evaluation of the system in each scenario. The Petri nets will model the framework for evaluating the resilience of the CPSS.

1.3 Research Scope

Cyber security and cyber resilience are important issues which are along with recent advancements and the popularity of information and communication technologies via smartphones, smart transportation, and critical infrastructures. Although cyber security is still a challenging and open issue, there is a significant increase in the studies in the resilience realm in different systems during recent years [11].

Furthermore, cyber resilience in CPSS in addition to the operational level is also important at the design level. The goal in cyber-resilience evaluations is to ensure business functions and missions are adequately run by "anticipate, withstand, recover from, and evolve in the face of persistent, stealthy, and sophisticated attacks focused on the cyber resources on which they depended" [12].

Considering the cyber-security approach for evaluating the resilience of CPSS, three main goals of their security should be regarded as consist of; Confidentially, Integrity, and Availability-the so-called CIA triad. Each of these criteria is measured by qualitative and quantitative metrics, for instance, in available properties in a web service technical point of view, queries per minute, and bits per second are two of the performance metrics.

Taking cyber-security metrics into an account, it is crucial to define the right meaning of cyber resilience terms and distinguish the similarity and differences of resiliency in different domains. Accordingly, modeling CPSS threats, vulnerabilities as well as defenses, their impacts on the CPSS, and defining an adaptable and scalable evaluation model for cyber resiliency.

The most related aspects, which intersect to determine the scope of this research are illustrated in Figure 1.1. It is noticeable that for analysis of resilience and security in CPSS I need to have a deep look at works on CPSS. Among current models for evaluating security in CPS and limited ones in CPSS, graphical analysis is vastly used. Tree-based and graph-based analysis methods, which have been intensive to enumerate potential attacks and possible loopholes or vulnerabilities to access and disrupt systems, are mostly used for describing the attack paths and goals in systems.

Besides the strengths and advantages of tree-based methods to represent attack scenarios, they have some disadvantages. For example, one problem for Attack Tree is that they are static and unable to adjust for dynamic systems. Another problem with AT and Attack Graph is that they are not scalable, and also regarding the automatic generation of the model, AT and AG [13] are not supportive. In this case, these models should be used with other methods to overcome these problems.

However, ATs and AGs are useful (and I apply them) for security analysis and planning resilience strategies, the initial step regarding system resiliency evaluation is to analyze the systems’ behavior in the ’norm’ and compare it in ’distribution’ after attacks and

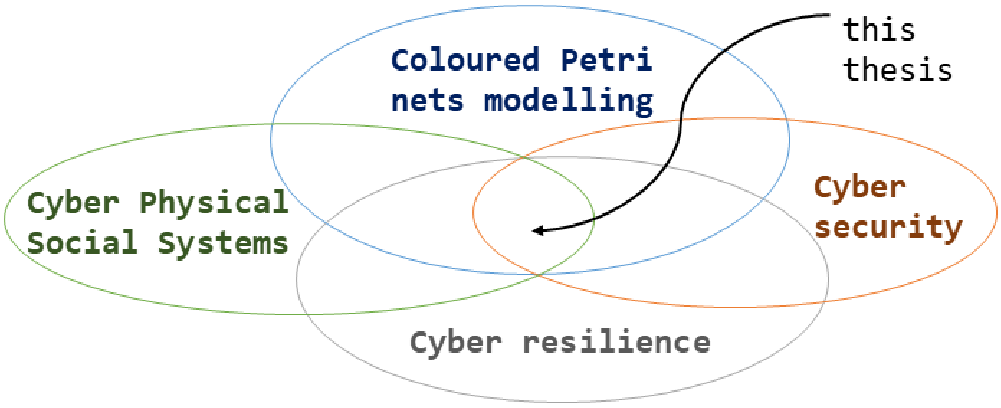


Figure 1.1: This thesis scope

defense. Haimes [14] describes this evaluation as: "the behavior of the states of the system, as a function of time, decision, exogenous and random variables, and inputs enable modelers to describe, under uncertain conditions, its future behavior for any given inputs (random or deterministic)."

As a result, enhancing system resilience is dependent on the ability of the selected security analysis model to describe and predict attack paths, as well as display the effects of defense tactics to ensure that the system's security and performance meet mission requirements. This subject gets more important when the model needs to adapt and describes human behavior, for instance, in evaluating cyber resilience in CPSS which in it, the social systems bring uncertainty and stochastic behavior for the system.

The objective of cyber resilience evaluation determines what is the proper model and technique to be applied. In general, resilience approaches can be divided into design and running time. In this thesis, I propose an adequate graphical model (Timed Coloured Petri Nets (TCPN)) [15] that is placed in the design approach and is adaptable with most security analysis graphical models. I study and research deeply on CPSS and design a framework to evaluate the CPSS cyber resiliency.

1.4 Research problem and Hypothesis

Based on the identified research gap to model and evaluate cyber resiliency in a CPSS, in this section, I outline research challenges that I address in this thesis. The primary objective of this thesis is to provide a framework and graphical modeling for evaluating attacks impact, countermeasures, and recovery strategies in CPSS to enhance cyber resiliency in these systems. The main reason for choosing CPSS in this thesis is their ever-increasing importance to interconnect heterogeneous components in application domains like smart and humanized technologies and domains, where interoperability with acceptable performance is essential. In this section, I outline the central hypothesis and research questions.

1.4.1 Research Problem

The cyber and physical vulnerabilities provide some threats to the system. Reaching the goal point of CPSS requires high confidence in system security, specifically cyber security by providing efficient defense and countermeasure strategies. Also, putting people into the loop brings more security challenges for CPSS that some of them are new and have not been recognized in the CPS.

Cyber security and resiliency are new areas for researchers and there are still many issues that should be addressed. Clear and well-defined taxonomy of threats, vulnerability, attacks, detection, defense, and finally, cyber resilience is needed. As a result, defining a suitable modeling method to measure and evaluate system performance in terms of cyber resiliency is another difficult and critical issue to research.

However, cyber security has uncertain nature, there is not possible to secure systems with complete confidence in security. Therefore, the idea is to make systems more resilient in any attacks (intentionally or not) and it seems by increasing cyber attacks, resiliency will be one of the unavoidable requirements for designing and modeling CPSS in the future. Proper models, designs, and evaluation methods for cyber resiliency in CPSS are the main challenges among academic, industrial, and business researchers.

I was concerned with two major issues that should be addressed when modeling cyber resilience in a CPSS. The first is about the definition of CPSS and how to describe it in terms of integrating social systems into CPS and the role of humans in it. The human role defines how people's behavior affects systems and which characteristics must be modeled and improved in order to have a resilient system. The second is concerned with the appropriate model(s) capable of describing attacks, defenses, and the impact of their occurrence on each other and the system.

1.4.2 Research Questions

In this section, I outline the primary research questions that I aim to address in this thesis. Each of the research questions addresses a key challenge that I identified for this research and individual aspects of the proposed solution. I validate the proposed solution by evaluating the degree to which each question has been addressed in the proposed solution (chapter. 7). In this regard, I should answer the following questions:

Research Question 1 (RQ1). *How can I evaluate the CPSS performance after an intrusion happens by a graphical model that shows attack impact as well as a countermeasure and recovery strategies efficiency?*

The primary objective of this research question is the development of an appropriate graphical model based on cyber resilience definition and theories and introduce a proper model for evaluating the resilience of Cyber-Physical Social systems. In any modeling approach, I need to know what the purpose is, and what I want to learn about the system by making this model, what kind of properties I am going to be interested in investigating. The purpose of this model will be to help system designers and security administrators evaluate taken strategies to enhance the resilience of CPSS.

Research Question 2 (RQ2). *How is our modeling approach adaptable to most used graphical security analysis models?*

The primary objective of this research question is to integrate cyber attack analysis, countermeasures, and (recovery if exist) models into a uniform state-based model to measure/evaluate resiliency. I explore an approach that is adaptable with existing models that can be interchanged if it is needed then administrators and system designers can predict and prevent incidents in the systems and transfer knowledge to the systems. It means I need to represent all the possibilities in a graphical model, which consists of attacks, countermeasures, defenses, and detection components. The well-matched approach offers a static analysis of attack and defenses. It can also, represent the performance of a system in both normal and abnormal events.

Research Question 3 (RQ3). *How well our modeling approach can model human behavior as a main component of a CPSS that shows the impact of their decisions on the performance of the system?*

The primary objective of this research question is to examine human characteristics and decisions in the social context and Human-Computer Interaction (HCI) and map them into a graphical model. The point is that, in a CPSS, human behavior has an important role to determine the performance and functionality of the system.

1.4.3 Hypothesis/Solutions

Central Hypothesis. If we use a uniform model that shows attack paths, their impacts on the system, and system behavior in terms of response and defense mechanism regarding the attacks, it helps to identify the best strategy to improve CPSS resilience.

Hypothesis 1. If we consider the resilience as a state of the system, then a language model which is state-based and can model stochastic behaviors (attacker behavior), is a proper tool to depict the behavior of the system. It is beneficial for comparing the performance of the system in the norm and during-after incidents. System performance and time are two main attributes that should consider in modeling system behavior in the resilience framework.

Hypothesis 2. For answering this question, there are two hypotheses: 1. If the attack is known for the system, we should model the behavior of an IDS regarding the attack, and the behavior of the system is dependable. In this case, we need to show the interdependency of the system on the performance of other sub-systems such as an IDS.

2. If the attack is unknown, the impact of the attack will be dependent on the human behavior (attacker skills, motivation, the objective, and cost of the attack), so we need to model the stochastic system performance in both situations whether the attack is successful or not.

Hypothesis 3. If we use a graphical model that is able to model the uncertain behaviors, we can classify and model the human decisions graphically and their impacts on the behavior of the system.

1.5 Thesis Vision

Based on the identified research challenges in CPSS and making them resilient regarding cyber attacks, I contribute to providing a survey to help full understanding of CPSS as well as most vulnerabilities, threats, and attacks in a CPSS. I fulfill the seen gaps in previous work to describe the social entity and system in the context of CPSS. I study human behavior in the context of social science to understand the mental and cogitative models.

I propose to model cyber resilience evaluation in a CPSS by Timed Coloured Petri Nets (TCPN). The TCPN model is a behavioral analysis model in that I can assign time attributes to performance analysis in the system. Also, this modeling approach is adaptable with most graphical security analysis models such as Attack Defense Tree (ADT).

Moreover, I show how to map human behavior to a TCPN model in the context of CPSS cyber security. To the best of our knowledge, this is the first attempt to model human behavior in formal modeling languages such as TCPN. This brings us an opportunity to apply the power of the PNs/TCPN to model the complex and stochastic behavior of humans as well as its impact on the resiliency of the system.

Generally, in this thesis, I contribute in following items and descriptions of them provided as well:

- Modeling cyber-attacks scenarios by Attack Trees in the Application layer of CPSS, specifically in web-based services and translate it to Coloured-Petri nets,
- Modeling cyber-attacks impacts on CPSS by Timed Coloured Petri Nets to show the behavior of the system in this stochastic situation, as well as intrusion detection systems behavior,
- Model three phases of the cyber-resilience (avoidance or detect survival and recovery) by Timed coloured-Petri nets,
- Considering social systems, bring the novelty of this proposal in the CPS area. The security of society and humans is not modeled explicitly in the CPSS. In this case, understanding the configuration of intrusion detection and defense systems is an essential part of analyzing attacks and countermeasures.

1. CPSS Taxonomy- (see chapter 4)

The first step in our validation methodology and one of our contributions is defining CPSS taxonomy to categorize the CPSS aspects, domains, and facets. This categorization helps to trace the impact of the specific threats of the systems and determine a proper defense strategy for them. Although the CPSS term is relatively new its components of that are the same as CPS addressing social systems as a full member of the system (not the external or environmental parameters). As one of the contributions of this research, I construct a comprehensive taxonomy of CPSS which covers the techniques, security, safety, and privacy in a CPSS.

2. Cyber resilience concept map- (see chapter 2)

I present the result of a systematic review of current definitions and evaluation techniques for cyber resilience which can be applied for CPSS. Analysis of resilience is impossible without first investigating security gaps and risk assessments. This work does not introduce any new concepts or techniques, but it provides a complete map for understanding cyber resilience aspects and techniques. It is necessary to scan and monitor the behavior of the system to find its vulnerability; indeed, detection attacks are part of the Plan and Preparation in the resilience analysis.

Graphical methods, both state-space-based and non-state-space-based, are systematically reviewed in this research as a tool for analyzing attack vectors, surfaces, and their impacts. Following that, I will discuss earlier works and methods used in cyber resiliency.

3. Introducing a set of rules and an approach for adapting CPN to GrSMs (see chapter 5)

Following a model-based approach for evaluating resilience in the systems, I model the behavior of the user (as a social component of the CPS), which impacts the behavior of the system by CPN. By modeling the behavior of the system in the norm and exploiting time in CPN, I can evaluate the performance of the system during recovery, and after that, I can measure the resilience of the system. As the resilience is evaluated in 5 phases (plan/ prevent, absorb, withstand, recovery, and adapt), using the framework, I can find potential attack scenarios in the CPSS, analyze the resilience of the CPSS through Ill-defined resilience metrics, and evaluate the performance of the system regarding different defense strategies, response systems, intrusion detection systems.

4. Applying ADT to model attack paths and defense system

Modeling cyber attacks scenarios by attack trees on the application layer of a CPSS, specifically in Ib-based services and translating it to Coloured-Petri nets:

The proposed framework is produced by paying attention to the resilience framework provided by NIST. In this regard, I propose to understand and plan for a cyber-attack, then respond and defend the system, and validate the plan by GrSMs, which I use ACT (Attack countermeasure Tree). To analyze the interaction and dependability of the performance of the target system with the mentioned system, I need to translate the GrSMs to PNs/CPNs. I improve the current translation rules and model the system regarding the possible scenarios and attack paths.

5. Introduce an approach for modeling

Modeling cyber-attacks impact on CPSS by Coloured-Petri nets to show the behavior of the system in this stochastic situation, as well as Intrusion detection systems limited to Phishing, Social Engineering, and DoS: Evaluating absorb, I model the IDS behavior and evaluate their performance based on the true detection so-called Accuracy in section 7. The result and performance of the response system consider the withstand phase. Evaluating resilience, I evaluate the performance of the CPSS based on the related metrics. For example, in web-based services, the response time, QoS (failed requests, accuracy), which generally I refer to availability, will be measured as well as the recovery time from a technical point of view.

6. Model humans behaviors- (see chapter 4 and chapter 7)

Considering social systems, bring the novelty of this proposal to the CPS area, in which I will show how society as a network of human behavior impacts the resilience of systems. (in terms of sabotaging security or protesting systems) As the SoA is studied, the security of society and humans is not modeled explicitly in the CPS, which is integrated with social systems. In this case, understanding the configuration of CPSS is an essential part of analyzing attacks and countermeasures. This part includes modeling the interaction of human behavior (as one of the social components in a CPSS) with the system in which I depict it by CPN and evaluating the trade-off between each part's goals, the steady-state analysis in the reachability graph will be used.

To restrict the variables in the study, first of all, our focus is on the application layer of CPSS with an analytical approach.

1.6 Adopted Research Method

The research is structured according to the classical research methodology that consists of main seven phases of the work plan as follows: 1. Identify and formulate the problem/questions, 2. Background and state of the art, 3. Formulate hypotheses 4. Design Experiment, 5.Test hypothesis/data collection; 6. Data analysis, 7. Publish findings. All the phases are shown in Figure. 1.2. This research methodology is adapted from the Research Methodology course presented by Prof. Camarinha -Matos [16]. These steps can be organized according to the following phases:

- Phase 1: Identify the problem/question [Jun 2017- Jun 2018]
  For this phase, I did a systematic mapping study, which means a board review of primary studies in a specific topic area that aims to identify what evidence is available on the topic. After a preliminary literature observation, needed motivation is found, a proper problem is identified, and the research question is formulated;

- Phase 2: Background/State of the Art [July 2018- Jun 2021]
  The stage of the literature review was devoted to background studying of cybersecurity, cyber-physical, social systems, machine learning, and Petri nets, which did

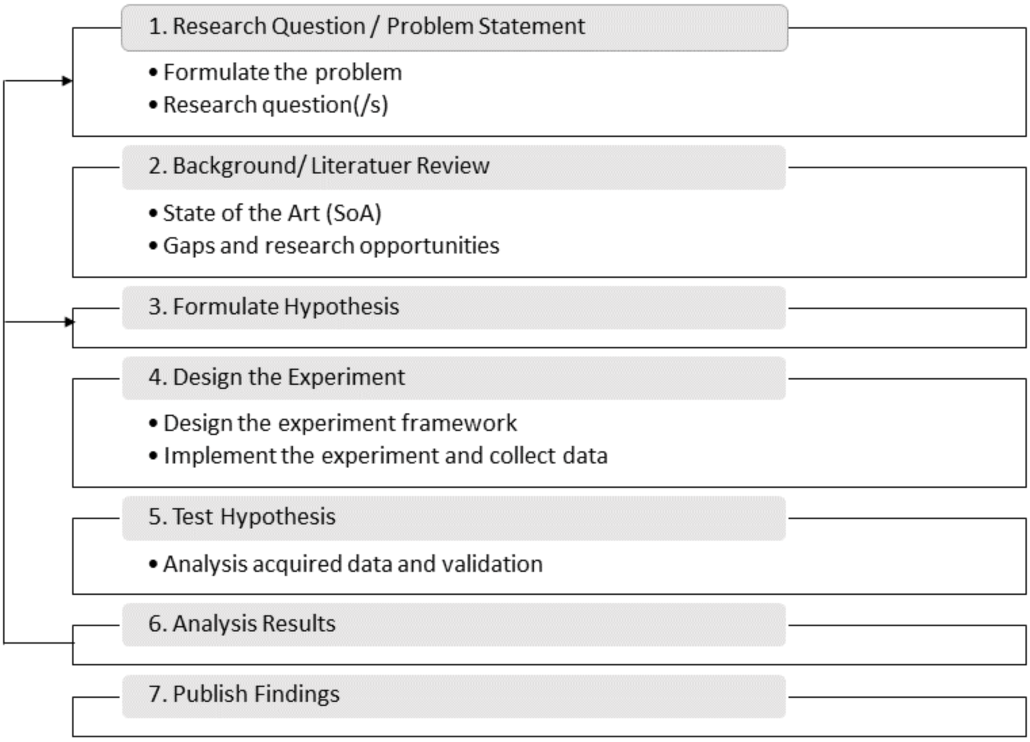

1. Research Question / Problem Statement
• Formulate the problem
• Research question(/s)
2. Background/ Literatuer Review
• State of the Art (SoA)
• Gaps and research opportunities
3. Formulate Hypothesis
4. Design the Experiment
• Design the experiment framework
• Implement the experiment and collect data
5. Test Hypothesis
• Analysis acquired data and validation
6. Analysis Results
7. Publish Findings

Figure 1.2: Adapted Research Methodology

in systematic literature review methodology;

- Phase 3: Formulate hypothesis [Jun 2019-Dec 2019]
  After analysis of the current state of the art, main open problems in the area, and definition of the research question, the hypothesis was formulated;

- Phase 4: Design Experiment [Jan 2020-Feb 2021]
  This phase can be divided into four steps:

  1. Development of an attack model detect attack to identify the vulnerability of the system, attack vectors, and a set of actions that will prevent or mitigate the attacker's goals;
  2. Setting software to extract attack data and events;
  3. Identifying the feature of the attacks; and
  4. Developing a model to find the attackers' patterns, and attributes and assign proper defense.

- Phase 5: Test hypothesis/collect data [May 2020- Feb 2022]

-Validation of the designed model and concepts for the use cases based on the legacy of data, and test data. The model is applied in validation scenarios.
-Design of validation scenario based on the use cases.
-Implementation of the designed model;

- Phase 6: Interpret and analysis data [Jan2021-Jan 2022]

  -Analysis and evaluation of the model, methodology, and proposed tools in the context of cyber resilience; and

- Phase 7. Publish findings [Jan 018-Jun 2022]

  - The continuing findings of the work are published/submitted in high-ranked conferences and journals indexed in recognized organizations such as Web of Science, Scopus, etc.
  - A survey of the SoA in this document is published as a review paper.
  - The main deliverable of this research work with combining all findings and that final conclusion.

1.7 Dissertation Outline

The structural organization of the thesis is illustrated in Figure 1.3. In the remainder of this section, I provide an overview of the contribution of each chapter.

Chapter 2 presents the research background and related definitions and concepts that I use throughout this thesis. I explain some of the fundamental concepts that provide background details before the discussion of the thesis contribution. In this chapter, I focus on the cyber resilient definitions, the role of models in designing and evaluating cyber resiliency of systems, and critically review the state-of-the-art of existing techniques.

Chapter 3 presents a detailed comparison of the related work according to the cyber security graphical modeling as well as Petri nets (PNs) classes that have been applied in cyber security analysis(GrSMs). In this chapter, the possibility of translation from GrSMs to PNs is studied.

Chapter 4 provides a uniform definition for the CPSS based on a comprehensive and systematic review of CPSS. In this chapter, A CPSS taxonomy is proposed which helps to understand our position in designing a model to evaluate cyber resilience in CPSS. The results in this chapter provide helped us to answer research question RQ3.

Chapter 5 proposes a set of rules to translate GrSMs to CPN which can be used in reverse as well. In this chapter, I first review the state-of-the-art of translation reasoning techniques and mechanisms, then propose and explain the rules. This chapter also presents experimental evaluations of the framework. The results in this chapter provide an answer to research question RQ2.

Chapter 6 describes in detail the framework, design, implementation, and experimental result of the isolated lab and data collection according to test the validity of the hypothesis. In this chapter, all the scenarios regarding the cyber attack, defense, absorb, and recovery phases in cyber resilience are explained.

Chapter 7 shows how the three phases of cyber resilience are integrated into a CPN model to enable the evaluation of each component of the system performance under a cyber attack situation. To conduct this research, I followed the guidelines of the action research methodology (Chapter 1) which provides a rigorous set of steps focused on planning (Chapter 2, Chapter 3) and conducting the research (Chapter 4, Chapter 5, Chapter 6) along with the evaluations of the research results (Chapter 7). Therefore, in this chapter, in summary, I show the validity of the research hypothesis. The results in this chapter provide an answer to research question RQ1.

Chapter 8 concludes our research contribution in the context of research gaps identified in Section. In this chapter, I review the contribution once again. I also discuss limitations, threats to validity, and the potential for future research.

Appendix A presents the design of the isolated lab used in Chapter 6.

1.8 Chapter Summary

This chapter provides the research motivation based on a brief overview of existing research and its limitations. Based on the identified research challenges, I outlined the central hypothesis that allowed us to identify the research questions. The role of individual research questions is vital in highlighting the solution requirements. I highlighted the adoption of a customized research methodology to plan, conduct the research, evaluate the developed artifacts and reflect on the research implications. I also specified our research claims, which become the main criteria for evaluating the approach. Finally, I provided an overview of the organization of the thesis. The chapter provides a foundation to present the results of our literature review and provides an overview of the proposed solution. A summary of the objectives and the outcome for the individual chapters in this thesis is presented in Figure. 1.3 which allows us to discuss the research positioning, contributions, and evaluation in subsequent chapters.

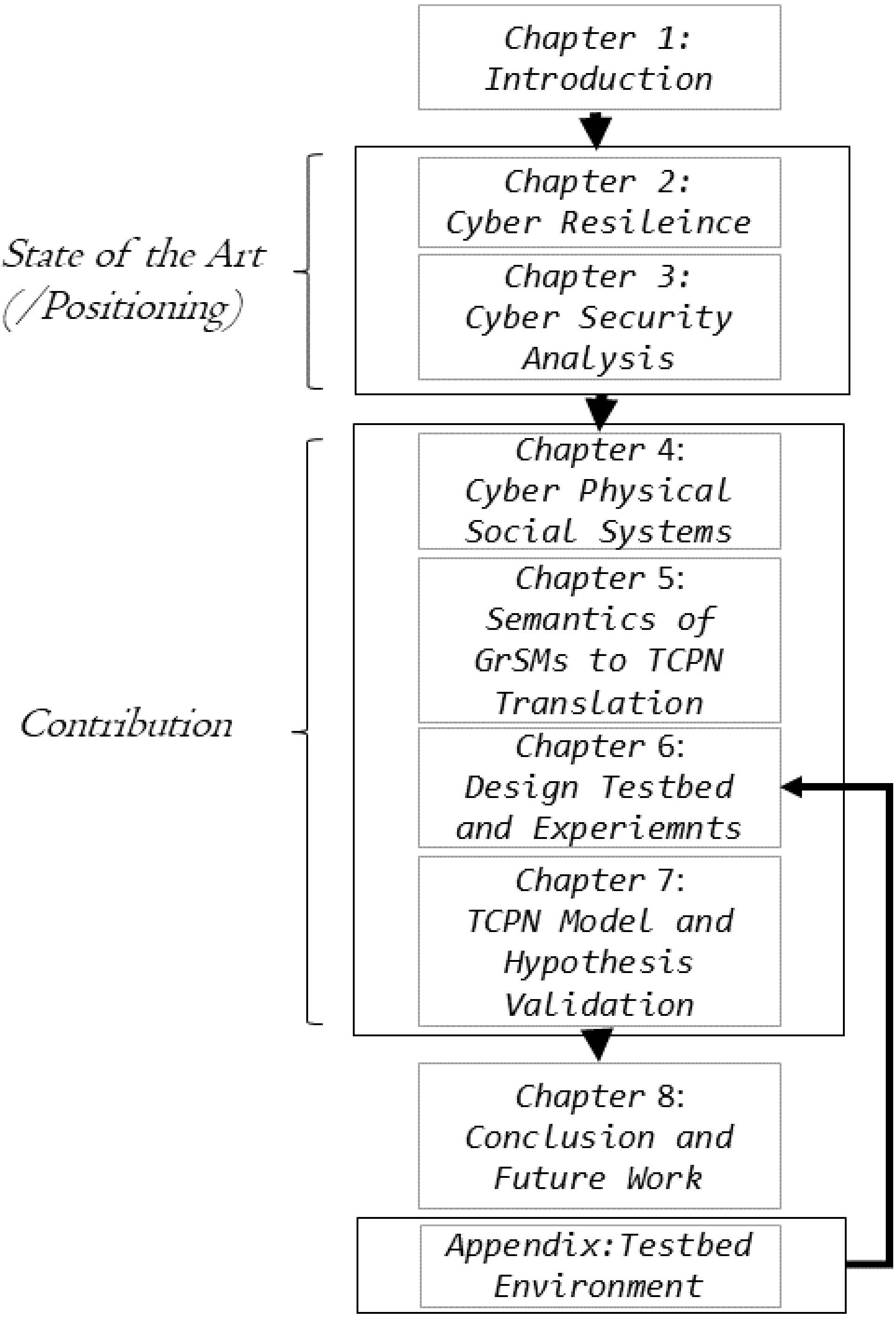


Figure 1.3: Dissertation Organization

2

Cyber Resilience in Cyber-Physical Social Systems

Intelligence is the ability to adapt to change.
Stephen Hawking (1942–2018)

2.1 Introduction

The most prominent research areas that have affected this thesis are "cyber security", "cyber resilience", "graphical analytic models", and "cyber-physical social systems". There are numerous study groups within each discipline, each of which focuses on particular facets of that field. The overarching themes of this thesis are cyber security and cyber resiliency. The graphical analysis models such as Attack Tree (AT) and Coloured Petri Nets (CPN) are closely related techniques to model and evaluate cyber security and cyber resilience in the system of interest. CPN modeling is chosen to be investigated, tailored, and designed for adaptation modeling to evaluate cyber resiliency in CPSS. In this thesis, the key domain to which I apply my solution framework in order to enable the design of and evaluate cyber resiliency is the CPSS. Considering that CPSS are a new paradigm, it is broadly discussed in Chapter 4. In this chapter, I will provide a proper definition of cyber resilience in a CPSS, its concept map to propose the evaluation methodology, and the relative metrics.

2.1.1 State of the Art

The relationship of each entity in the CPSS by emphasizing human factor incorporation which is tightly integrated with physical and cyber elements differs from traditional CPS. To the authors' best knowledge, a literature review that analyzes different approaches in designing and developing services in CPSS and associated taxonomy has not yet been conducted. Although several studies and reviews have focused on the design of CPSS, there are still some interesting and relevant problems to be addressed.

The primary challenge in designing a CPSS is the manner in which physical, social, and hardware can be efficiently integrated and described in real systems [17, 18]. In the CPSS, both physical and social sensor networks are connected to their physical and social operating systems respectively. They communicate and be controlled through cyber systems alike the CPS. Subsequently, physical and social systems based on their applications can be mapped equivalently to their cyber systems which form the idea of a platform-based approach for system-level designing in CPSS. Taking into account the heterogeneous networks and social components of the CPSS, system-level designing is one of the solutions to overcome the complexity of designing the CPSS. Based on these ideas, Zeng et al. [17] proposed a system-level design methodology called "Hyperspace Space Flow". The proposed methodology comes with three components. The function specification is considered in the Intermediate Representation Model (IRM), and the control flow is modeled by hierarchical Petri nets (upper Petri Net models that are refined by bottom Petri Net models), which model the states and events of the physical and social components. A drawback of this methodology is considering the social system for one user which is not what social entity means in the CPSS. In another work by Zeng et al., [19], the same system-level design framework was proposed but for fulfilling a functional specification requirement of a CPSS including energy consumption, user satisfaction, and security focusing on confidentially as well as corresponding constraints. They leveraged Dynamic Voltage and Frequency Scaling (DVFS) to reduce energy consumption and solve several issues, including reliability and user satisfaction. They have used the Multi-Objective Combination Optimization Problem (MOCOP) methodology and a genetic algorithm to find an optimal solution for the three objectives of their work. In another work by Pasandideh et al. [20], controlling traffic lights as CPSS is modeled using a web interface tool called IOPT-Tools [21]. In this work, human (social information) plays the role of information resources for the system. In this model, Petri nets are used to model the IRM to control the physical and social flow.

As a matter of fact, the integration of social systems and relationships with other systems brings more challenges to CPSS in terms of modeling and designing. Wang [22] perfectly mentioned this issue and was in an option that new science is needed for social studies. The social systems need to be studied from a new multidisciplinary approach involving the physical, social, and cognitive sciences integration with the cyber world. He reckoned that Artificial Intelligence (AI)- based systems will be key to any successful construction and deployment of the CPSS. He proposed adopting a traditional three-stage model including modeling, analysis, and control. He called his new model ACP, which is one of the pillars of CPSS applications and models. The ACP approach stands for artificial societies for modeling, computational experiments for analysis, and parallel execution for control. Artificial societies include agents, environments, and rules for interactions for describing and modeling the system, Computational experiments, which are an extension of computer simulation techniques to evaluate a system, and Parallel Systems, by comparison, evaluation, and interaction of artificial systems to control and manage a complex system. The introduced approach can solve the complexity of CPSS, and the core of the approach is based on data and knowledge discovery. Current advanced and smart technologies, such as cloud computing, big data analysis, and high-throughput communication, are in line with the ACP approach.

The efficient interaction of the resources of both physical devices and humans in a CPSS as a self-organization system was formulated by Smirnov et al. [23, 24] in a context ontology inspired by Zimmerman et al. [25]. The context consists of information; individuality, activity, location, time, and relations. Information is captured from the agent's environment and the results of its activity, the individual defines the entity by properties and attributes; activity is related to the allocated tasks to the entities in the community that define events and vice-versa; location and time provide the spatiotemporal information about the respective entity, and finally, the relations category depicts possible relations between one entity and others [26]. The well-defined definition and interaction of entities (especially social entities) and the multi-agent approach in this ontology can be considered an important reference for understanding the CPSS and designing convenient models, and development services in the CPSS ecosystem.

The data-fusion framework is another challenging issue when considering the heterogeneous nature of CPSS. Wang [27] proposed a tensor-based Cyber-Physical-Social big data framework with seven layers for CPSS design to overcome the lack of a uniform data fusion model in CPSS. The tensor-based framework layers 1 to 7 consist of:

- Data source ("Tri-Spaces": Cyber, Physical, and Social);
- Perception layer (which is divided into "Hard sensors": physical devices and "Soft sensors": networked sources like a social network);
- Data representation;
- Fusion layer (which uses Tensor-based Uniform Fusion (TUF) model);
- Data processing/mining by applying Tensor Decomposition algorithm (TD);
- Rule layer by introducing Eigentensor;
- and the last layer is the Application layer.

The architecture consists of four modules, namely Inter-Sensing Module (ISM), Data Fusion Module (DFM), Rules Module (RM), and Application Module (AM).

From the CPSS framework point of view, Guo [28] presented a D-CPSS (which stands for data-driven CPSS) framework for designing and deploying CPSS applications and services considering a four-layer architecture, namely resource management, cooperative sensing, data processing, and data analysis. Each of these layers has different functionality. In this cross-data fusion framework resource management and cooperative sensing, the layers correspond to data collection but the data processing task is covered by data processing and data analysis. This framework provides an initial step for researchers to understand data mostly in the context of urban management and can be helpful in designing and applying a proper data management system for CPSS domains.

A CPSS is a concept that is defined from a different point of view, such as multi-agent systems, or multilevel systems. The manner in which I describe and define CPSS components and the relationships among them can change the system model. Different categories of these approaches are provided in Table 2.1.

Table 2.1: Proposed CPSS Models and Frameworks

Approach	**Data driven**	**Tensor Based**	**Event Driven**	**Model Based**	**Platform Based**
Multi-level	[27, 29]	[27]			
System-level				[20, 23, 30]	[17, 19]
Multi-Agent	[31]	[27]			[26]
Upper-level Ontology			[24]	[23, 30]	[26]

In all of these conceptual models, the computation mechanism is not well remarked. Sheth, Anantharam & Henso in 2013 [32] introduced Physical-Cyber-Social (PSC) computing as a relatively novel and strong emerging paradigm to support and formulate CPSS. It supports the Computing for Human Experience (CHE) vision by involving observation, experiences, background, knowledge, and perceptions. It encompasses a holistic treatment of data, information, and knowledge from PSC worlds to integrate, correlate, interpret, and provide contextually relevant abstractions to humans.

One of the issues in real-time and big data computation in CPSS is redundancy. This might occur with historical and periodic incoming data, for which Wang[38] proposed a Distributed column-wise High-Order Singular Value Decomposition (DHOSVD) and Incremental HOSVD (IHOSVD) algorithm to perceive dimensionality reduction, extraction, and noise reduction for tensor-represented supporting online computation on temporally incremental data streaming big data. Processing massive CPSS data is a considerable issue. The k-nearest neighborhood (KNN) as one of the widely-used clustering machine learning techniques for processing massive amounts of data has gotten attention [33]. Nevertheless, they have limited storage capacity and computational power. In this regard, Zhang [34] proposed a Distributed storage and computation k-Nearest Neighbor algorithm (D-kNN). Their experimental results showed that this algorithm can be easily and flexibly deployed in a cloud-edge computing environment to process big datasets in CPSS.

2.2 Cyber-Resilience Definition

Resilience is a broad term that is applied differently in each discipline to achieve a specific goal. The method for defining a system's restoring force defines its characteristics, metrics, measurements, and evaluation methods. In fact, the cyber resilience discipline is more focused on the performance of the system under and after intrusion /distribution and has its own idiosyncrasies that be conquered.

One of the ways that may be taken in this area is to comprehend and categorize cyber-attacks according to the impact that they have on the overall performance of the systems as well as their collective behavior and characteristics. However, there are a variety of semantics and graphical models that may be used to evaluate cyber attacks. These models were not developed to display the dynamic state of systems, nor are they relevant for automatic detection and protection in the event of a cyber attack. The interconnection of different resilience phases is something that is poorly reflected in a lot of different frameworks. This indicates that the performance of the system and the value it provides in each phase can be altered by the phase that came before it. For instance, findings from the recuperation phase aid to enable a stronger planning and avoidance phase, which ultimately leads to improved performance in the absorb phase.

2.2.1 Background

Concerning cyber-attacks, depending on the system's configuration, different vectors can be used to intrude on physical, and cyber systems as well as people and social systems. An individual or a combination of methods can also be utilized to plague human factors in the business process. Nevertheless, human roles and behavior are not fully understood or explicit in the analysis. For instance, situational awareness can be devalued through a DoS attack [35]. Therefore, system resilience modeling and evaluation of complex, large-scale systems such as CPSS have recently attracted the attention of practitioners and researchers. The term resilience is interpreted in various ways in different applications and domains.

Resilience in the Merriam-Webster dictionary means the capability of a strained body to recover its size and shape after deformation caused especially by comparative stress and also an ability to recover from or adjust easily to misfortune or change. To the word meaning and many other definitions provided for resilience in different systems such as social, physical, and cyber, the focus of this study is on cyber resilience.

The first definition of resilience that has been considered in research is about understanding the differences in the stability of systems such as equilibrium ecosystems, societies, and organizations. Then, how the dynamic system behaves when exposed to stress and out of this equilibrium [36].

In a document provided by the MITRE corporation [9] in 2011 as, one of the complete references for the resilience framework, they gathered the definition of cyber resilience as well as its characteristics from DARPA, ENISA, DHS, etc. MITRE defines cyber resilience as "The ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function” [37].

The ability to avoid, survive, recover after a disruption, and return to desired performance. Based on the Sheard in INCOSE definition, disruption is 'the initiating event of a reduction in performance that can be sudden or a sustained event' [38]. The US Department of Homeland Security (DHS) defines the terms risk as the 'Potential for an unwanted outcome resulting from an incident, event, or occurrence is determined by its like hood and associated consequences' and resilience as the 'ability to resist, absorb, recover from or successfully adapt to advisory or a change in conditions. Resilience is considered a time-based variable [39].

In other words, resiliency refers to the system's ability to recover or regenerate its performance to a sufficient level. An expected impact produces a degradation of its performance [40]. According to the proposed definition of resiliency by the National Academy of Science (NAS) resilience in all type of systems have a set of key features. The common features include critical functions (services), thresholds, cross-scale (both space and time) interactions, and memory and adaptive management [41]. I used two figures to illustrate the concept: one to show the cycle, description, and characteristics of each phase, and the other to show the system performance 2.3 during each phase. 2.1.

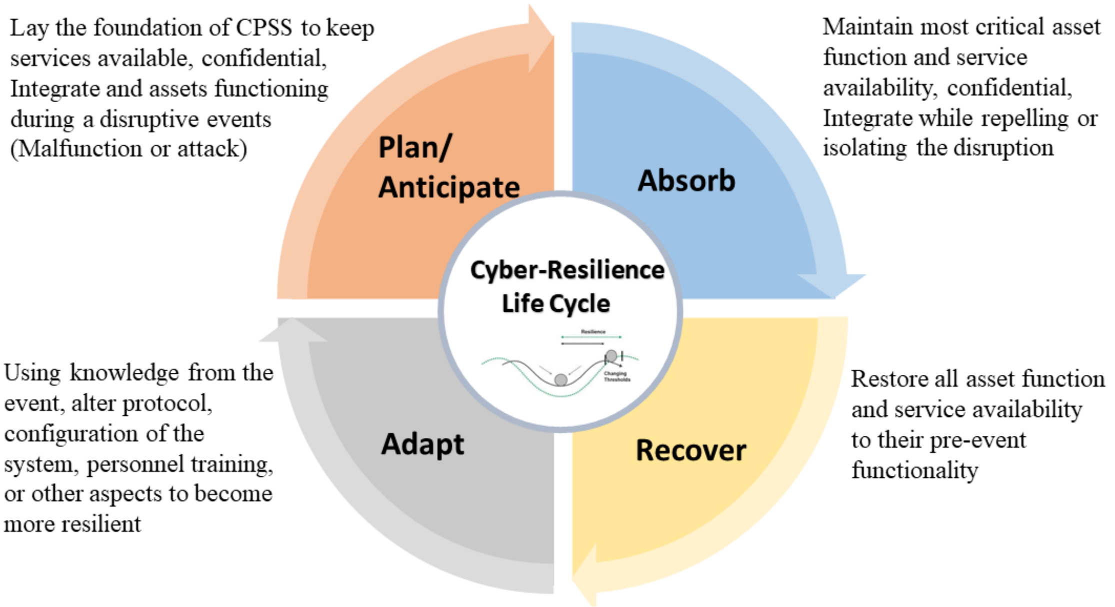

Lay the foundation of CPSS to keep services available, confidential, Integrate and assets functioning during a disruptive events (Malfunction or attack)
Plan/ Anticipate
Absorb
Maintain most critical asset function and service availability, confidential, Integrate while repelling or isolating the disruption
Cyber-Resilience Life Cycle
Resilience
Changing Thresholds
Using knowledge from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient
Adapt
Recover
Restore all asset function and service availability to their pre-event functionality

Figure 2.1: Cyber Resilience Phases

2.3 Cyber Resilience in CPSS: Cyber-Security Approach

In the CPSS, to consider a social system as an internal component of the system, I need to define a tailored definition and measurements for assessing cyber resilience in this system. By defining social computing formed CPSS that considers the social and human role as a component of this system that is not an external element in the environment.

This term brings the scalability challenge to analyze the resiliency of the systems, which is not studied enough to find out attacks and vulnerabilities of the systems. In this work, this aspect of these systems will be studied in terms of cyber security. Mostly like CPSs, considering the dependency characteristic of these systems can be evaluated for their security, but attack vectors, types, and their impact in CPSS can be different from CPSs. In this work, this plausibility will be considered entirely. To solve this problem, there are some resilience metrics to measure and analyze in CPSs that even they are not very clear. One of the objectives of resiliency is minimizing the time of recovery by considering three main security metrics for data: Confidentially, Integrity, and Availability. Another step in this work is determining these metrics in CPSS by three scenarios in the application layer. To restrict the variables in the study, first of all, our focus is on the application layer of CPSS with an analytical approach.

2.3.1 Approaches and Assessment Methods

In developing systems, beyond security, they are examined to be intrusion resilient, which means the ability of the system to continue to perform its intended function despite partially successful attacks [42]. Proper and capable attack analysis methods and tools are crucial to the quick detection of cyber-attacks to minimize the attack's impact on the normal performance of the system [43]. The main question is how to enhance the resilience of the systems. To answer this question, NIST, MITRE, and ENISA have published documents that describe the framework and definition of cyber resilience, and also, there are some works on analysis resilience in CPS and computer networks

Hosseini [11], Kott & Linkov [44] have provided a proper overview study on resilience and their assessment methods in multi-domains. In one study by Khan [45], besides the overview of a different definition of resilience, they have worked on computer and network resilience by focusing on "change" in systems as a key aspect of resilience that can be in system's structure or parameters from a dependency point of view. They analyze resilience from different dependability attributes such as; Survivable, Performance, and Availability in telephone switching systems with Continuous-Time Markov chain (CTMC).

Paridari et al. [46] consider the resilience from the control point of view in industrial control systems into two Lower layers and the Supervisory layer. Their proposed framework for attack-resilient is for the supervisory layer, which means that the resilience policies for attack/fault detection, isolation, and controller reconfiguration. For attack detection, the Security Information Analysis (SIA) tool is used. In another work done by Imtiaz Kahn et al. cyber-resilience is modeled, measured, and verified in the computer network realm. They proposed a framework for resilience engineering called the "Cyber Resilience Engineering Framework (CREF)." In this work for network resilience, three metrics are introduced: Proactive, Resisted, and Reactive. Their measuring method is categorized into Nominal resilience, Tolerance threshold, and Resilience evaluation graph, which represent the expected resiliency of security properties, the lower bound that defines the tolerance margin for the resiliency of security properties, and index how much a network system model is resilient regarding attacks or properties, respectively.

Scalability for evaluating and modeling resilience in the systems is a challenging issue, especially in CPSS, with their homogeneous and complex nature. Respectfully to this issue, Kanniche et al. [47] have summarized the techniques for modeling resilience from a model-based dependability point of view, and they applied it to web services and General Pocket Radio Service (GPRS). They suggested state-based models as one proper candidate that is able to take to account the stochastic and homogeneous character of the systems. These models, like the Markov chain, have a scalability problem. So other techniques such as largeness avoidance and largeness tolerance are mentioned in their work. They work with a combination of two dependability modeling and evaluation Markov chain and stochastic Petri nets. Their model for web service availability is hierarchical in resource, service, function, and user level. A graphical model that is the extension of the attack tree called Challenge Countermeasure Tree (CCT) is used in resilience design in Distributed Denial of Service (DDoS) attacks in a web server by Natouri et al. [48]. Another work by Zonouz et al. [49] proposes a new approach to automated response called response and recovery engine (RRE), which is based on game theory and applies an attack response tree in network security. Talking about the resilience of the system's architecture, Pradhan et al. [50] have proposed a novel design-time reliability analysis tool and also run-time dynamic reconfiguration infrastructure that support autonomous resilience via transition points computed at runtime by using encoded configuration space. They also used Coloured- Petri nets for analysis of the behavior of the system, and they applied their model in a mobile cyber-physical platform of fractioned spacecraft. There are some factors to determine Key Performance Indicator (KPI) for cyber resilience based on ENISA documents [51]. A KPI refers to a critical criterion for measuring the performance of the objective of the system. The key notion for cyber resilience is the collaboration between the sector and the later development of cybersecurity capabilities in the joint section. Raising awareness is also part of this key objective [51].

As described in the previous sections and Cardenas, et al [52] discuss, there is no solid rule for successful attacks, in this case, it is important to detect and respond to attacks specified in CPSS. These attacks mostly are not detectable from the IT side, especially when human or social components bring a new challenge in resilience management in the system. Resilience is a property of the entire system and should be assessed accordingly, not focusing on one operational domain such as physical, social, and so on, but on interconnection among the whole component of the system, which is called cross-domain characteristics.

Two primary approaches for assessing resilience (or resiliency) are introduced in [44] as Metric-based and model-based; also, it is possible to use a combination of these two. In figure 2.2, I can see that model-based approaches use a system configuration model and scenario analysis to measure resilience and mostly is practical for the prediction of the state of the system too. By this description, the models or graph analysis that are state-based are proper choices for modeling resilience in CPSS. On the other hand, a metric-based considers the performance of the system (by specific function, or component). In this case, it is important to know in which context I need to assess the performance by paying attention to the mission of the system, sources, thresholds, and expected level of performance to measure the recovery performance. In this work, I use both approaches to measure resilience in the CPSS. In this work, metrics include Mean Time to Recovery (MTTR), Mean Time to Respond (MTTR), and Quality of Service (at user level: number of failed packets, from the security point of view: availability, function level: the failed host nodes).

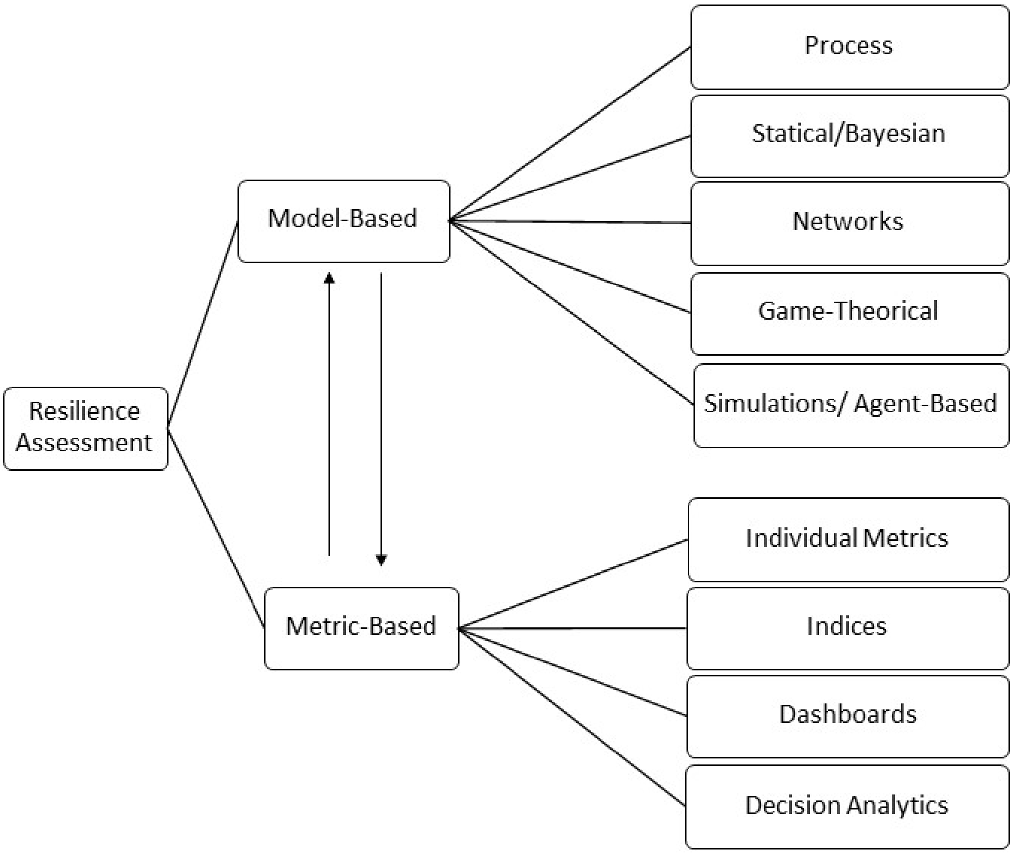


Figure 2.2: Resilience Assessment techniques [44]

2.3.2 CPSS Cyber-Resilience Analysis

Metrics for analysis performance in the CPSS are complex and require a multi-attribute utility function, and when considering the resilience of the systems, the choice of the metrics should be described and documented explicitly[45]. Linkov et al., [44] combined resilience definitions from NAS and Network-Centric Warfare (NCW) about disaster resilience to provide a matrix of resilience metrics in four operational domains; Physical, Cognitive, Social, and Information considering four stages of resilience. They consider the homogenous nature of cyber systems and their metrics are interdependent. This work does not answer the question of how resilience emerges from systematic interaction.

Another confusion about the resilience concept is "robustness," which means the degree to which a system can withstand an unexpected or unexpected external or internal disruptive event without degradation in the system's performance. While resilience is the ability of the system to recover i ts performance after an unexpected event impact on the system [53].

The social decision-making component examines how people's preferences are changing due to disruption-induced stresses. It involves a series of laboratory experiments on how stress alters social preferences, and how social and cultural identities shape those changes. The goal is to gain insights into changes in preferences and behavior when stress is induced by crisis and duress[88]. For instance, taking social media into account, Meier discussed that by 'providing norms, information, and trust, denser social networks implement a faster recovery' [36]. Regarding measuring resiliency, there is no unique indicator and it is defined differently in different systems and the objective of resilience in that system. Resilience is about estimating the maximum intensity of an absorbable force (E max) without perturbing the system's functions [54]. Security and resilience metrics have some differences and common features. In resilience metrics, both physical system and human metrics are needed. Performance analysis includes the response time to task A, cost of execution of task A by unit U, usage of the server's CPU: utilization of unit U, Transition time or time for a specific web request: Response time to task T, Apedex (Application Performance inDEX): User satisfaction or QoS, Percentage of leakage of credential information: Confidentially, Error rate, Uptime for Service Level Agreement (SLA): Availability.

It is essential to remind that resilience is not about risk management. In CPSS resilience metrics, mental space features should be determined beside other CPS resilience metrics. In this case, it can numerate observations, experiences, background knowledge (skills), society, culture, and perceptions (human intelligence and social organization: communities) [55].

In this work, I followed the MITRE cyber resilience framework and engineering. They have provided different techniques for different phases of the resiliency of a system. I adopted their proposal for a CPSS and specifically in cyberspace. In Table 2.2 the summary of cyber resilience characterization is provided. The phase and features follow the NAS definitions [41] and the objectives and techniques are given from MITRE cyber resilience engineering framework [56].

The designed system is monitored and analyzed in the plan, absorb, and recovery phases. However, the objectives are to understand, prevent and continue the functionality of the system. The chosen techniques are adaptive response and analytic monitoring.

Table 2.2: Cyber resilience phases, goals, features, objectives, and techniques- inspired by [56]

Phases	**Features**	**Goals**	**Objectives**							
			Understand	Prepare	Prevent	Continue	Constrain	Reconstitute	Transform	Re-Architect
Plan	Critical functions (Services)	Anticipate	x	x	x					
Absorb	Thresholds	Withstand	x			x	x			
Recover	Time (and scale)	Recover	x			x		x		
Adapt	Memory /Adaptive management	Evolve	x						x	x
Techniques related to the objectives										
Adaptive response (AR)							x	x		
Analytic Monitoring			x	x			x	x		
Coordinated Defense				x		x	x	x		
Deception			x			x				
Diversity						x				
Dynamic Positioning			x			x				x
Dynamic Representation			x	x					x	x
Non-Persistence						x	x			
Privilege Restriction						x				x
Realignment									x	
Redundancy							x	x		
Segmentation / Isolation						x				
Substantiated Integrity			x				x	x		
Unpredictability			x			x	x			

Considering the system´s performance, the behavior of a system in the event of an accident can follow one of three patterns; Collapsing, Ductile, and Robust. how the system behaves depends on many factors which in CPSS is more uncertain and complicated to predict. In a CPSS it is needed to take mental space and social system behavior in the response and recovery phase, also, the capacity is different. In this work, I interfere with human decisions and reactions in the phase of the response and before the incident.

In Figure 2.3 the system behavior in different phases of resilience situation is shown. As it is shown in Figure 2.3, both events incident and recovery during the resilience phase are temporal and are not one-step events [57, 58].

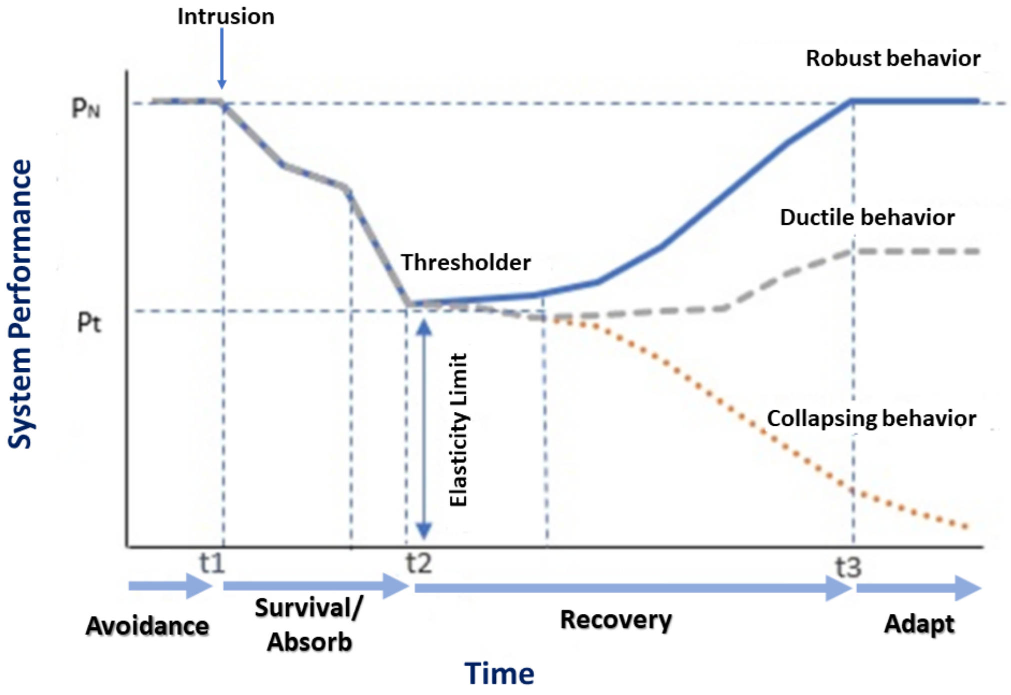


Figure 2.3: System behavior [57, 58]

2.3.3 Cyber Resilience Concept Map

The NAS identifies four stages of the event management cycle that a system needs to maintain to be resilient as shown in Figure. 2.1 based on our idea, resilience is not a liner stage, but it is a cycle, and temporal which needs to describe it as a cycle, in this definition I adopt it based on security criteria (CIA Triad) in CPS.

Four stages of resilience in CPSS with security approach: Making a plan and preparing the system aims to reduce potential damage, and it needs an adequate threat model and scenario. One of the most used and practical methods that many researchers have worked on is graphical security models like non-state space-based models: Attack Tree/Graphs, stochastic and state-space models: Stochastic Petri nets, checking models which can use mostly for attack analysis. These models will explain in the following sections as well. However, resilience is firmly connected to the time and performance of the system in the recovery phase; understanding the vulnerabilities and threats in a system is the initial phase. Among the studies on resilience metrics and evaluation and also solution, the is the most focused on the two first stages, plan and absorb, and there is a lack of attention to the stages of recovery that is a part of the goal of resilient systems. According to the definition of resilience in the systems and by critical infrastructure approach, the National Infrastructure Advisory Council considered three main components for resilience systems: Robustness, Resourcefulness, and Rapid recovery.

To consider the stages and phases of cyber resilience, a comprehensive analysis of threats, defenses, and their impact on systems is necessary. To facilitate a more effective evaluation of our work, I created a conceptual map of cyber resilience by referring to standard frameworks and references. This map provides a visual representation of the various elements and relationships involved in the process of achieving cyber resilience. [59][60]. This concept map is illustrated in Figure 2.4.

2.4 Chapter Summary

The objective of a cyber-attack is to compromise the integrity or authenticity of data or information, as noted by Bodeau [9]. Since attackers' behavior is not predictable, and it is impossible to create entirely secure systems, a combination of deterministic (non-deterministic) and stochastic methods is necessary to assess the performance of systems under attack. In this chapter, I have highlighted various methodologies and approaches to cyber resilience that have been employed in recent research. For our thesis, I have opted for model-based methodologies and a behavioral modeling approach. After researching the literature, I have selected the hybrid technique (Process Model-based and individual metric from metric-based) for measuring cyber resilience.

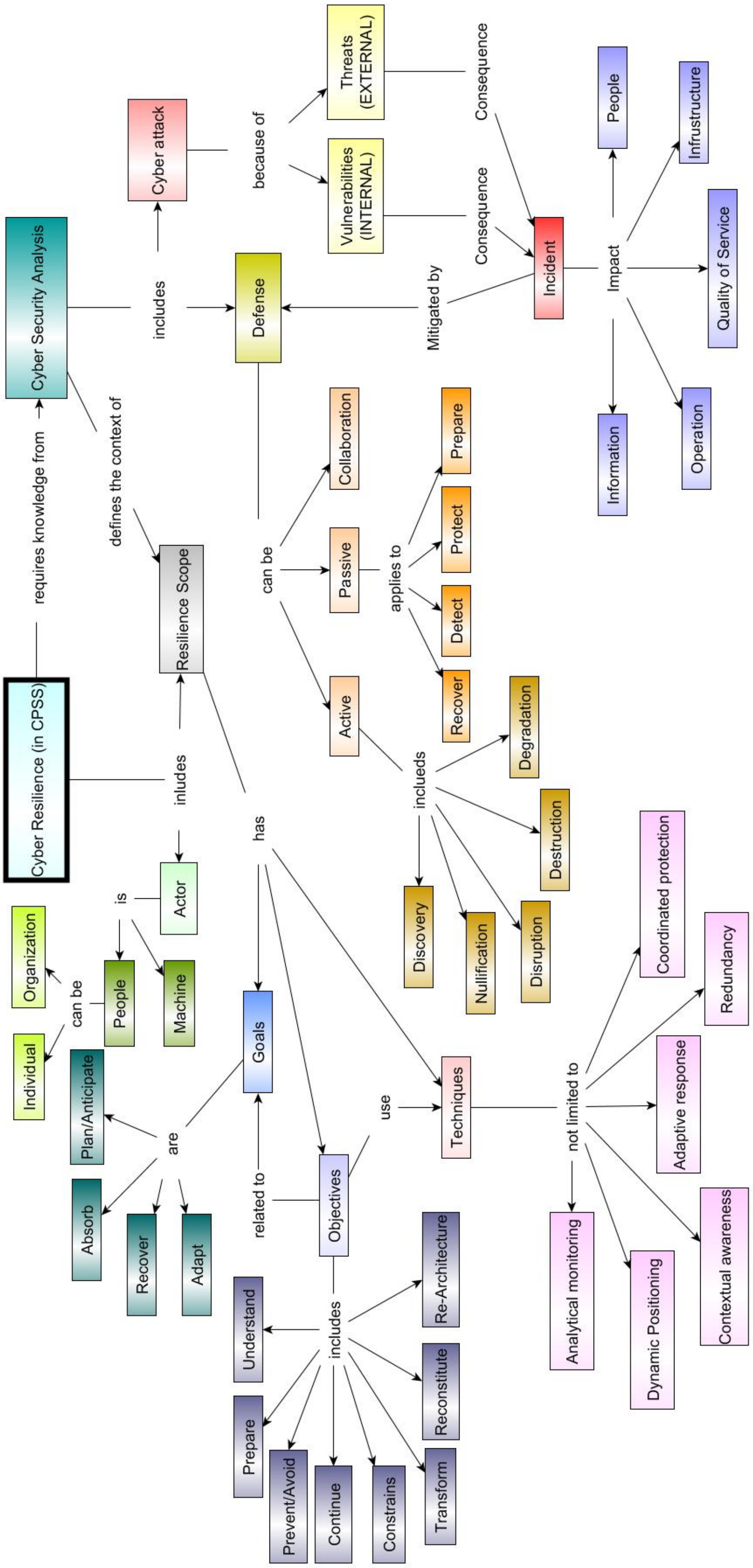


Figure 2.4: Cyber Resilience in CPSS Concept Map

3

Cyber-Security Analysis: CPN and GrSMs Representation and compatibility

Research is to see what everybody else has seen, and to think what nobody else has thought.
Albert Szent Györgyi (1893–1986)

3.1 Introduction

Ensuring the security of systems against attacks or unauthorized access is crucial for both academic and industrial research in the field of cybersecurity. This is particularly true for cyber-physical social systems (CPSS), which are vulnerable to a wide range of cyber attacks on a daily basis, exploiting various system vulnerabilities. Cyber systems are integral to the success of a wide number of corporate endeavors, as well as those in a variety of other sectors, including network communications, social life, and the lives of individual people. Conversely, insecure networked systems have the potential to cause sensitive information to be interrupted, leaked, or led to online fraud or attacks. Denial of service attacks, theft of intellectual property, breaches of credit card data, threats to national security, and problems with health care are only some of the widespread consequences of cyber attacks. Attacks on CPSS can take many forms, ranging from those directed at the system level to those directed at the network level and application level. [61] and target physical (e.g. CIs), cyber(e.g. information) and social assets (e.g. people).

The knowledge of existing vulnerabilities, and attack mechanisms together with modeling the behavior of cyber attackers assist security analysts to apply more efficient defense methodologies and mitigation strategies to secure a CPSS [62]. Security analysis models may provide information about threat analysis, anomaly detection, mitigation strategies impacts, risk assessments, etc, However, models for security analysis must describe how and where security breaches occur; they must describe attacks' behaviors impact on a system as well as defense and mitigation actions from incident response mechanisms. In addition, it is important that the model is able to be robust and carry on environmental and informational changes.

Among current models for evaluating cyber security, state-based and non-state-based graphical analyses are used vastly and successfully. Graphical Security Models (GrSMs) refer to conceptual models with tree-based or graph-based analysis methods, which have been intensive to enumerate potential attacks and possible loopholes or vulnerabilities to access and disrupt systems. GrSMs and other graphical representations tackle questions such as: How do cyber-attacks impact the behavior of the system? How graphical representation of the system behavior and attacker's behavior helps system designers evaluate each component's interaction and the impact of the selected defense strategy or response on the system's performance? In this regard, they are mostly used for describing the attack paths and goals in systems [63] and help to identify possible attacks on the system and relative defense solutions. As a promising tool for modeling complex systems, the Petri nets have been applied in security analysis and system risk assessment. Some works have applied Petri nets and Attack Trees together to analyze the system behavior[64][65].

Although tree-based models such as Attack Tree (AT) and their refinements, which will be explained in subsection 3.2.1, are powerful tools for security analysis, they suffer from some gaps and weaknesses such as using different notations in each extension, and lack of compatibility with other models. Also, they are not state-based and are not suitable for the system's performance analysis. Considering the ability of high-level Petri nets, in this chapter, we aim to define a set of rules for mapping all ATs refinements to Coloured Petri nets (CPN) to overcome weaknesses in ATs. Also, we model an attack scenario of a malicious insider attack in Supervisory Control and Data Acquisition (SCADA) systems based on ATs refinements (called Attack Countermeasure Tree (ACT)) in a CPN.

The remainder of the chapter is organized as follows: Section 3.2 outlines a literature review of cyber-security analysis and its graphical assessment techniques. Section 3.3 provides related works namely in GrSMs, Generalized Stochastic Petri Nets, and Coloured Petri Nets. Finally, section 3.5 summarizes the result of this work and conclusion.

3.2 Cyber Security Analysis

An adversary's capabilities and/or behaviors can be described in an attack model. In general, attack models aid in the discovery of design flaws in order to aid in the search for mitigation strategies and to promote an understanding of attacks. As a result, the first step in security analysis is to create appropriate attack models. Following that, the risk of potential attacks is estimated, and appropriate countermeasures can be defined by the system's goal, cost-benefit, and other criteria [66]. Research in graphical security analysis has led to a variety of models, each focusing on particular levels of abstraction. They represent attack, defense, protection, and response characterizations which can be measured by different attributes. These attributes or metrics are categorized as cost, meantime, probability, impact, risk analysis, and Return of Investment (RoI) [13].

In this respect, research and developing models for visualization using tree and graph-structured techniques are widespread. These models, which can call them generally be Graphical Security Models (GrSMs) [13] have many modifications and changes in their features and representations through these years, which have their own pros and cons for modeling systems. These models, which are mainly divided into Tree and Graph structures (Attack Trees and Attack Graphs) can use in different systems with different goals. Defenders can choose one or more of these models for modeling their security systems. However, their concepts are almost the same based on Attack Trees, which was first time coined by Schneier in 1999 [67].

Similarly, other models based on state-space, such as Petri Nets, have been recognized as valuable tools for security and system behavior analysis. Petri Nets are a mathematical and graphical representation developed by German mathematician Carl Adam Petri in the 1960s, which utilize the concept of event and condition to model the behavior of a system [68]. This formalism has shown promise in the design and analysis of discrete event systems, making it a valuable tool for security and system analysis.

3.2.1 Graphical Security Models

In recent years many extensions to the basic AT model have been built to enhance its modeling power and the flexibility of using the most used ones will be mentioned in this section. Models for security analysis must describe how and when security breaches occur, as well as the impact on the system, as well as the mechanisms, effects, and costs of system recovery, system maintenance, and defenses [69]

Initial AT was extended during the past years to fulfill the gaps and cover different goals. For instance, Defense Tree (DT) [70] models security scenarios by utilizing the defense concepts which means that for generating Defense Tree, possible countermeasures are added to each leaf node. The authors used two approaches quantitative and qualitative Risk management. The economic concepts included RoI and ROA (Return of Attack) are used for the measure. In this model, each event node considers a vulnerability node and adds a set of countermeasures to them, and then by economic indexes for countermeasures they measure the risk of that attack. The disjunctive norm form and aggregate AND gate are applied for events to have a direct connection to the parent node. Near to this concept in another work by Edge as his Ph.D. dissertation, Protection Tree (PT) introduced which assigned protection(countermeasure) events to nodes. It means that instead of using attack or vulnerability analysis, the protections for each event will be analyzed. This process should be continued from the leaf nodes to cover root nodes by protection [71]. In PT Attack nodes replace with Protection Nodes. This tree is a bottom-up tree also that starts to put protection for the system from leaf nodes till covers the node. For a visual representation of the ATs components and structure, the reader is referred to Table. 3.1.

Table 3.1: Attack Tree /and its refinements Structure

Components	Definitions	Other Terms	Represent
Root Nodes	The first node (Upper level) in the structure which depicts the ultimate goal up to the aim of the model can be the attacker´s goal or the defender´s one. It is called a parent node which can be reached via a directed path.	Top event; main goal; main consequence, objective or action.	The top node on the Trees.
Intermediate/ sub-goal Nodes	It can be interpreted as a consequence of previous events and cause of the next ones in inductive and deductive ways.	Intermediate goals	Middle nodes
Leaf Nodes	The last nodes in the structure which cannot refined anymore. They display an atomic component.	Primary event, initial attack, protection, detection, mitigation.	Atomic nodes the lowest part of the trees
Edges	The node´s link and thusly determine relation between the events. In some models,edges may have special semantics and detail a cause-consequence relation, a specialization or some other information.	Arc, arrow, or line	Arcs
Combiners	Connectors specify more preciously how a parent node is connected with children nodes. A connector might be a set of edges connected by different notation and reparations.	Connectors or logical gates	AND,OR, k-of-n, Priority AND
Attributes	Attributes represent aspects or properties that are relevant to quantitative analysis.	Metrics	An attack impact , cost, risk, probability

Another extension of ATs is called Attack Response Trees (ART) [72]. ART is built to make it possible to consolidate possible countermeasures (response) actions against attacks and also to detect invasions due to false intrusion in the system while considering its current state of it. It is designed offline by experts in computing assets like SQL servers. Using attack consequences instead of attack in ATs, provide the advantage of getting rid of illustrating numerous attacks that have the same response. The purpose of ARTs is to define all possible combinations of attack consequences which are causes of destruction in the systems. A major goal of an ART is to probabilistically verify whether the security property regarding ART's root node has been violated, given the sequence of 1) the received alerts, and 2) the successfully taken response actions.

The attack trees approach is goal-oriented and does not represent a comprehensive model for the analysis of network vulnerability [73]. Roy and et. al., [74] introduce another extension of ATs that assigns countermeasures in the tree. It has a similarity to DT, but countermeasures are not only related to leaf nodes, they can be in any child nodes, and by categorizing countermeasures detection and mitigation be considered separately. He called it Attack Countermeasure Tree (ACT) and used it for analysis of Cyber security in the SCADA system. In this tree, both attacks and countermeasures are modeled precisely without taking states into account (in comparison to ARTs where states are considered) because they claimed that is less expensive. They used minimum cut sets in ATC to automate the generation of Attack scenarios. The goal of this tree is to select the optimum defense for the system by providing an algorithm based on both repeated and non-repeated events in the tree. In this case, the probability of attack (root node) is calculated by considering the attributes such as cost, system risk, RoI, and RoA. They implement the ACT module in the SHARPE software package.

Kordy [75] introduced a new concept called Attack Defense Tree (ADT), which decorated AT by Defense nodes not only in Leaf level but in any levels of the tree and provides a tool to generate the ADTs named ADTools [76].

Kumar et al. [77] proposed another extension of AT, which analysis both the security and safety of the system named Attack Fault Tree (AFT). This model has the advantage that analyzers can consider two situations of the system in a single model. Attack Defence Diagram [78] has created the attack-defense diagram formalism extending the attack defense tree with trigger and reset gates, which allow expressing temporal behavior.

Attack Net [79] introduced by McDermott in which the places of a Petri net represent the steps of an attack and the transitions are used to capture precise actions performed by the attackers falls in the first class of methods. While attack structure captures the steps of an attack and their interdependencies.

For solving the scalability problem in AG, Hierarchical Attack Representation Models (HARM) are introduced in [80]. The same authors in [13] have an accomplished survey about the usability and practical applications on GrSMs which they produced a state of the art in terms of networked system security analysis in regards to efficiency, application of metrics, and availability of tools.

3.2.2 Petri Nets

Petri net as a graphical model for modeling systems has four main elements: Places, Transitions, Arcs, and Tokens. A bipartite graph with two types of nodes (places and transitions) graphically represents a Petri net model. Several classes of Petri nets have been proposed, covering different goals, such as place/transition nets, timed nets, and Coloured Petri nets, to mention a few.

Places are represented as circles or ellipses and can be associated with the static part of the model representing states or resources. On the other hand, transitions capture the dynamic part of the model allowing explicit models of concurrency and synchronization, and are represented by bars, squares, or rectangles. These two elements represent the first concept of the Petri nets. As a bipartite graph, an arc can connect nodes (places or transitions) of different types. It is noticeable that the connection between two places or two transactions with a direct arc is impossible. Figure 3.1 shows a Petri net with two places marked with one token, and a transition enabled to fire.

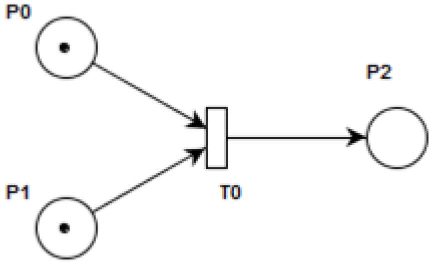


Figure 3.1: Petri net: T0 enabled for firing

A Petri net models the dynamic behavior of a system concerning its states and state changes by tokens in each place. A place can have a zero or a positive integer number of tokens. Tokens are a fundamental concept for Petri nets in addition to places and transitions. The condition of a system is determined by the presence or nonexistence of a token in a place associated with regular or false, for instance. Marking in a Petri net is an assignment of tokens to the places of a Petri net. Tokens reside in the places of a Petri net. The number and position of tokens may change during the execution of a Petri net. The tokens are used to illustrate the execution of a Petri net. Two rules regarding the flows of tokens describe as Enabling and Firing rules flow:

1. Enabling rule: A transition "t" is enabled if each input place P of t contains at least the number of tokens equal to the weight of the directed connection arc from p to t.

2. Firing rule: The enabled transition can fire. When a transition fires, token(s) from the input place(s) are removed and tokens are generated in output place(s), according to the weights of the associated arcs.

In the following, some important characteristics of Petri Nets for modeling the behavior of systems are briefly presented, which will be used in terms of attack trees translation to Petri nets.

Sequential Execution: It is used for describing "if-then"logic (the same logic for the sequence of events in attack trees) as shown in Figure. 3.2

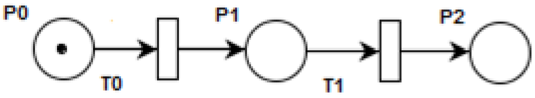


Figure 3.2: Petri nets: Sequence

Concurrency: When multiple transitions are fired simultaneously. For instance, in Figure 3.3, T10, T11, and T12 are enabled to can be fired concurrently.

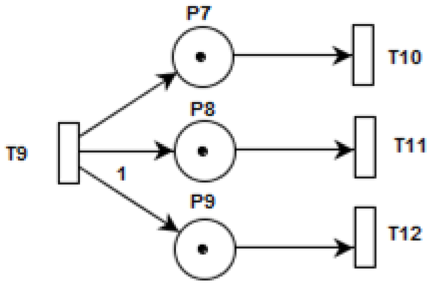


Figure 3.3: Petri nets: Concurrency

Conflict: If a place in a PN model is connected to several transitions, those transitions are said to be in conflict.

Synchronization: A synchronization between different processes can be modeled by a transition receiving arcs from different places, as illustrated by T2 in Figure. 3.4.

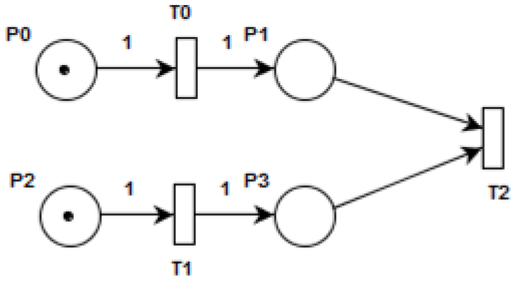


Figure 3.4: Petri nets: Synchronization

3.2.3 Time Concept in PNs

Petri nets are able to describe the logical structure of the modeled systems, but for responding to the need for the temporal performance analysis of discrete event systems, the time notion has been added, and Timed Petri nets were proposed [81]. Timed PNs are useful for performance evaluation and can be implemented using stochastic or deterministic timing [82]. Stochastic timing is helpful in model events where time is important, and all the enabled transitions in the model are equally as likely to occur. Constant timed PNs are useful to time-dependent model events where transitions occur after some predetermined time.

In this work, we applied the time concept for the analysis of attacks and defenses (cyber security) translated from GrSMs. Generalized Stochastic Petri Nets (GSPN) add both immediate and deterministic transition times. Thus a GSPN can be described uniquely by the 5-tuple: GSPN (P, T, I, O, W) where T can include both timed and immediate transitions, and W is a set of rates/ weights. PN simulation tools allow the assigning of rates for the individual negative exponential transitions, as well as assigning weights to non-timed (immediate) transitions. These weights then enable probabilistic simulation [83].

3.2.4 Generalized Stochastic Petri Nets

This class of PNs is proposed by Balbo and Conte to solve the limitations regarding Stochastic Petri nets (SPN), supporting performance evaluation [84]. A GSPN is an extension of an SPN by allowing infinite transition firing rates, comprised of two types of transitions: Timed transitions, which are associated with random, exponentially distributed firing delays, as in SPNs, and Immediate transitions, which fire in zero time with firing probabilities. The graphical representation of immediate transition in GSPN uses segments and the timed transition is represented by white or black rectangular boxes. Analysis of GSPNs: it is complicated because of immediate transitions which due produce multiple simulations events in the process that describe the time behavior of a GSPN and possibly an infinite number of events in a finite-time interval. It can be considered as a continuous-time stochastic point process (SPP).

3.2.5 Coloured Petri Nets

Coloured Petri Nets is a modeling language aimed at systems in which concurrency, communication, synchronization, and resource sharing play an important role. Coloured Petri Nets provide structured tokens in the form of so-called colors and provide a significant increase in the expressiveness and compactness of models. Coloured Petri Nets extend Petri nets with data types, functions, and modules to obtain a scalable formal language suited for modeling concurrency, synchronization, and data processing.

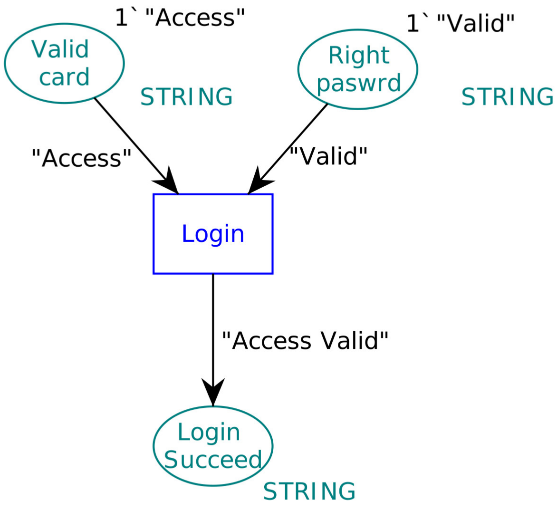


Figure 3.5: Coloured Petri Nets Model: Login Event

In a Coloured Petri net, each place is associated with a color set (type) that specifies the kind of data related to the system´s properties/states, or information that may be stored in the place, as illustrated in Figure 3.5. Transitions, on the other hand, represent events or actions. An arc connects a place and a transition, and it determines the dependencies between these nodes, may contain values, and can have defined conditions. A state of Coloured Petri nets is called marking. A marking describes how colored tokens are distributed among the places in a net at a specific point of the net execution. A token has a color (a value) from a color set, and a token can only be present in a place if the color is from the defined color set in the place. A place may have several tokens with the same color.

3.2.6 Analysis Petri nets models by behavioral properties

In this work, we study the proposed models by the behavioral properties of the nets. This type of analysis depends on the initial marking and focuses on Reachability Graph (RG). Reachability analysis studies the dynamic properties of any system [85]. "A marking M_n is reachable from M_0 if there exist a sequence of firing that transforms M_0 to M_n" [85]. This is assessed for each Petri net state, finding states that might be attained through a feasible compromise.

3.3 Related Works

Petri net as a promising tool for modeling complex systems has been applied in security analysis and system risk assessment. But by increasing the states of the system, reading Petri net-based models is getting more complicated. Some works applied Petri nets and Attack tress together to analyze the system.

Linyuan [86] propose a model for modeling and analysis of network security of Software Defined Networks (SDN) by using the Place Transition class of Petri nets for modeling of Network structure and state transitions and Attack Tree for analysis attacks on the network. They have used the STRIDE method to build up the attack tree. In the realm of computer security, STRIDE is a threat modeling framework used to identify potential threats. It stands for Spoofing, Tampering, Reputation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege. Each of these categories represents a different type of threat that a system may be vulnerable to, and by considering each category, security professionals can better assess and address potential security risks.

Attack nets [87] and Stochastic Activity Network(SAN) [88] borrowed the Petri net concepts and model for applying in the ATs. Codetta [89] explains how AT and Petri nets can be complementary in terms of security analysis. Pudar [64] proposed a new model and tool to analyze the security of the system by translating Petri nets from Attack trees to be readable, called PENET. In this model, they used AND, and OR logic in ATs and introduced PAND or Propriety AND for sequence events. In similar work by considering intrusion detection mechanism, a set of translation rules from AT to GSPN is used to analyze SQL injection impacts on systems by Industry 4.0 (I4.0) approach [90].

Additionally, Stochastic Petri Nets (SPN) are successfully applied for power grid security analysis [91]. The study focuses on evaluating the reliability of smart grids under topology attacks and countermeasures. The metric for evaluation is based on reliability and includes Transient Analysis: Mean Time to Distrust (MTTD) and Mean Time To Fail (MTTF).

For solving the problem of state-space explosion in security analysis, the hierarchical method is applied to model and quantitative predict for software security based on Stochastic Petri nets [92]. For overcoming the same drawback in PNs, another hierarchical method is introduced as new construction of PNs [93]. This method includes two levels PNs; Low-level PNs for describing different security domains, and high-level PNs for abstraction level. Then by model description language, the explanation process is described. In this work, defense or intrusion systems are considered in the method.

Considering command and control systems resilience in CPS, in a study by Pflanz and Levis [94], a quantitative approach is proposed to measure the expected resilience based on the system's architecture. This work does not consist of the avoidance and recovery phases in resilience evaluation. They evaluated the survival phase by elementary Petri Nets and used three main attributes of resilience; capacity and flexibility, and tolerance.

Coloured Petri Netss have been applied effectively in security analysis and anomaly behavior modeling. For instance, Jasiul et al. [95] utilized CP-nets for tracking malware in web services and detecting them. In another study, Yang and Xiaoyao [96] analyzed a security protocol named Andrew using CP-nets. They applied a high-level variant of Petri nets called CP-Net with the CPN Tools. This approach overcomes the state space explosion problem. Liu et al. [97] also employed CPNs to model components and information flow in the Advanced Metering Infrastructure (AMI) architecture of smart grids. They highlighted the advantage of CPNs in describing data types and complex data manipulations by attaching a data value, known as token color, to each token.

Timed Coloured Petri Nets is utilized to verify Temporal Role Based Access Control (TRBAC) [98]. TRBAC model is used in designing and implementing of security policies in large network systems. To give CPN model the capability to model security properties and be compatible with existing formalism, a semantic interpretation of CPN components called "Secure Coloured Petri nets- SCPN"is introduced [99]. For mitigating complexity, hierarchical CPN is applied and the work´s focus is on information flow security. CPNs are applied for modeling the behavior of RESTful services and their composition and also are used to verify relevant composition behavior properties [100].

General and time interval Coloured Petri nets are used for modeling and executing Penetration testing on Time Of Check to Time Of Use (TOCTOU) [101]. The TOCTOU is a refinement of the McDermott work called attack nets to provide a level of sufficient details for modeling attackers' behavior.

The Coloured Petri Net (CoPNet) modeling approach was proposed by Bouchti et al. [102] to align with the purpose of this work, which aims to extend attack trees with new modeling constructs and analysis approaches. However, despite their good notation descriptions for mapping attack trees to CPNs, their proposed model suffers from complexity and may hinder its assimilation and follow-up. Additionally, it lacks support from simulation and validation methods, and its notations and logical gates from attack tree extensions to CPN are not well-structured based on existing attack tree models.

Such GrSMs are summarized and depicted in Table 3.2, Table 3.3, Table 3.4, and Table 3.5.

Table 3.2: GrSMs: Attack Tree

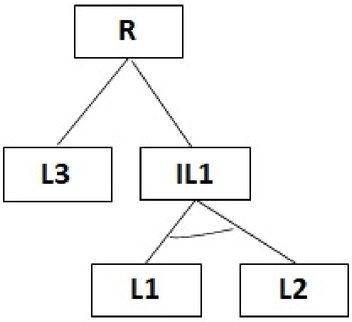
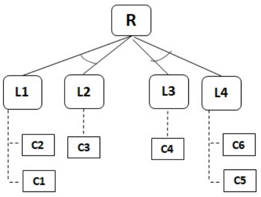
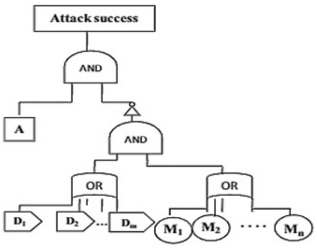
GrSMs	Attack Tree
Graphical Presentations	
Logical Gates	AND /OR
Attributes (Metrics)	Cost, Risk, Resistance[103], Regression[70]
Translated to PNs	Y (PN, GSPN)
Coined by	Schneier [67]
Applied in	Privacy protection, SCADA, Social Engineering[2], Mobile system[7]

Table 3.3: GrSMs: DT, ACT

GrSMs	DT	ACT
Graphical Presentations	 R L1 L2 L3 L4 C2 C3 C4 C6 C1 C5	 Attack success AND A AND OR OR D_1 D_2 D_m M_1 M_2 M_n
Logical Gates	AND/OR	AND/OR/k-out-of-n
Attributes (Metrics)	Cost, ROI, ROA [70]	ROI,ROA [102]
Translated to PNs	N	N
Coined by	Bistalli [102]	Roy [74]
Applied in	Select set of countermeasures /attacks [8]	Split-protocol[9]

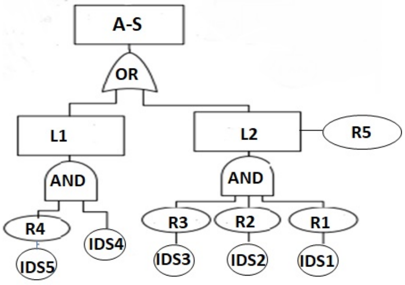
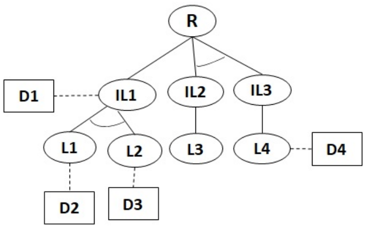
GrSMs	AR	ADT
Graphical Presentations	 A-S OR L1 L2 R5 AND AND R4 IDS4 R3 R2 R1 IDS5 IDS3 IDS2 IDS1	 R D1 IL1 IL2 IL3 L1 L2 L3 L4 D4 D2 D3
Logical Gates	AND /OR	AND/OR
Attributes (Metrics)	Probabilistic Success /failure [9]	Impact, cost, probability (attack /defense)
Translated to PNs	N	Y (GSPN)
Coined by	Zonouz [9]	Kordy [75]
Applies in	Security game attacker/defenders [9]	Cyber-Security in CPS [80]

Table 3.4: GrSMs: AR, ADT

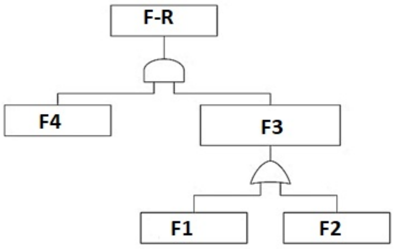
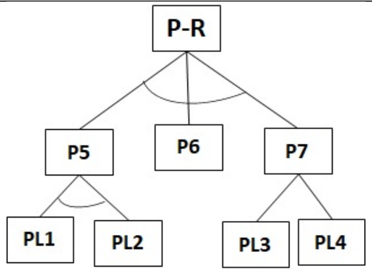
GrSMs	FT	PT
Graphical Presentations		
Logical Gates	AND/OR, Priority AND (PAND) gate / Dynamic gate: Sequence Enforcing (SEQ)	AND/OR
Attributes (Metrics)	Mean time to the occurrence and the corresponding rate for each event	Probability, cost, Intrusion Detection and Prevention
Translated to PNs	Y (GSPN, PN, CPN)	N
Coined by	As security analysis: Kumar [77]	Edge [71]
Applies in	Safety, IDS (software fault analysis), cyberattack [71]	DDoS [78]

Table 3.5: GrSMs: FT, PT

3.4 Applied Tools

In this section, the main tools that are used for editing proposed GrSMs and CPN models in this thesis are described.

3.4.1 ADTool

The ADTool [76] provides security consultants and academic researchers and supports the attack-defense tree-based security analysis and risk assessment processes. It incorporates the development of security models and their quantitative analysis, two essential modeling facets. Attack-defense trees can be formalized as attack trees, protection trees, and defense trees. So all of the aforementioned formalism can be used to automate and facilitate the use of the ADTool. The ADTool has adopted the bottom-up technique for evaluating the characteristics of ADTrees.

3.4.2 GreatSPN

GreatSPN2.0 [104] is a software package that uses Generalized Stochastic Petri Nets and their colored extension, Stochastic Well-formed Nets, to describe, validate, and evaluate distributed systems. The tool offers a user-friendly environment for experimenting with timed Petri net-based modeling methods. It employs efficient analysis algorithms, allowing it to be used on complicated applications. GreatSPN2.0 is made up of many distinct programs that work together to build and analyze PN models by sharing files. Various analysis modules in a distributed computing environment can be performed on various machines using network file system capabilities. GreatSPN2.0's modular structure allows for the addition of new analysis modules as new research findings become available. I used GreatSPN to edit my GSPN model.

3.4.3 CPN Tools

CPN Tools [105] is a high-performance computer tool for creating and analyzing CPN models. CPN Tools ables us for creating, editing, simulating, and analyzing hierarchical Coloured Petri nets (CPN or CP-nets). CPN Tools can be used to simulate the behavior of the modeled system, verify properties using state space methods and model checking, and perform simulation-based performance analysis [106].

CPN Tools is intended to replace Design/CPN, a popular CP-net software package. CPN Tools can be compared to other Petri net tools such as ExSpect, GreatSPN, and Renew, all of which are described in the Petri Nets Tool Database. In 1989, Design/CPN was released with support for editing and simulating CPnets. Since then, considerable effort has been expended in developing efficient and advanced support for simulation as well as generating and analyzing full, partial, and reduced state spaces. While the Design/CPN analysis components have steadily improved since 1989 [107].

3.5 Chapter Summary

In this chapter, we presented a state-of-the-art background of graphical security analysis models (GrSMs and PNs classes). These methods and their tools can be state-based or not. In this chapter, we provided different presentations of ATs and their refinements as well as Petri nets classes to show the possibility and compatibility of these two graphical assessments. In chapter 5, we elaborate more about the comparison of these models and the possibility of being translated to each other. We argue that PNs are a promising formalism to be translated from and to ATs. This PNs' strength brings the opportunity to define and show cyber resiliency in CPSS.

4 Cyber Physical Social Systems

If we are ever going to see a paradigm shift, we have to be clear about how we want the present paradigm to shift.

Gary Lawrence Francione (1954–)

4.1 Chapter Overview

The novel paradigm in Cyber-Physical System (CPS) is called the Cyber-Physical-Social system (CPSS) [1].

A CPS integrates computation, communication, sensing, and actuation with physical systems to fulfill time-sensitive functions with varying degrees of interaction with the environment, including human interaction [108]. The CPSS introduced changes in the relationship between humans, computers, and the physical environment. As a new research frontier, CPSS integrates ubiquitous computation, physical processes, social agents (Social IoT [109], social networks), communication, and effective control [17]. The widespread development of CPSS, and its essential role in industries, businesses, organizations, and individual's daily life, can be seen in personalized product productions [110], smart cities [111] [31, 112], intelligent transportation [113], and artificial societies, to mention a few. The key techniques for designing CPSS are combinations of CPS and Cyber Social Systems (CSS) including device management and discovery, human-computer interaction, seamless mitigation, technologies of a heterogeneous network, social computing, context awareness, and management, user behavior-based proactive services [17].

The CPSS by emphasizing human society and its interaction with other components of the system aims to gather and organize resources in a semantic manner that can be used for machines and humans[18]. The CPSS obtains data from virtual and real entities including cyber, physical, and social systems through sensors, mobile crowds, and social networks and aims to provide information for users to support their decisions and enhance their performance [113].

This chapter reviews several streams of research on CPSS definitions, as well as proposed or used frameworks in different domains. Most past review works on CPSS have largely focused on the conceptual framework and meta-model for CPSS, but this work seeks to survey the state of the art of CPSS to define a uniform definition, formulate a taxonomy of CPSS and challenges, opportunities, and open issues in CPSS.

This review contributes to providing the following information for researchers and developers:

i . A review of published papers/established works in CPSS represents the advancement in the most highly cited and important CPSS-based works.

ii . Discuss social entities in CPSS and human roles in similar concepts such as the Internet of People (IoP), Social IoT (SIoT), and Cyber Physical Human in The Loop.

iii . Propose a uniform definition for CPSS.

iv . Provide a taxonomy of this new CPSS paradigm.

v . Identify and classify open issues and challenges corresponding to CPSS as well as opportunities for rebooting products and services by adding social computing concept in their business model.

The remainder of the chapter is organized as follows; In 4.2 I describe the CPSS paradigm and its relationship with CPS and IoT, in 4.3 I respectively define the social entity in CPSS, and verify the human role in CPSS, and finally, in sub-section 4.4 I provide a definition of CPSS and following it I propose our CPSS taxonomy. In Section 4.5, I represent open issues and challenges in CPSS as well as its study domains. Next, in Section 4.6, I provide a reference model of the human awareness model which later in modeling human behavior I will refer to that. Finally, Section 4.7 summarizes the result of this work.

4.2 Cyber Physical Social System paradigm

Having initiated the Internet of Computers (IoC) to form cyberspace, cyber systems can work in parallel with physical systems, bringing more intelligence to physical space. The movement from desktop information to the Internet, linked information, and cloud computing has changed the relationships among entities. As a result, the integration of High-Performance Computing (HPC) in daily activity and products paved the way for smart factories, smart cities, and many smart productions. Also, it lead to considerable changes in business models which might be viewed as shifting traditional business platforms to online and web-based platforms, such as YouTube, Instagram, and communications through video conference platforms such as Google Meet, Zoom, and Virtual communities [114]. Thanks to social computing [115], socials with basic knowledge of information technologies have integrated communication technologies and applied their applications to their daily lives, businesses, and communities.

All these technologies and developments are grounded in a paradigm such as the Cyber-Physical System (CPS) [116]. A CPS was coined with two-dimensional space; physical and cyber as "an orchestration of computers and physical systems. Embedded computers monitor and control physical processes, usually with feedback loops, where physical processes affect computations and vice versa." [108].

Although all the traditional CPS are designed for human interest, recent studies have found the importance of the human role in the context of CPS, and new terminology has been introduced called Human-in-The-Loop (HiTL) [117–119]. Such a concept includes works on Human-Machine Interfaces (HMI) within I4.0 or natural Human-Machine Interfaces (NHMI) in human gesture recognition systems and Cyber-Physical Production Systems (CPPSs) [120].

Nevertheless, HiTL CPSs have some issues describing the human role in the traditional CPS framework and its human factors such as cognition, intents, emotions, behavior predictability, and human motivation and performance. Therefore, considering HiTL in CPS, there is a need for another discipline which Jirgle [117] calls "Human Reliability Assessment (HRA)", and its critical area is human behavior modeling and prediction. Therefore to overcome this issue and based on a new technology concept, Physical-Cyber-Social (PCS) computing [17], a novel paradigm in the cyber system domain, have been introduced called Cyber-Physical-Social Systems (CPSS) or Physical-Cyber-Social Systems (PCSS) [32].

The CPSS expands the CPS dimension by combining social systems. In this sense, the CPSS has changed the relationship between humans, computers, and the physical environment. The CPSS, the first time coined by Wang in 2010, is the fusion of four elements including Physical, Information, Cognitive, and Social domains [5]. A social system is an independent system with different characteristics, while considering its interaction with other components of CPS, the social system should be equivalent to other systems (physical and cyber) in terms of their interaction with other components. The interaction of each component of CPSS can be defined as the Physical-Social (PS), the Physical-Cyber (PC), and the Cyber-Social (CS), as shown in the Figure. 4.1.

In other words, CPSS is an extension of CPS considering its integration with Cyber-Social Systems (CSS), as shown in Figure. 4.2, and has three dimensions cyberspace, physical and human social spaces, and so-called hyperspace [29]. Cyberspace or artificial world encompasses the social domain and human features such as cognition, physiology, experience, decision, behavior, mental and environmental perception, human participation, and interaction to facilitate social users sharing and exchanging data through the close association with cyberspace and the physical world [121]. In this sense, the interaction within the CPSS includes social characteristics and relationships between humans and other social communities/societies. This means that putting the human in the system introduces another dimension of mental space consisting of human knowledge, mental capabilities, and sociocultural elements [1]. In this way, the CPSS is constituted by the physical system, its social system including human-to-human interaction, and the cyber

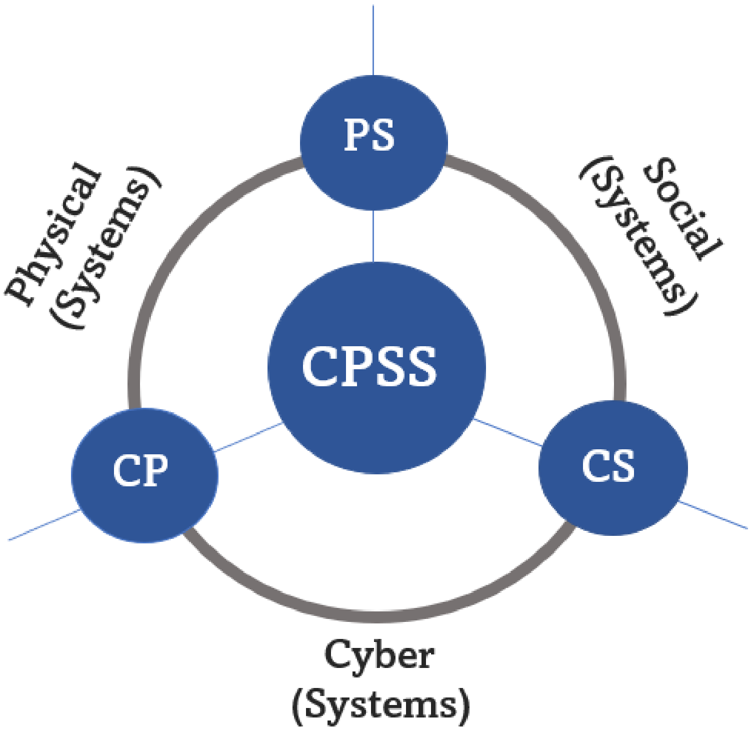


Figure 4.1: CPSS Dimension

system that connects both.

One of the main purposes of the CPSS is to use social behavior data and relationship analysis such as sentimental analysis to provide high-quality, proactive, and personalized services for humans [122]. The CPSS receives human social commands and reacts physically as traditional control systems but with cyberspace interaction. In CPSS, social computing is a supporting technology that can discover patterns of human behavior, prediction, and management.

The CPSS is a complex and multi-objective system and through its heterogeneity of networks and complication computation, the traditional mathematics algorithms and computing techniques are insufficient to control and manage this system. Withal, considering the speed and accuracy of high-performance computing, they can address most of the issues in CPSS [123].

Figure 4.3 outlines the evolution of physical and social systems by integrating cyber systems. From this figure can be seen that the abstraction and data volume increase since the dynamic and unpredictable components augment the system.

4.3 The Social Entity in CPSS

In recent years, the social system got more attention from both the business point of view and research in the CPS realm. Some of the social system applications are e-businesses,

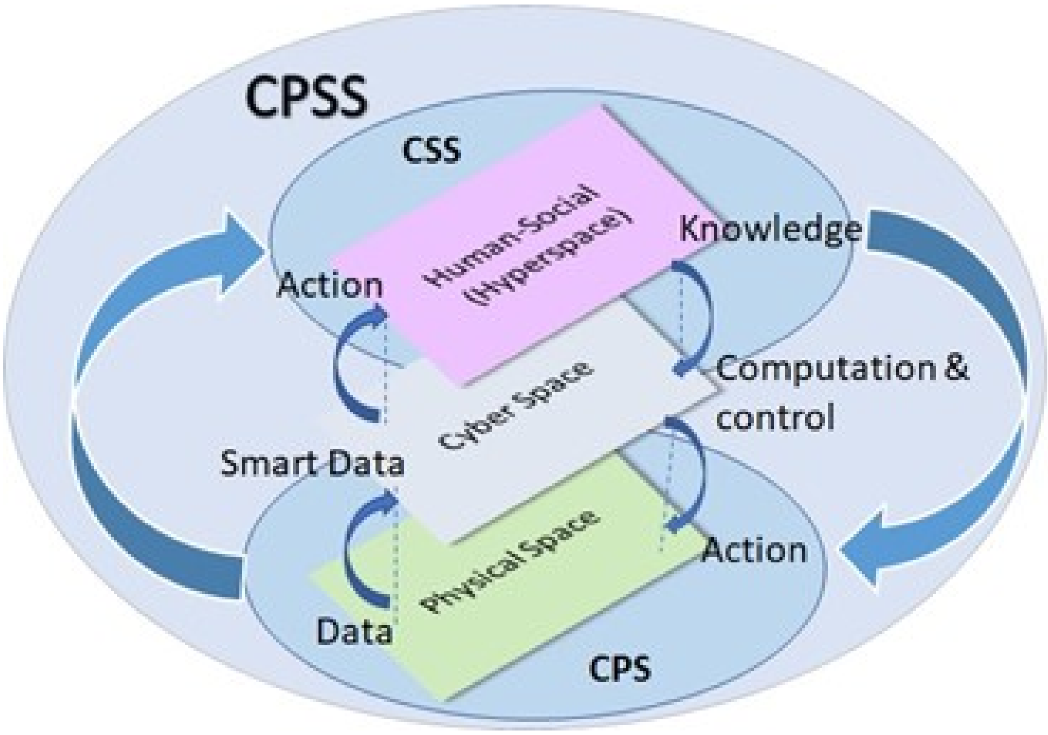


Figure 4.2: The Cyber Physical Social System (CPSS) Ecosystem

serious games- which are adaptable with ‘user’s characteristics [29], and social network applications. In these systems, individual humans’ behavior interferes with the system’s responses and tasks; the group mindware and practice can change the systems’ regular functions. The widespread use of sensor-enabled [124] smartphones and online social networks and tighter interaction between them and their users means an increasing number of people sharing information, in near real-time about the ambient environment and personal information. Social computing applies Information Communication Technology (ICT) with social context to provide a platform for human communication and exchanging experiences. Social computing’s goal transcends general personal computing, facilitating collaboration and social interactions, it spotlights social intelligence by capturing social dynamics, appointing virtual social agents, and managing social knowledge [125]. To trace back the history of social interaction with machines like computers, the first discussion was initiated in the work by De [29], in which the expression “As we may think” introduced a new term called “Memex” which means Memory and Communication device. Then, “the computer as a communication device” in the 1960s led the researchers to the concept of social computing in two main areas of technological and computation techniques or “groupware”. The social entity in Multi-Agent Systems (MAS) and HiTL-CPS approaches is any agent able to interact with other ones, also putting humans in the ‘loop’ as an embedded system and their environment [126]. The cyber-Physical network enables the user to interact and connect to the physical world which is mapped

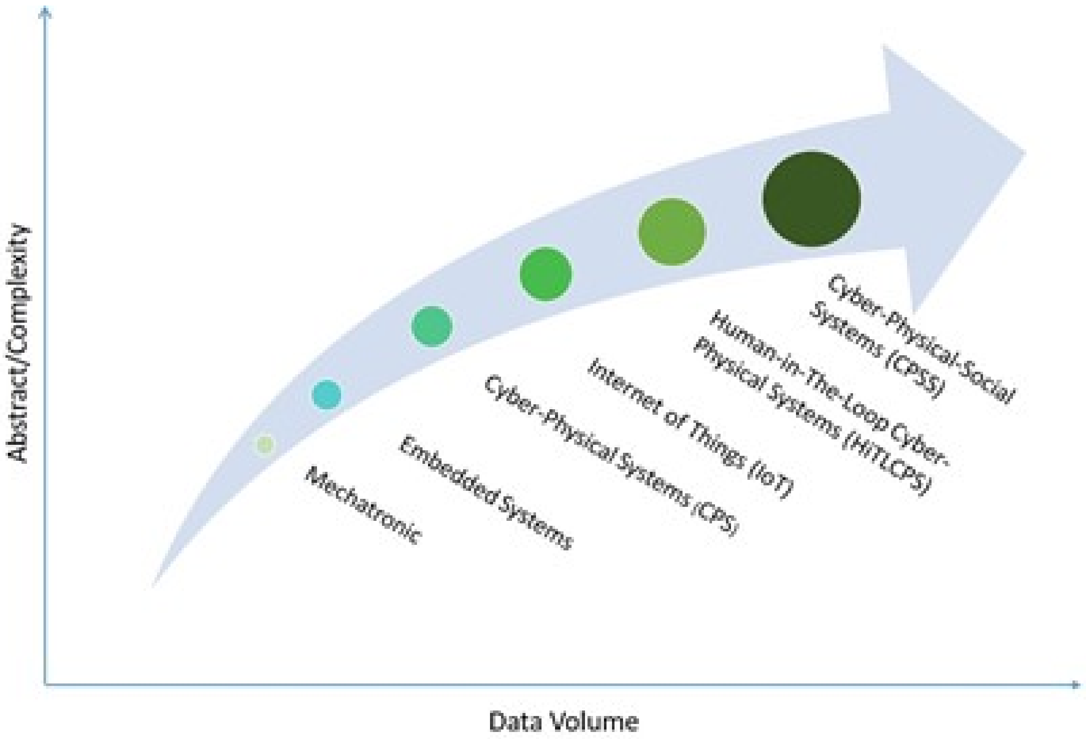

Abstract/Complexity
Data Volume
Mechatronic
Embedded Systems
Cyber-Physical Systems (CPS)
Internet of Things (IoT)
Human-in-The-Loop Cyber-Physical Systems (HiTLCPS)
Cyber-Physical-Social Systems (CPSS)

Figure 4.3: Physical and Social Systems Evolution

into cyberspace. In comparison, defining the social system as not being an external agent and pushing human-social- integration further in the CPS conducts the idea of CPSS. In CPSS, social systems are independent agents which integrable with physical and cyber systems, therefore a cyber-physical social network with its logical topology incorporates social entities such as individuals and special-interest communities, activities, and services [127]. Social dimension in CPSS to focus on social factors and conceptual evolution regarding automated production systems' sociability [3] by integrating social entity in CPS. Human society, as an entity in CPSS via social sensing, is to manage human activities and social occasions by providing supervision, coordination, restraint, and other effects, by addressing different domains such as educational, behavioral conventions, legal regulations, social administration, public services, and other issues. The CPS and the CS integration services include the user´s behavior pattern, proposing a proactive service, providing a pervasive environment for humans, sense the social phenomena [6, 128]. Human features such as experience, decision, and data in interaction but in the social concept, the better categorization described by Haouzi [116] into three main. They are Social Human-In-The-Loop Cyber-Physical Production System (Social-HIT-CPSS), Social Interactions Based on Peer-to-Peer Communication Interfaces, Social-Network Services Based Approach as a Media for Social Interaction, Human-Inspired Social Relationships-Based Sociability Model: From Social Integration to System Integration.

4.4 CPSS Definition, Models and Aspects

The development of computing systems has provided an opportunity to embed social systems into intelligent systems. Recently, social notions imported to different domains of studies created new terms such as the Internet of People (IoP) [129]. Also, social aspects have been introduced in several works [130] [126] to integrate social networks with the IoT. In this regard, a new term “smart community” is formed which basically close to CPSS but it emphasizes social aspects and social networks [131]. In a review by these authors [131], from 2019 to June 2021, the CPSS term was used in 114 pieces of research and technical papers in different publishers, including Elsevier and IEEE. The search strings were “Cyber-Physical-Social Systems” and “Socio-Cyber-Physical System”. According to a systematic review by [30], the number of papers related to CPSS was approximately 431 from 2001 to May 2020.

4.4.1 CPSS Definition

In the CPSS, the human role should be well defined, and when it is related to shareable resources, the human is not an individual entity; hence, it should be considered in the social optima [111]. For instance, this can be seen in scheduling traffic in traffic information management, energy efficiency in energy management, and other frameworks such as e-business and social networks, smart tourism, and hospitality where people access the same information and share their data on defined platforms. Similarly, the human role as a trainer of smart systems as well as social systems is an important point that needs to be studied.

However, the social entity in CPSS has an arguably different role from those traditionally considered by CPS and smart systems, insofar as they are not concerned with CPSS as much as a certain social entity. Likewise, the social system is an integrated element in the CPSS that changes the system´s design and analysis by providing human-human interaction in cyberspace. More recently, several studies have also addressed social space integrity with cyber and physical systems and introduced new concepts mainly as IoP, Cyber-Physical-Social Thinking (CPST), and Social Internet of Things (SIoT). The related definitions are provided as follows:

Internet of People (IoP): "Personal mobile devices may act as their users would do when communicating, managing data, or computing. Indeed, IoP is device-centric, as users’ devices play an active role in network algorithms, as today’s core nodes are active elements of the Internet algorithms."[129].

Cyber Physical Social Thinking (CPST): A broader vision of IoT by merging the thinking space into the CPS and highlighting the importance of cognitive intelligence and social organization [18]. Thinking space refers to the space created by human thoughts and thoughts of smart things.

Social Internet of Things (SIoT): This idea is based on a “social network of intelligent objects” [12] and navigating a community of objects that are connected together [132]. The main objective comes to "publish information/services, find them, and discover novel resources to better implement the services also through an environmental awareness"[130].

System designs and models for social-integrated systems must describe human features that compromise experience, decision, and data including human participation and interactions in social systems. The difficulty, of course, is determining the human role in these systems. For instance, in **CPSS**, “humans are full members of it, sometimes they full fill role of resources in providing information, knowledge, services, etc. Another time they are users of the CPSS in consuming information, knowledge, services, etc.” [24]. Because of confusing definitions of human roles in each of the mentioned paradigms I identified common and different features in the human role in newly mentioned paradigms HiTLCPS, IoP, CPSS, CPST, and SIoT, which are summarised in Table 4.1.

Table 4.1: Human role in Cyber Physical Social Systems

System	**Human Role**	**Features Individual in social interaction**	**Platform**
HiTLCPS /HCS	Collaborative, command, and control	Consider human as an individual entity, improve virtual machine to be close to reality	CPS
IoP	“Main resources” sometimes replacement of physical sensors Provider of information (willing and unwillingness) via smart devices, end to end connection	Mostly seen as individuals who interact with other components, “center of the Internet system”, Human and computers seen as “participant machinery”	Internet
CPSS	Full member of the systems, Producer, and Consumer of products-services	It is not isolated, however, has interaction with other social and physical sensors, impacts on and from a social network, social economy, social culture, (social contexts), and environment	CPSS
CPST	Data provider (through contribution in online and social networks or offline physical presents and interacting with others)	Individual and in the social context	Hyper IoT
SIoT	Without human interaction	Human information is seen as an object of a social network of “things”	IoT

In cyber-social systems, human actors and their interactions with a system play an important role in the state and functioning of the system, also, people's operating and the system's operation depend on each other behavior assumption [133]. Human roles in CPSS can be categorized from a system engineering point of view into human roles as a sensor, and human roles as a system component [30]. From an application point of view -based on human behavior- its interaction with systems is mostly classified as active or inactive, where the former group is divided into contributor, disrupter, and intruder, whereas the latter refers to legacy systems in which the user does not interact with the system intentionally or unintentionally [126].

Generally, from the authors' point of view, the main difference between CPS/IoT and HiTLCPS concepts with CPSS is cybering human and social factors such as movement, behavior, and cognitive features to develop reliable, flexible, and scalable systems, which assist stakeholders in making their decisions faster and in a safe, secure, and reliable way.

The CPSS develops sensing, computation, and actuation. The control aspects and actuation are changed concerning social sensing and computing integration. I argue that CPSS can be seen as a System of System (SoS), which such as a CPS bridges multiple purposes, domains, and data [134]. I refer to SoS as "an integration of a finite number of constituent systems which are independent and operable, and which are networked together for a period of time to achieve a certain higher goal [135]". The CPSS domains, aspects, and facets are similar to the CPS domains, but the contrast is that in the CPSS modeling human behavior-individually and in the social context- is more complex and stochastic than considering human-in-the-loop in the CPS. In addition, social networks and applications bring new sources and customers into the system.

From the output of our investigation on the CPSS paradigm and according to the undertaken studies, mainly [4, 24, 32, 121, 122], the CPSS can be defined as follows [136]:

The CPSS tightly integrates data processing into physical systems, cyberspace, and the social world through heterogeneous resources, including sensors, actuators, and computational systems to form a unit in cyber environments. Furthermore, the configuration and computation in a CPSS aim to achieve superior Quality of Service (QoS), quality of the experiment, and performance. Therefore, the multi-objective optimization of the CPSS operation strongly depends on trustworthy and efficient computation and communication among several layers of the three subsystems.

4.4.2 Defining a Taxonomy of CPSS

Our proposed CPSS taxonomy is described with six categories and related areas and disciplines (Figure 4.4). Based on the thesis's objective, I have studied several resources that CPSS examined and presented. I found the footprint of CPSS in many types of research and applications that have taken them into account to make our taxonomy.

The goal here is to conceptualize the CPSS through surveying, sanitizing, and explaining works in the domain. A taxonomy of the CPSS in six categories is created using a combination of literature review and systematic research methods. Existing studies and

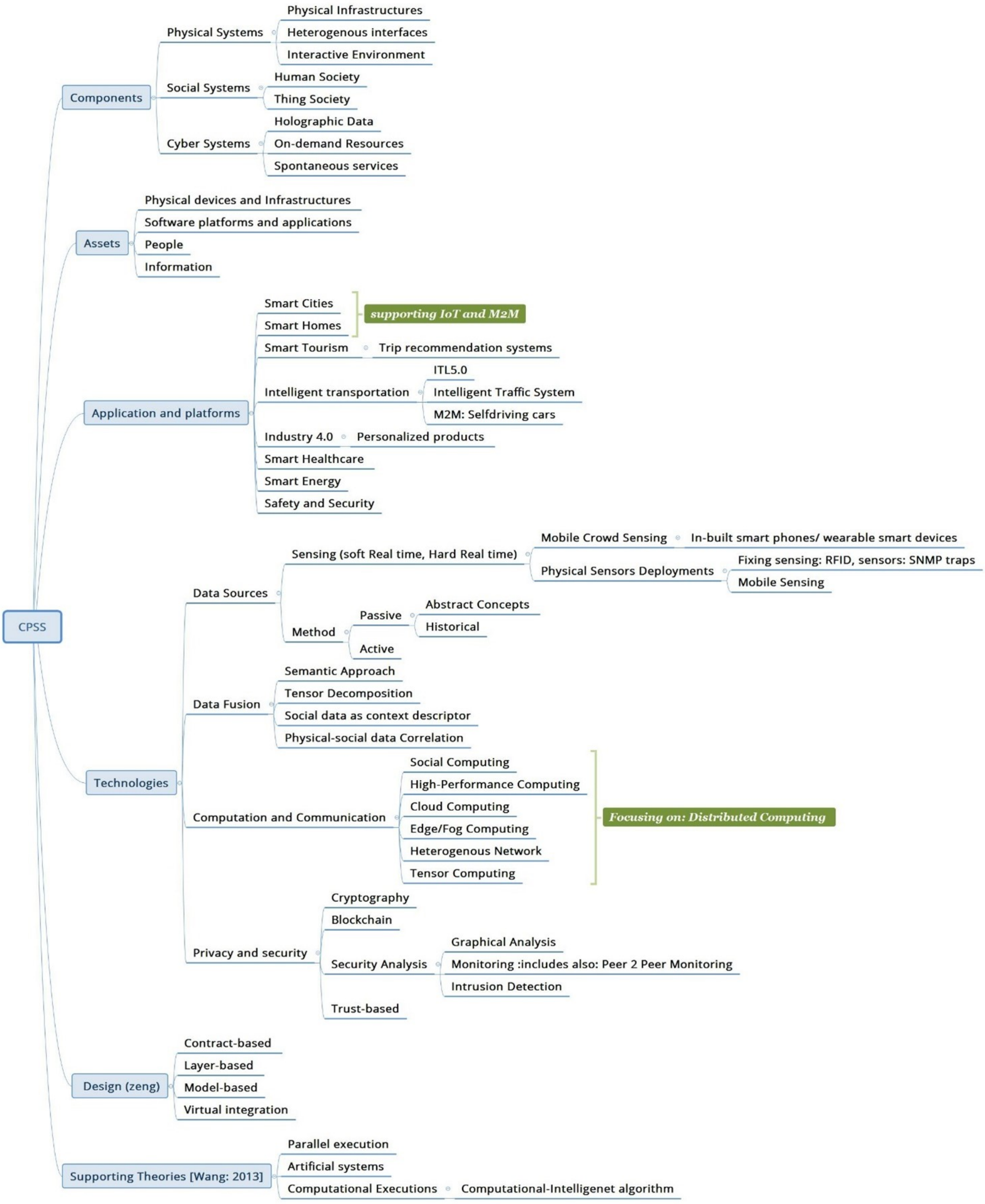


Figure 4.4: CPSS Taxonomy

research within each category were studied, and the results are provided. This taxonomy will help formulate and conduct future research and prototype products related to CPSS in a more structured way and method. In further studies, this taxonomy can be expanded for the user´s best interests.

A considerable lacuna in the direction of CPSS work has been determined. Little work has been conducted on modeling the interaction of social objects with cyber and physical systems, which are the most challenging components in a CPSS to assess and model. Considering the studies done in the CPSS, there is still no taxonomy for this new paradigm. In the following, I propose a CPSS taxonomy based on the CPSS definition, state-of-the-art, and supported technologies. I consider the proposed taxonomy as an initial step, with the potential to be developed in the future. The proposed CPSS taxonomy paves the way for a better understanding of the CPSS ecosystems and their characteristics.

This work is the first attempt to create a CPSS taxonomy. For generating the CPSS taxonomy, I studied and analyzed recent articles, and literature on CPSS databases. I was inspired by the taxonomy of system of systems from NIST to provide a framework for CPSS [134]. I categorized CPSS based on facets, domains, applied technologies, theories, and design approaches. Each category aims to present a different dimension of the system, thus, the proposed taxonomy makes it easier to understand CPSS aspects and characteristics towards developing design mechanisms, and reliable and accessible services considering user satisfaction. The taxonomy is also leveraged to identify open problems that can lead to new research areas within CPSS domains.

Components: The components of CPSS include physical, cyber, and social systems.

Physical systems: Physical systems refer to all geographical objects in the world including infrastructure, physical devices, sensors, cooperative actuators for collecting real-time data, and communication networks. In CPSS, physical space represents real-world physical systems through smart objects and communication systems.

Cyber systems: Cyber systems refer to computing, storage information processing, and sharing services, especially situations awareness and decision support services that directly command and control and are represented by cyberspace. Cyberspace is a time-dependent set of generalized information from resources including virtual and digital abstractions aiming to have to interconnect cyber entities [18, 137].

Social systems: Social systems that are represented by social space in CPSS reflect social attributes and interactions in the human social world either from cyber entities or physical systems in a semantic way. Indeed, social systems are logical components of CPSS [18].

Assets: Any tangible and intangible valuable resources for individuals, communities, organizations, and governments can be categorized as assets [138] of the CPSS. These assets include any hardware: physical devices for digitization and Communication (or IT) objectives such as switches, routers, and computers; software, and applications which consist of all platforms, and databases publicly and privately available and used.

Another asset is information that refers to critical and sensitive information related to individuals, communities, organizations, and critical infrastructure- collected by information systems/services, stored, analyzed, and transmitted through cyberspace. Finally, people in a CPSS refer to those who interact with cyberspace, either customer or provider data and services.

Application and platforms: The CPSS offers various applications such as managing traffic, autonomous vehicles [113], customization in industrial products and services [55], recommendation systems for tourists to choose the best routes [6], and behavioral profiling to predict future behaviors [133] which have both security and marketing purposes, and many other examples.

These applications provide services for users to monitor, control, and manage the assets and the environment of the system. CPSS application data can be obtained in either an active or passive manner using homogeneous and heterogeneous sensors. I have categorized these applications based on business purposes including smart cities [111], smart homes [139], smart tourism [6, 140], intelligent transportation [113], social manufacturing explanation of Industry 4.0 [110, 141], Industry 5.0 Critical Infrastructure (CI), smart healthcare, smart energy, humanoid robots [139], digital twins, safety and security.

Smart cities: The population residing in urban areas is increasing every year, as of 2018 forms 55% of the world´s population and it is expected to reach about 68% by 2025 [142]. In this regard, the key issues are management and sustainable urbanization which can provide social welfare to citizens. A new prototype called a smart city by emerging new information communication technology with urban management infrastructure seeks to bring a convenient quality of life, improved services, and a clean and safe global environment [5, 143, 144]. Smart city characteristics can be defined as sensible, connectable, accessible, ubiquitous, sociable, sharable, and visible [111]. In this sense, the IoT, CPS frameworks, and architectures are mostly applied for designing platforms of a smart city [145], but the social factor is not the well-defined or human role is seen as an individual, which will be a problem for managing shareable resource systems unless defining smart cities as a CPSS [111]. The social space for humans in smart cities in the context of CPSS refers to the participants of different activities in the city [112]. Distributed Sensor Networks (SNs) [146] and sensing physical systems alongside inhabitants´ sensor-enabled smartphones and online social networks provide near real-time large-scale sensing for big data mining and knowledge discovery which allows the systems to offer more proactive and responsive services for their users and citizens [29]. The deployed platforms and implemented services increase people's awareness about the dynamics of their environment, and prediction of citizens' activities and movement, including smart parking systems, environment monitoring [29], and event sensing [28].

Smart city platforms in the CPSS framework can lay the foundation for correlated applications such as smart homes, smart tourism, and intelligent transportation. They carried out studies and work on designing and conceptualizing CPSS for smart cities categories into the data-driven approach, and networks and communications approach.

The objective of the smart city platform is to generate smart data and obtain urban intelligence, which owing to the unstructured or semi-structured data in the CPSS requires a different conceptual framework for the data management framework [147]. A data-oriented conceptual CPSS framework was proposed in [29] which consisted of four layers: data sourcing, data processing, data fusion, and application by leveraging big data and mobile sensing in their approach.

Smart homes: Smart homes integrate smart devices and Smart Home Technologies (SHTs) consisting of sensors, actuators, monitors, interfaces, appliances, and devices that are networked to provide information and services considering multiple preferences. SHTs enable automation, localized and remote control of the domestic environment [148]. Successful scenarios and implementations of smart homes would be more adaptable to human daily life. They need to consider human preferences and design psychologically-inspired systems [26] which require the integration of social systems with traditional information computing. In this regard, Smirnov proposed [26] self-organization approach for CPSS and devices, using a cleaner robot as an example, they presented an ontology-based information model for smart home device interaction in cyber-physical space. In this platform, the devices, domains, and vendors are independent of the smart space. The three-level organization is applied at the top level called the strategic level to adjust customer preferences that are transmitted to the physical level and in the middle layer, and planning-level services are designed to control domains.

Smart tourism: "Smart Tourism", which could be a web-based or/and mobile application, inherits from "Smart City" as a platform. Smart tourism should provide attractive and real-time information such as location, route, images, rating, and captions of tourist attractions anytime and anywhere [140, 149]. CPSS in smart tourism is a new approach that integrates social systems and Service-Oriented Architecture (SOA) methodology increases the quality of trips and tourist information and computes the influence and accuracy of exchanged and shared information via social networks and web platforms as well as the influence of shared information and experience with other users, and for further actions [6].

Intelligent transportation: Merging result integration of social systems and human dynamics level up the transportation system and bring wide perspectives and advantages. CPSS-based transportation systems called Transportation 5.0 or ITS 5.0 aim to optimize traffic control and management by adapting strategies on control technologies, data perceptions, and analysis, as well as the management of which social aspects become paramount. To solve the social system complexity in these systems, the ACP approach is applied to model and design ITS 5.0 [113] in CPSS. Another promising application of CPSS in intelligent transport is an integrated hybrid system for enhancing driver behavior prediction which can be useful for autonomous driving [126].

Social manufacturing: Following the I4.0 -and recently Industry 5.0 (I5.0) by focusing on customization- paradigm, the new manufacturing concept is integrated with social systems and is called social manufacturing [141] with three core aspects of Dynamic

Resource Communities (DRC)-based self-organizing and configuration. Therefore, a CPSS service-oriented platform was introduced [110] to provide personalized products and services in the context of I4.0. This platform integrates different manufacturing resources in the social manufacturing environment to provide mediators for customer-producer interaction.

Smart healthcare: Smart healthcare is one of the domains in smart cities but with a different approach and business model, and includes assisting diagnosis and treatment, assisting drug research, health management, disease prevention, risk monitoring, virtual assistants, and smart hospitals [150]. Despite the strengthening of smart healthcare systems to assist physicians and patients, it is challenging to secure and maintain the privacy of their sensitive data [151]. Smart devices and Wireless Body Area Networks (WBANs) with multiple sensors as wearable devices are gaining popularity and providing information about body temperature, heart rate, falling detection, oxygen saturation, etc.

To the best of our knowledge, there is no CPSS framework for smart healthcare systems but here I believe the ideas and works in CPS [152, 153] should be expanded and promoted based on social integration in the systems as one of the important constituents of smart health.

Smart energy: Smart energy systems seek the most efficient and least costly solution by using all infrastructure, low-temperature district sources, and renewable energy heat sources. The Smart Grids (SG) is a traditional concept that is widely used in smart energy systems. SGs are electronic networks that use ICT, self-healing technologies, and control theories and models to provide better connection and operation for distributors and generators as well as more reliability, security, and flexible choices for users [154]. In the CPSS framework, for the energy efficiency area, a novel concept of a robot for energy control based on parallel cyber-physical-social systems for the next generation of energy and electric power systems is proposed [155]. Considering environmental factors, economic, social, and human behavior for smart energy modeling, a CPSS conceptual model was introduced [154] taking SGs as a core, but also other factors such as gaming behaviors of participants, carbon markets and their regulation, strong volatility, and intermittent renewable energy sources.

Safety and security: Security and privacy can be considered as a service category and application. Their mechanism provides support services, and products as an important and broad domain in CPSS. The privacy of a CPSS is important for eventual acceptance by the public. Therefore, any communication must preserve data privacy anywhere and at any time. CPSS security -like CPS- presents several characteristics that distinguish it from more conventional IT systems security. The security objectives have not changed compared to traditional IT systems, and they are not the only service expected from CPSS security and safety. Designing this new generation of CPSS requires other requirements in terms of system security. In this case, the conceptual model might be different, and the systems' behavior changes owing to the interaction of human decisions [156–158].

Technologies: In CPSS, technologies are adapted and integrated from IoT, CPS, social networking, and computing with new approaches and conceptual models. Technologies in CPSS can contribute to solving human-computer interaction, seamless mitigation technologies of a heterogeneous network, security, privacy, social computing, context awareness, management, and user behavior-based proactive service. With the homogeneous and complex nature of CPSS, there are a variety of challenges regarding data fusion, processing, and analysis, computing and communication, privacy, and security. In this section, I provide an overview of proposed solutions from different works and points of view.

Data sources: The initial step in deciding on data management and usage is to determine how and where the data is acquired [159]. In this study, the data sources were categorized based on the data collection method to answer "how" in terms of methodology and to answer "where" in terms of technology for data acquisition. The methodology is grouped into passive and active, and technologies are categorized based on mobile crowdsensing, social network sites, and physical sensing. The term Mobile Crowd Sensing is defined as "where individuals with sensing and computing devices collectively share data and extract information to measure and map phenomena of common interest" [160]. Generally, crowd systems are systems that congregate people who are interjecting and communicating with each other and exchange experiences and information physically or virtually towards the fulfillment of the system's objectives [118]. As is the case in CPSS, the complexity of crowd systems arises from the existence of a human factor that can never be fully controlled. Consequently, certain inconsistencies and systemic instabilities remain in crowd systems. Examples of such systems include crowdsourcing platforms, Wikis, and museums equipped with smart guidance systems [55]. People interaction in social online services called Social Network Sites (SNS) provides social big data on any topic in large volumes with different formats and contents, and to some extent, SNS reflects the social circumstances [156]. Along with social sensing, physical sensing reflects what happens in the physical world through physical sensors. Physical sensor node deployment can be classified into static and mobile, both of which can be deterministic or random [161].

Data Fusion: Data fusion in CPSS is a very challenging task that is mainly related to how to represent and address higher-order and higher-dimensional heterogeneous data from multiple and heterogeneous sources [162]. Despite the traditional data fusion method that is simply processed from physical devices, in CPSS, social data can be collected on a large scale, multiple resources such as transportation applications and devices such as cars, wearable sensors, medical services, social media/networks application, web browsers, cross languages, heterogeneous networks with different formats and representations, etc. [27]. A widely used method for categorizing data fusion-related functions is the data fusion model which is maintained by Joint Directors of Laboratories (JDL). They define data fusion as: "A multi-level process dealing with the association, correlation, combination of data and information from single and multiple sources to achieve refined position, identify estimates and complete and timely assessments of situations, threats and their significance" [163]. Data fusion methodologies are classified mainly by their space in the work by Wang [27] into CPS, CSS, and CPSS groups. They introduced their model in CPSS called tensor-based models by extending the Markov Chain (MC) model to the transition matrix of MC. They proposed a multivariate multi-step transition tensor M2T2 model to fuse data arising from CPSS, including mobile sensor data, and Point of Interest (POI) in the city. To overcome the multi-space service problem, they proposed a social network information Cyber-Physical-Social Transition Tensor ($CPST^2$) to fuse the CPSS data in a unified form. Generally, tensors in a CPSS represent objects and they are heterogeneous. In another work by Chen[164], a sensor-network-conversion-based data fusion approach was applied, which can simultaneously analyze multiple matrices and tensors. CPSS data processing challenges should be addressed by an overarching approach that tackles the problem from different perspectives, i.e. Edge/Fog Computing – on the one hand, and Big Data – on the other, converging into a lightweight solution for data processing through computation offloading to collocated edge devices.

Computation and Communication: The dynamic, customized, mobilized, complex nature of CPSS, in addition to the challenges in data fusion, brings unsettled data processing frameworks and models in CPSS from a computational and communication point of view. One solution [109] is augmenting CPSS data processing modules with current technologies such as cloud computing, edge computing, and big data. In the context of SIoT(Social IoT), Dautove uses multi-tier computational with Data Information Knowledge Wisdom (DIKW). Studies have shown that combining multiple techniques tackles the limitations and problems of a single method and enhances the data processing and computing objectives [18]. A brief explanation of each of these technologies is provided below. Cloud/Edge computing is useful in the presence of big data, as it can provide on-demand computation and storage resources for CPSS applications and it has been deemed the key technology for practical use in various fields of CPSS [120, 165]. Socially Intelligent Computing (SIC) aims to merge intelligence, knowledge, and human experiences through social, crowd, and end-user computing to provide knowledge and wisdom called collective intelligence and social perceptions[7].

Privacy and security: Cybersecurity is of paramount importance when designing and modeling CPSS. Interoperation among heterogeneous devices and applications and unpredictable human behavior is a complicated task. However, the interaction of physical components with cyber processes in CPSs and social elements in CPSS brings new challenges for identifying, classifying, and analyzing cyber-attacks and determining a proper defense strategy to design cyber-secure systems. The attackers implement five steps of intrusion: access, discovery, control, damage, and clean up, to gain complete control of the system directly or indirectly, and to hide any traces of any caused intrusion [166]. Current technologies such as blockchain cryptography [167] can be applied to CPSS security and privacy policies.

Design: Combining human and artificial intelligence is a promising direction for enhancing efficiency and meeting customer requirements. The CPSS is a suitable solution that adds a Human Intelligent Teaming (HAT) layer to the design of elegant systems [168]. Based on a survey by [17], CPS system-level design can be extended to CPSS, and categorized into five categories: component-based, layer-based, model-based, virtual integration, and contract-based design. In addition, they proposed a flow-based methodology showing data, physical and human flow. It is based on a directed acyclic graph, and to determine how specific state transitions and events occur in CPSS, they successfully applied the Petri nets model.

The tools which can be applied in modeling and designing the CPSS should adaptable to three CPSS subsystems. From existing tools, the model-driven languages/techniques that can be considered to be useful are those compatible with the heterogeneous nature of CPS and not be specified for one domain. In a conducted survey by Liu et al. [169], they compared ten different tools and showed among them, the Ptolemy and the PtolemyCyPhySim can cope with CPS challenges. The selected assessment criteria were some of the CPSS modeling requirements including heterogeneous modeling, time, concurrency, system evaluation, and meeting diverse Quality of Services (QoS).

To ensure the system is effectively designed, it is crucial to establish tests for the developed processing design. For this purpose, in [170] learning factories are considered an effective way in the CPS environment namely manufacturing and Industry 4.0 (I4.0) which I reckon can be applied in the CPSS context as well. The learning factory integrates real-world applications in a small-scale model to explore the developed design and improve the knowledge related to the systems.

Supporting theories: The CPSS supporting theories proposed by Wang [4] called Artificial, Computational, Parallel (ACP) is described in Section 2.1.1. The fundamental idea of ACP has been applied in intelligent transportation[113], and artificial healthcare systems [171] as a method for controlling and managing these systems. In the ACP theory, as mentioned above, artificial systems (A) image/mirror and transmit the data and events flow in the physical-social systems in cyberspace, computational experiments (C) are used for the validation of the control plans, and finally, parallel execution (P) determine the stepwise control and management of the CPSS.

4.4.3 CPSS Threats

The loss could be referred to in safety measures, confidentiality, integrity, or availability of resources. Hence the harm implies harming people, the environment, or systems [172]. “Only amateurs attack machines; professionals target people.” (Schneier, 2000) [173]. Talking about CPSS, the social aspect is included in this context, besides the safety and security of people, communication assets, and information in the system. In Figure 4.5, I classified the main threats and cyber security aspects in a CPSS.

Therefore, developing a threat model that takes into account the distinctive qualities of the CPSS components and their correlation with them can be effective in managing the risk of cyber-attacks. Determining the assaults and the best defense technique to secure the systems is one of the CPS security facets and a step in the process. Answering who and what should be protected is the fundamental question that needs to be addressed at this point. Threats are primarily determined by their sources, targets, motivations, assault methods, and potential outcomes. [174].

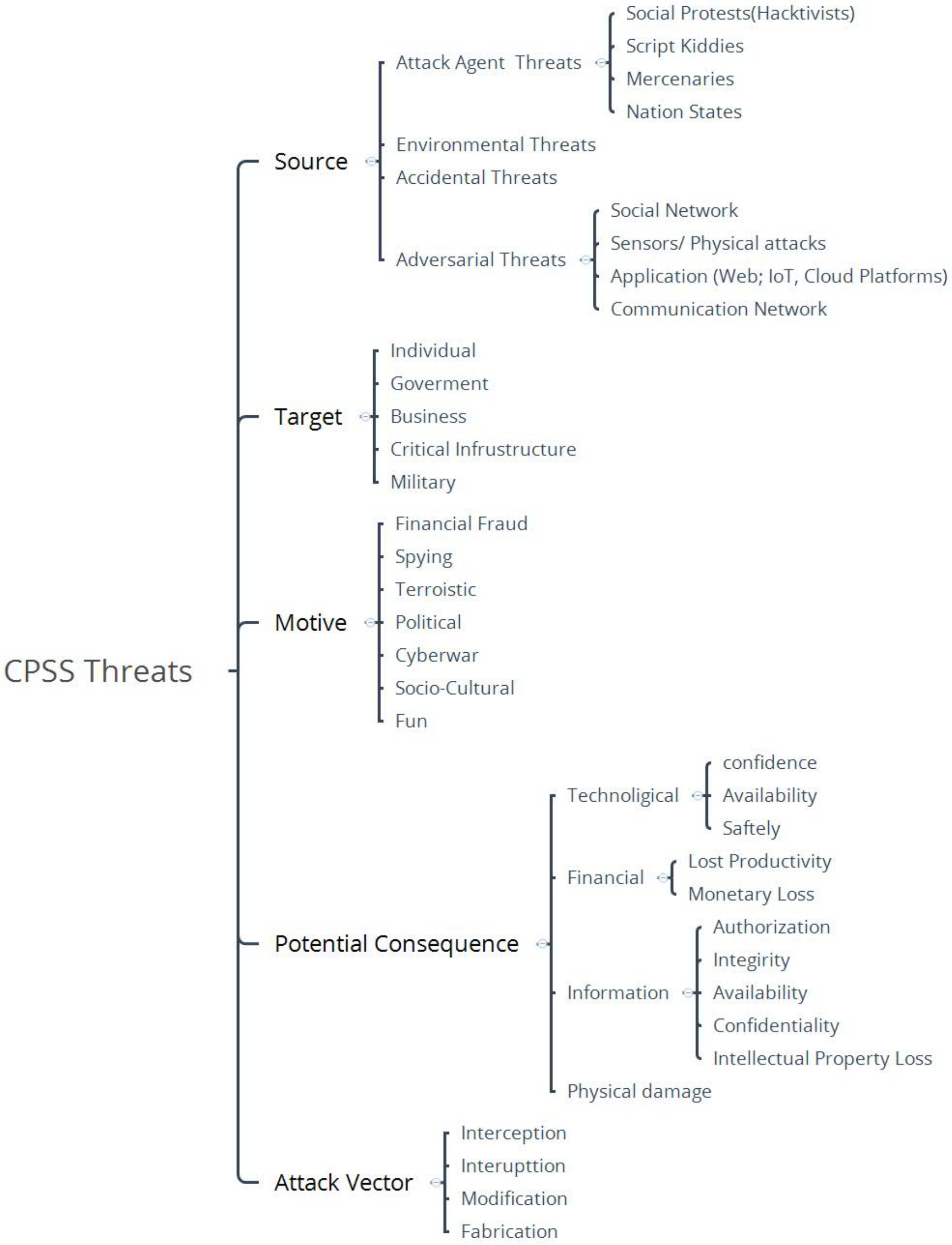


Figure 4.5: CPSS Threats

4.5 CPSS Challenges and Open Issues

Generally, the intrinsic heterogeneous, concurrent, and sensitivity to the timing of CPS and CPSS poses many modeling and analysis challenges. Moreover, this means that time plays a critical role in the performance of a CPSS, not only the function of a task [134].

The integration of social aspects in systems poses issues such as medical safety, human rights, security, energy scheduling, traffic management, and even resource sharing such as vehicle sharing, urban management, and many other examples. As a result, before building systems with social components, it is vital to conceive from the CPSS perspective and include social entities that interact with other components, as the system is not isolated.

Another issue is related to social acceptance. Social acceptance of new technologies such as IoT and CPSS is something that if the human is not considered as the user and provider of the system's information, we cannot make user-friendly applications and even appealing human interfaces [175]. Energy consumption plays an important role in the CPSS design. The development of next-generation smart energy systems requires innovative computational methodologies and models. The design of the energy-aware and data-driven CPSS has become critical for sustainable development [151, 154, 176]. Another challenge besides energy management in data collection and actuation methodology is integrating heterogeneously distributed devices into a common platform[111]. The main issues addressed by researchers are provided in table 4.2. I categorized these into four classes: data fusion, energy efficiency, privacy and security, and network and system design.

Table 4.2: CPSS Open Issues

	Domain	**Studies**
CPSS Open Issues	Data Fusion	[27–29, 156, 162]
	Performance Optimization	[123, 177]
	Privacy and Security	[127, 133, 156, 178]
	Network and System Design	[126]

In the future, CPSS applications can be expanded to different businesses such as robotics, smart education systems, smart societies s-Society 5.0- moving from e-learning 3.0 [179] to Learning 4 [180] using Virtual Reality (VR), Augmented Reality (AR) and adaptive Massive Open Online Courses (MOOCs) [181]. Moving from traditional social systems to cyber social systems under the CPSS ecosystem requires a closer and more precise methodology for implementation. As seen in the pandemic crisis in 2019-2021, some e-learning ICT infrastructures are not ready [124]. One of the ultimate goals of intelligent systems such as CPSS is to provide information "anytime anywhere"for their users. For instance for a natural tourist accessing an accurate location is necessary, which is still an issue in current smart solutions [6].

4.6 Human Behavior Model

More study [182, 183] testifies to the significance of knowing human behaviors in order to learn how to create and construct systems that encourage users to perform responsibly.

Understanding human behavior is critical when developing cyber-secure and resilient CPSS that are intended to be used by humans and their behaviors have a huge impact on the system´s performance.

The process of transferring the findings of behavioral studies conducted in the real world into an environment dominated by technology can be a difficult and timeconsuming endeavor. Nevertheless, in today's world, it is feasible through the utilization of big data and sentimental analysis, as well as the discovery of recurring patterns in people's decision-making processes.

Many cyber security issues have been tackled by the field of behavioral science. Secure systems are sociotechnical systems, according to to [184] and they urge that I apply behavioral science to "prevent users from being the 'weakest link'". Kevin Mitnick in the book "the art of deception"admits that he rarely broke a password because it was easier to manipulate or mislead individuals into revealing it through the use of various social engineering tactics".

One of the prevention strategies is enhancing situational awareness during a "cyber event". The concept of Situation Awareness (SA) plays an important role in people's decision-making process. Based on Endsley (1995) [185], even while there is not always a direct connection between SA and performance. In general, it is to be expected that poor performance will occur when SA is either incomplete or inaccurate, when the appropriate action for the identified situation is not known or calculated, or when time or some other factor limits a person's ability to carry out the appropriate action. In all of these cases, it is expected that poor performance will occur.

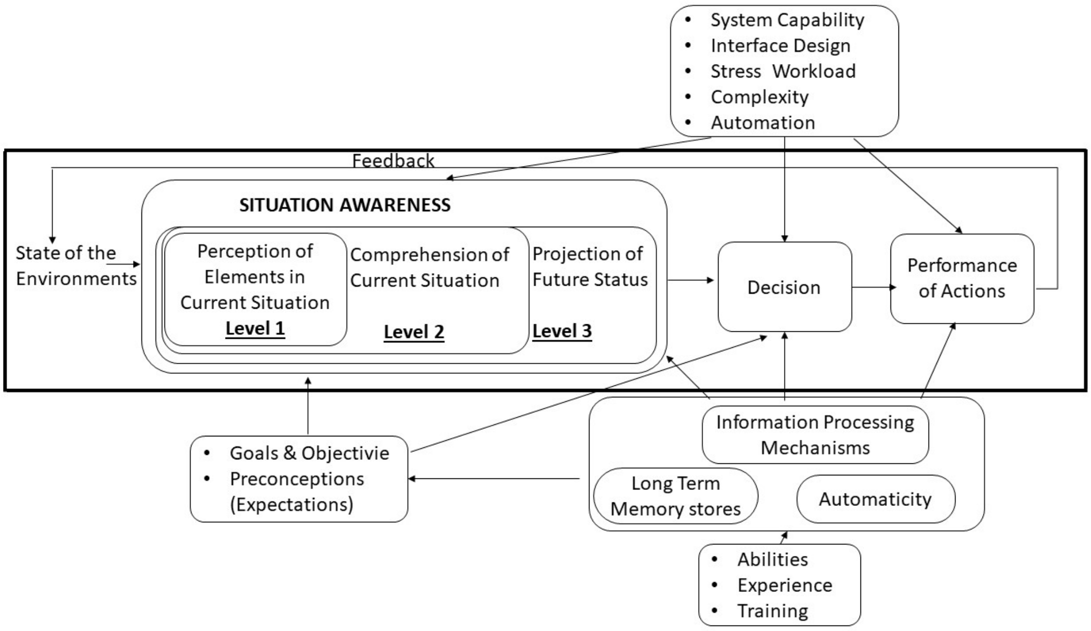


Figure 4.6: Situation Awareness [185]

Endsley SA theory creates the foundation of my model. The idea of this work is not to prove the human behavior elements or the impact of their behavior in security breaches, but the goal is to demonstrate how Coloured Petri nets can be used to represent human behavior in cyber security scenarios. For this purpose, and based on my research on human behavior in social systems (cyber and physical), skill, experience, and time pressure are chosen to describe a person's behavior. These elements represent SA in figure 4.6. This theory provides a primary framework for our work to answer **RQ 3**.

4.7 Chapter Summary

Designing and deploying CPS without paying attention to human behavior in the shadow of social behavior – crowd behavior– will fail to satisfy goals such as the best recommendation and optimizing decision-making. Therefore, social systems are pivotal components of CPSS, and they are already transforming how humans interact with the physical environment by integrating them with the cyber-physical world. The integration of social systems in CPSS provides new frameworks for smart cities, intelligent transportation, energy management, and sustainability to enhance people's daily life tasks, system availability, and reliability. This is a relatively new research field that requires new approaches and techniques. In this work, almost all applications of CPSS are studied and introduced for further research and future developments. The operation and configuration of CPSS require methods for managing the variability at design time and the dynamics at runtime caused by heterogeneous resources and complex ecosystems. The literature review in this chapter provides a deeper look at CPSS and what advantages they bring for users as individuals and public interests. Furthermore, I described state-of-the-art CPSS approaches and methodologies. The key techniques, theories, and design approaches are clustered based on the categorization and description of previous studies. In addition, the present and potential applications of CPSS are argued.

A uniform definition of CPSS provided in this chapter helps to find a common understanding of this new paradigm. The given comparison of SIoT, IoP, HiTLCPS, and CPSS, clarifies the human role in designing a CPSS. To describe CPSS, this chapter delivered a taxonomy of this new paradigm based on the system-of-systems approach inspired by the CPS-NIST framework. The CPSS taxonomy includes assets, components, applications, platforms, technologies, design methodologies, and newly supported theories. This taxonomy is an initial attempt to formalize the CPSS, and sub-classes can be expanded by introducing new methodologies and theories in the future.

The CPSS as a new paradigm tackles some issues that can be seen as opportunities for research. The issues that researchers consider in CPSS are in the following domains, data fusion, analysis, performance, network, system design, and security/privacy. Another important issue is that there is insufficient work related to the human role in CPSS. Even though the challenge, it is an advantage of CPSS in terms of social learning techniques. To that extent, a technique such as deep learning is applied to integration, and interaction with physical and cyber systems, and still the human role, and interactions in CPSS are not well-defined. Even in some CPSS studies, the human role is considered as individual and not in the social context.

5

Graphical Formalism of Cyber Resiliency Analysis

Sometimes it is the people no one can imagine anything of who do the things no one can imagine.

Alan Mathison Turing (1912-1954)

5.1 Introduction

This chapter aims to introduce a set of rules for translating or mapping GrSMs to PN classes and explain which class is more useful and pragmatic in the case of cyber security and resilience. Also, it examines the aforementioned items in chosen PNs. In chapters 2 and 3, as well as in Figure 2.4, I emphasized the importance of having a comprehensive understanding of a system's cyber security, including its vulnerabilities and defenses, when analyzing cyber resilience. To achieve this, a suitable graphical security model should possess certain characteristics such as scalability, flexibility, the ability to consider pre and post-conditions for vulnerability analysis, encompassing social engineering scenarios, and providing a distinct and concise way to design countermeasures, defense, and protection nodes- It allows to cable managers to make better decisions and develop efficient strategies.

In this context, I proposed using Attack Defense Tree (ADT) to graphically model the attack-defense scenario as a way of illustrating vulnerabilities and defense strategies. To address this, I propose using attack trees (ATs) to graphically model the attack-defense scenario, as they are effective at illustrating vulnerabilities and defense strategies. Once the AT model is established, it can be translated into one of the Petri Net (PN) classes and augmented with time constraints (or attributes) to validate the model and assess system performance under various scenarios.

In this chapter, I discuss the use of GrSMs and PNs as a means of translating ADT to GSPN. I also introduce a set of rules that can be used to analyze the cost of both attacker and defender actions, which are then integrated into the translation process. I validate that these rules are reliable and can be applied to various classes of PNs, including GSPN and TCPN. Additionally, I showcase how the same rules can be upgraded for use in CPN modeling, allowing for the translation and performance analysis of the system at each phase of cyber resiliency. In this regard, two different graphical models were chosen, ADT and Attack Countermeasure Tree (ACT).

The remainder of the chapter is organized as follows; in section 5.2 I describe how to map ADT to GSPN; in section 5.3 a set of rules is provided to translate ATs to CPNs that is valid for all PNs; Therefore in section 5.4 the CPN notations for cyber resilience is explained, and finally, in section 5.5 the summary of the chapter is provided.

5.2 Semantics for Translation of GrSMs into GSPN

In chapter 3, I explained the GrSMs and PN classes compatibility. When translating a GrSMs model (for example an ADT model) to GSPN or CPN/CPN, it is assumed that in any PN models the approach is bottom-up and the PNs modeling starts from leaf nods in the GrSMs.It clearly describes that the reachability set of synchronized events in the PN models depends on the initial marking (leaves in GrSMs).

In the translated PN models, all of the input events, states, transition functions (Actions), and output events are displayed in GrSMs in their entirety. The models have finite states. In our environment, resources in a CPSS (and resources in any other system) can be modeled by places, although PNs classes differ depending on the introduced notations, and their instances can be represented by tokens. The transitions in PNs must correlate to the actions taken by invaders and defenders (including IDS). Any arc that extends from a resource place to a transition represents the direction of the action and fired transitions show the token release and acquisition of some resources that are being processed by a system.

5.2.1 ADT and Transition to GSPN

In the initial step, I translated at and then adt to gspn. In particular, I have been inspired by [83] and I introduced a new translation of ADT to GSPN [90] as it is shown in Figure. 5.4. The main reason to select GSPN for modeling and analysis of the security of the system is its ability to show the dynamic behavior and stochastic variables in the system under attack. It means that each attack scenario can be an option for the system [186]. In addition, as cyber-attacks can be stochastic and independent, it is important to analyze the security of CPSS by considering these characteristics.

Figure. **??** illustrates a straightforward AT example in graphic form. The goal of the attacker is shown by the root node and the sequence of activities to reach this node is shown by events (E). Here, D1 is used for intrusion detection as a defense technique.

For translating AT to GSPN, the rules presented in Figure. 5.2 are proposed, defining

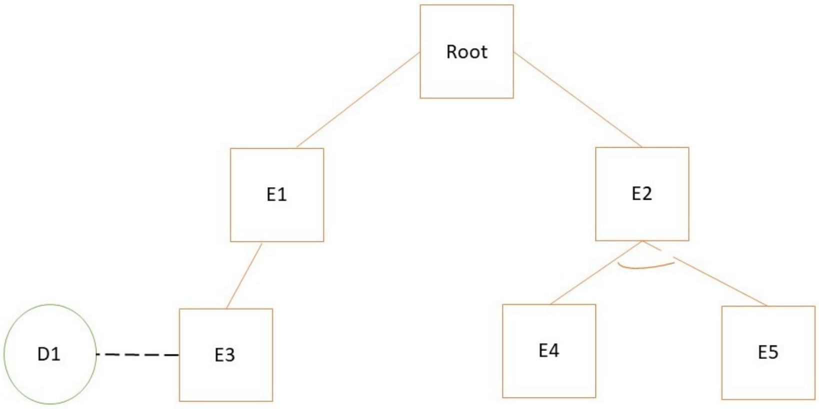


Figure 5.1: Attack Defense Tree (ADT) presentation

translation to each node [90]. In this methodology, the translation of leaf nodes and subgoals is represented by transitions in the generated PN model. Places in the pn model represent the arcs in AT.

The assault can be carried out in stages up until it reaches its ultimate objective, which is denoted by the Root node in the AT and which is represented by a location in the PN model. This location shows the condition of the system about the attack. For a successful attack, this place is marked with a token. Constructs considered in the translation mechanisms are shown in Figure. 5.2:

- **Sequence**; in the AT, E1 a depended event by conducting E2, which in PNs is translated in a sequence.

- **OR**; in the AT, it defines the two possible events which are translated to concurrency in PNs. E2 and E3 are called concurrent if they are neither casually dependent nor in with conflict one another.

- **AND**; In the AT means two dependent events that in PN, E1 cannot be fired without firing E2 and E3.

- Finally, the detection node in the AT is shown by a loop in Petri nets. Applying the rules presented in 5.2 to the ATD of Figure. 5.1.

The idea of modeling a system with GSPN is to show the behavior of the system regarding the possible reaction of the system to each attack. I propose to translate each event as a transition in PNs considering Immediate transition for the kind of attacks that happen as a sequence result of a certain attack. For independent and distributed attacks Exponential transitions are defined. General Transitions illustrate the consequence of some actions which happen in an interval of time.

The estimated time and probabilistic to conduct an attack successfully depend on the attacker's technical skills, social engineering skills, facilities, level of access to information

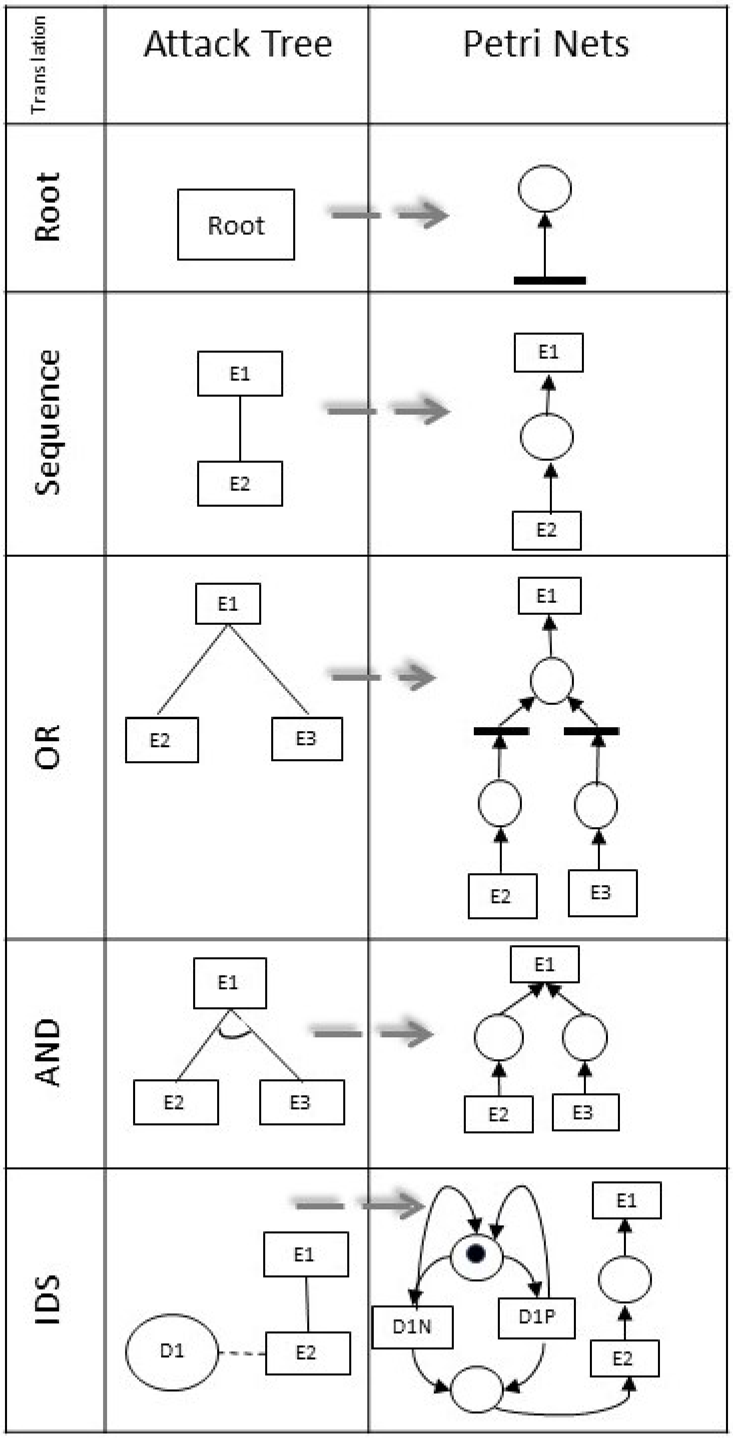


Figure 5.2: Attack Defense notations mapped to Generalized Stochastic Petri nets notations

resources, and so on. On the other hand, the maturity level of an organization's security systems, their team education and knowledge, also resources, and so on are other affected parameters that determines the values of each leaf.

5.2.2 Security Analysis By GSPN Based On Attack Defense Tree

In this work, the provided example is about a 3D printer borrowed from [187]. In this instance, the attacker's objective is to increase feed speed by SQL injection. This increase destroys the tool and leads to a low-quality finished product. As a result, the attacker may be able to control the spindle speed in the G-code file, which may lead to drilling bit breakage. The possible attacks and defenses are illustrated by an ADT in Figure. 5.3.

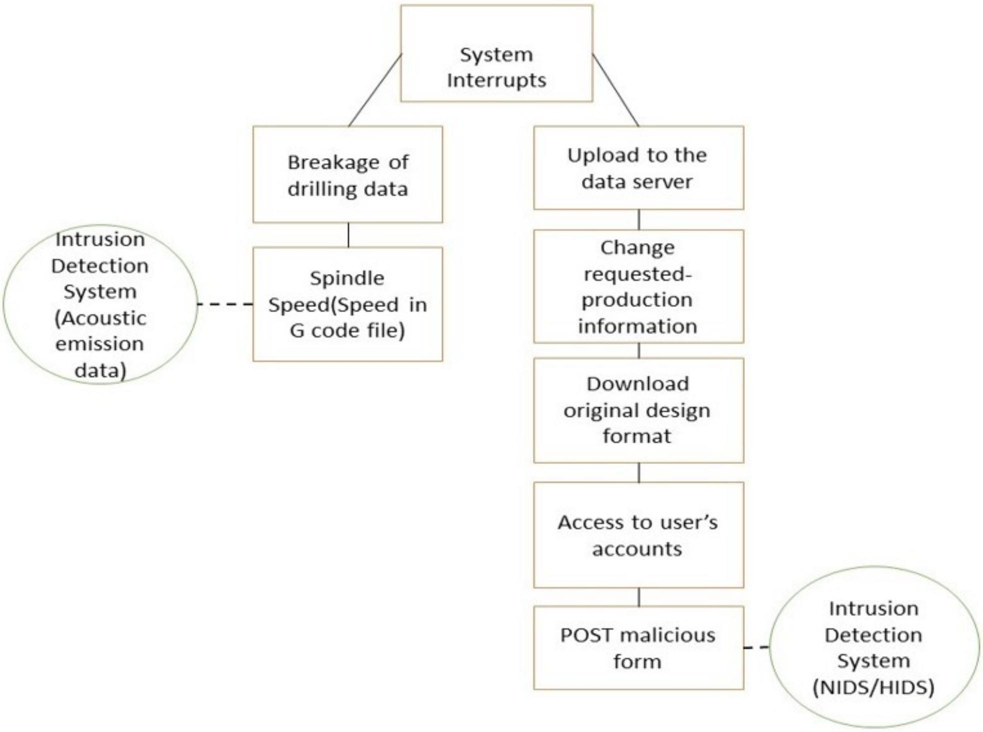

System Interrupts
Breakage of drilling data
Upload to the data server
Intrusion Detection System (Acoustic emission data)
Spindle Speed(Speed in G code file)
Change requested-production information
Download original design format
Access to user's accounts
POST malicious form
Intrusion Detection System (NIDS/HIDS)

Figure 5.3: Attack Defense Tree for SQL injection in 3D printer

When the attacker publishes a malicious form on the website, there are three possibilities:

1. User opens and fulfills the form;
2. User informs the fraud and does not use it;
3. Intrusion detection system actives and detects.

The fraud and abandon the attack and remove the form and block the access of attackers to the website. The proper model to show the behavior of all the systems by considering the random behavior of attackers and not in the deterministic time is Generalized Stochastic Petri Nets (GSPNs) as presented in Figure. 5.4. (GreatSPN tool was used for its edition).

Table 5.1: Transitions in SQL injection detection GSPN analysis

Transitions	**Descriptions**	**Firing time**
T1	Intrusion Detection (NIDS/HIDS) Positive alarm	D
T2	Intrusion Detection (NIDES/HIDS) Negative alarm	S
T3	POST malicious form	S
T4	Access to user's account	S
T5	Download Original form and user's information	S
T6	Change the user's Information	S
T7	Upload information to the data server	D
T8	New information Submitted	I
T9	Intrusion Detection (Acoustic) Positive alarm	D
T10	Intrusion Detection (Acoustic) Negative alarm	D
T11	Spindle Speed Requested Production	S
T12	Attempt to Breakage of drilling bits	D
T13	Breakage of drilling bits	I
System Interrupts	System Interrupts	I

In Table 5.1, all transitions for possible scenarios in cyber-attack are provided. For T2, T3, T4, T5, T6 and T11. firing delay is stochastic and can be different for each attack. T7, T9, T10, and T11 firing delays are in an interval time that depends on the system. Cyber attacks transition on Petri nets is a combination of the deterministic and random firing delay distribution. The objective of the analysis of the system is to reduce the interval time to detect the attack and also, to distinguish between false and true attacks. In Table 5.1, Immediate (I), Stochastic(S), and Deterministic(D) transitions are listed.

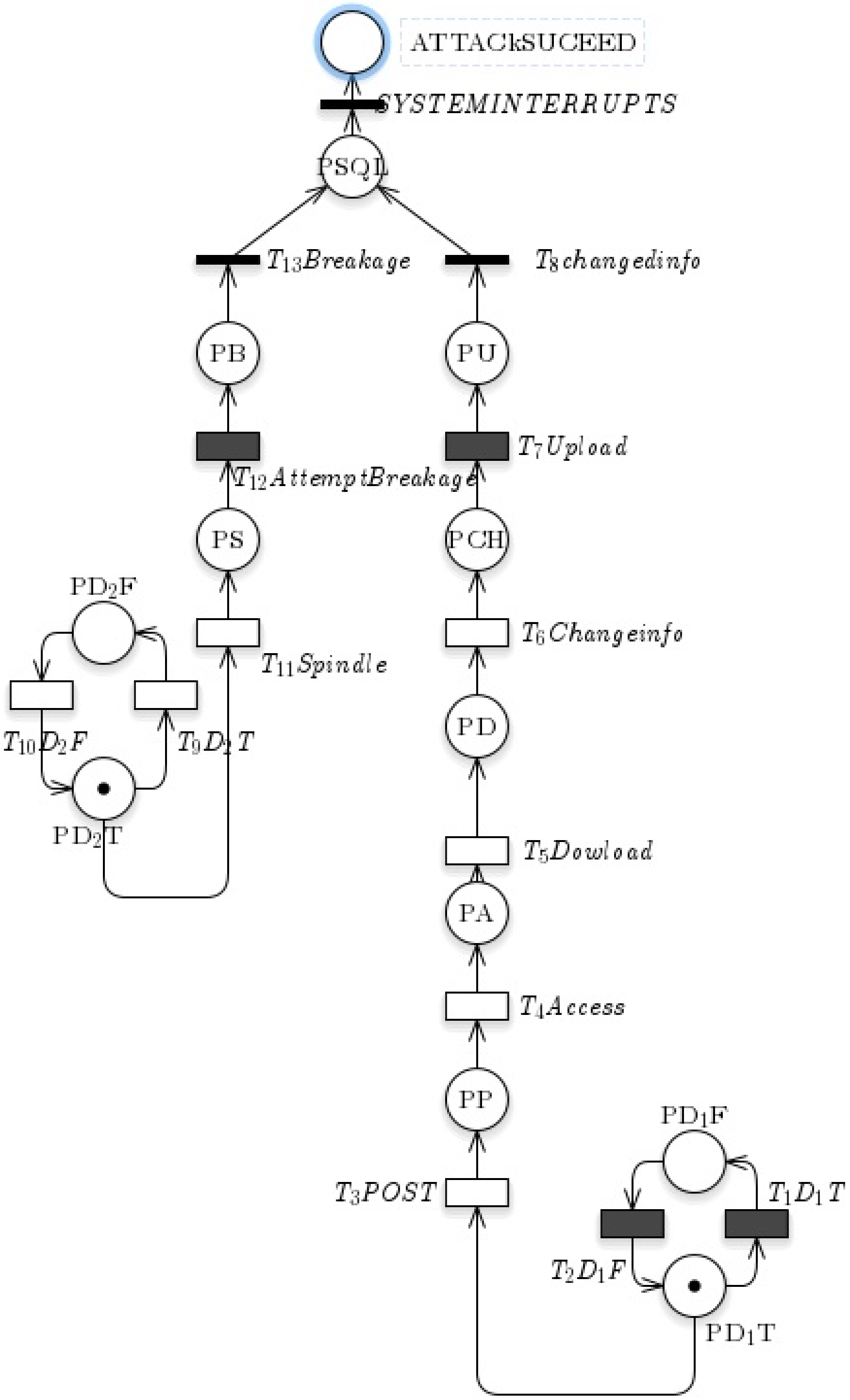


Figure 5.4: Attack-Defense Tree translated to Generalized Stochastic Petri Nets

5.2.3 GSPN VS. CPN

The GSPN model that was suggested may successfully represent both the dynamic of the ADT and the behavior of the system. However, having diverse types of data is essential for maintaining both cyber security and cyber resilience. For example, the IP/TCP request packet contains a variety of information, including the source IP, the destination IP, the protocol type, and the body information. In order to model this kind of request on a website, several separate places in GSPNs are needed. Each place describes with its unique sort of token. Using CPN or TCPN is the alternative method to analyze the performance and behavior of systems while simultaneously reducing the size of the model.

An additional benefit is a potential for employing hierarchical CPN to fold systems as subsystems. This method allows the designer and the analyst to analyze the impact of the behavior of each subsystem on the overall performance of the system, while at the same time allowing the designer and the analyst to consider each subsystem's behavior in isolation.

5.3 Semantic of Mapping GrSMs to CPN

It is possible to display a variety of attributes in each node by CPNs, including probability, duration, and cost, amongst others. The modeler is assisted in computing the values as well as representing the data by colors (in CPN Tools: Colour sets).

5.3.1 Preliminaries ACT

AT [188], ADT [189], and ACT [190] all contribute new semantics and formalization. Because the introduced formalism used different notations, logic, and presentations, I need to use completely new semantics to generate each of these security analysis trees automatically.

A_k an attack event

D_k a detection event

M_k a mitigation event

CM_k a countermeasure

$ACT = \{V, \psi, E\}(V : setofallverticesinACT,\psi$: set of all gates in ACT, E: set of all edges in ACT) where V=$\{\forall k, v_k :\in \{A_j\} \parallel v_k \in \{D_i\} \parallel v_k \in \{M_l\}\} Where A_1$, A_2,..; D_1,D_2,...; M_1, M_2,... are the events of the ACT,$\psi = \{k, k : k\} AND, OR, k-of-ngate, E = \{k, ek : ek(vi, j) \| ek(i, j)\} and X = (xA1, xA2, ...xD1, xD2, ...xM1, xM2, ...)$ is a state vector for the ACT where xAk, xDk, xMkare the boolean variables associated with events Ak, Dk, Mk respectively

5.3.2 Definitions

Considering the CPN definition [15] as follows, I introduce the mapping rule from ATs to CPN.

Definition CPN.[15] A non-hierarchical Coloured Petri Net Module is a nine-tuple $CPN = (P, T, A, \Sigma, V, C, G, E, I)$, where:

1. P is a finite set of Places.
2. T is a finite set of transitions T such that $P \cap T = 0$.
3. $A \subseteq P \times T \cup T \times P$ is a set of directed arcs.
4. Σ is a finite set of non-empty colour sets.
5. V is a finite set of typed variables such that Type $[v] \subseteq \Sigma$ for all variables $v \in V$.
6. $C : P \rightarrow \Sigma$ is a colour set function that assigns a colour set to each place.
7. $G : T \rightarrow EXPR_V$ is a guard function that assigns a guard to each transition t such that Type $G(t)$= Bool.
8. $E : A \rightarrow EXPR_V$is an arc expression function that assigns an arc expression to each arc a such that Type $E(a) = C(P)_{MS}$, where p is the place connected to the arc a.
9. $I : P \rightarrow EXPR_0$ is an initialization function that assigns an initialization expression to each place p such that Type $I(p) = C(P)_{MS}$.

5.3.3 Rule Sets

The proposed CPN model in this work allows the perception of the impact of selected behavior by both intruders and defenders, as well as the consequence of their interactions on the system based on the given attack scenario. Input to the model is intruder behavior which also shows possible vulnerabilities of the systems, such cases are depicted in Fig. 5.6 as attack nodes. Assuming that states of the systems will be represented by places (P), taken actions for each type of attack will be represented by transitions (T), and each type of attack, defense, and mitigation strategies, also metrics, or attributes in ATs be declared by a Colour set Σ in a CPN, I set the mapping rules as follow [191]:

Rule 1. *Root Nodes Mapping*: The roots in ATs will be mapped to the final place P_{final} in a CPN model which is represented by an attack-type Colour set containing attacks value(/s).

As described in subsection 3.2.1 the root in ATs is dedicated to the ultimate goal/result that intruders want to achieve in different ways, which can be interpreted as a state of the compromised system in the CPN model. As per the focus of this work is on cyber-security, I employ cyber expressions and call the final place in the CPN a cyber-attack success. Nevertheless, the attempts to exploit a system technically have two possibilities of success and failure. In the case of the attacker´s attempts failure as a result of defense and/or mitigation systems interference, another state (place in the CPN) needs to be defined to also meet the model "liveness"as the final state containing defense/ mitigation value(/s).

Rule 2. *Leaf Nodes Mapping*: The leaf /atomic nodes in AT and AT refinements be mapped to the initial place in the CPN model assigned by $C : P \rightarrow \Sigma$ which containing $[v] \subseteq \Sigma$ representing attack/defense/mitigation types in the ATs.

Both bottom-up and top-down methodologies can be used to illustrate ATs; which approach is used is determined by the purpose and the level of awareness of the system's defenses and vulnerabilities. Bottom-up thinking helps rely on the abilities and opportunities of the assailant and can assist in profiling the intruder's conduct and the possibilities they may present. In ATs, there are a few but a restricted number of nodes that are atomic nodes. These nodes are characterized as follows in table 3.1.

In CPN they are shown by multisets which represent the possible behavior of the intruder. The consequence of the atomic behaviors will be shown as a sequence of the state and the color set will be changed.

Rule 3. *Intermediate/sub goals*: Sub-goals are consequences of previous events in ATs which will be mapped to CPN as a sequence or AND/ OR representation. Intermediate goals show the dependency on the events in the system. They can be the result of one or more events. The logic gates (AND, OR, NAND) determine the sub-goal conditions. IN ATs, if the intermediate goal satisfies immediately after the previous node, it is translated as a sequential. In the case of AND/OR, and NAND sees Rule 5.

Rule 4. *Edges Mapping*: The path and connection of the events illustrated by arcs in CPN and their directions show the path. $A \subseteq P \times T \cup T \times P$ is a set of directed arcs.

Rule 5. *Combiners Mapping*: Logic gates in GrSMs are translated in the CPN as:

5.1 *"AND", "OR"*: The "OR"combiner in ATs has the same concept and functionality as "concurrency"in PNs, refer to Figure. 3.3. In the same way, the "AND"combiner is translated to "synchronization"in PNs, Figure.3.4. As a result, the logical gates in ATs are translated as AND transitions and OR transitions respectively in CPN as shown in Figure 5.5.

5.2 *"NAND"*: The "NAND"gate, which is specific to ACT and models countermeasures (considering detection and mitigation) is translated into a sub-net using guarded transitions (control flow) in the CPN, where outer place (Place P7 in Fig. 5.5) will be marked whenever at least one of the two incoming dependencies failed (related to detection and/or mitigation) which means that the guards are evaluated as unsuccessful.

As shown in Tables 3.3-3.5, different combiners or logical gates are applied in ATs refinements. In Table 5.2 the logic and result of the gates are provided.

Table 5.2: Logic of Defense System by Logical Gates (AND /NAND)

Mitigation	**Detection**	**Result (AND)**	**Result (NAND)**
1	1	1	0
0	1	0	1
1	0	0	1
0	0	0	1

Rule 6. *Attributes/metrics Mapping*: They are colsets that can be assigned with different color sets. The attributes or measurements (referred to as metrics in the context of ATs) such as cost, probability, etc. can be specified as a closet with different types, including

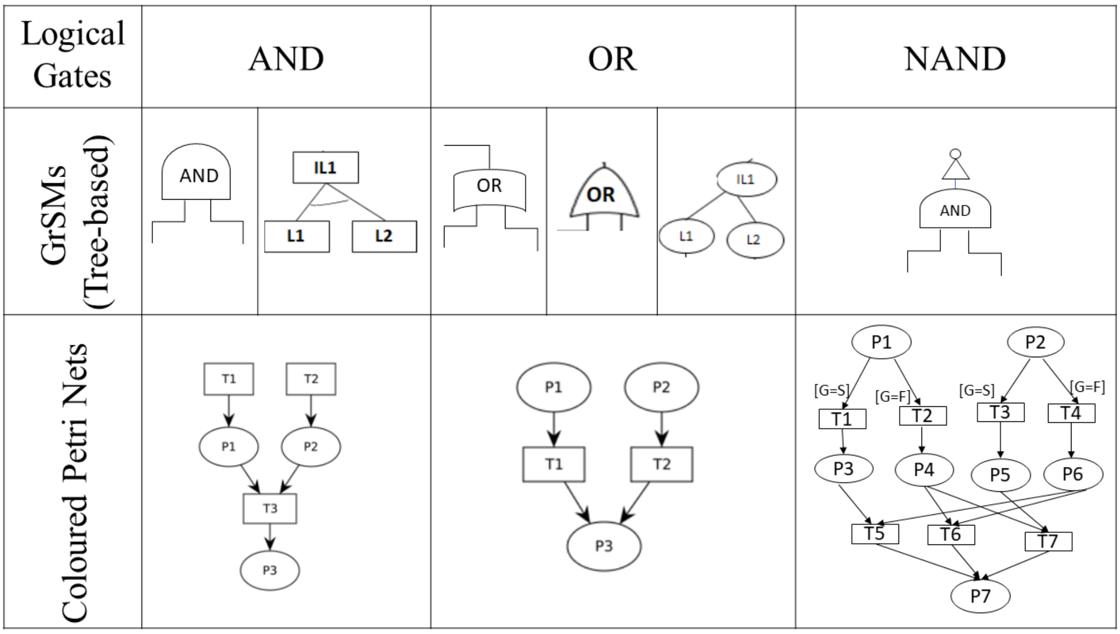


Figure 5.5: AND,OR and NAND gates in CPN

INT, Time, Boolean, Float, and so on, and can be allocated to the data token. For example, the cost can be considered an INT metric for the cost of each attack and intrusion detection or mitigation. The **PRODUCT** in CPN indicates the allocation. An event can have multiple metrics simultaneously. By introducing metrics in CPNs, it is possible to perform both qualitative and quantitative analyses.

5.3.4 Graphical Representation

For testing the feasibility of the work to security analysis, I borrowed a scenario from [74] and integrated the costs of attacks and defenses. In the first step, the translation of ACT to CPN is provided and in the next step, the cost computing is considered in subsection 5.3.5.

Figure 5.7 represents the CPN model translated from the ACT 5.6 taking into account all the rules conveyed in this section.

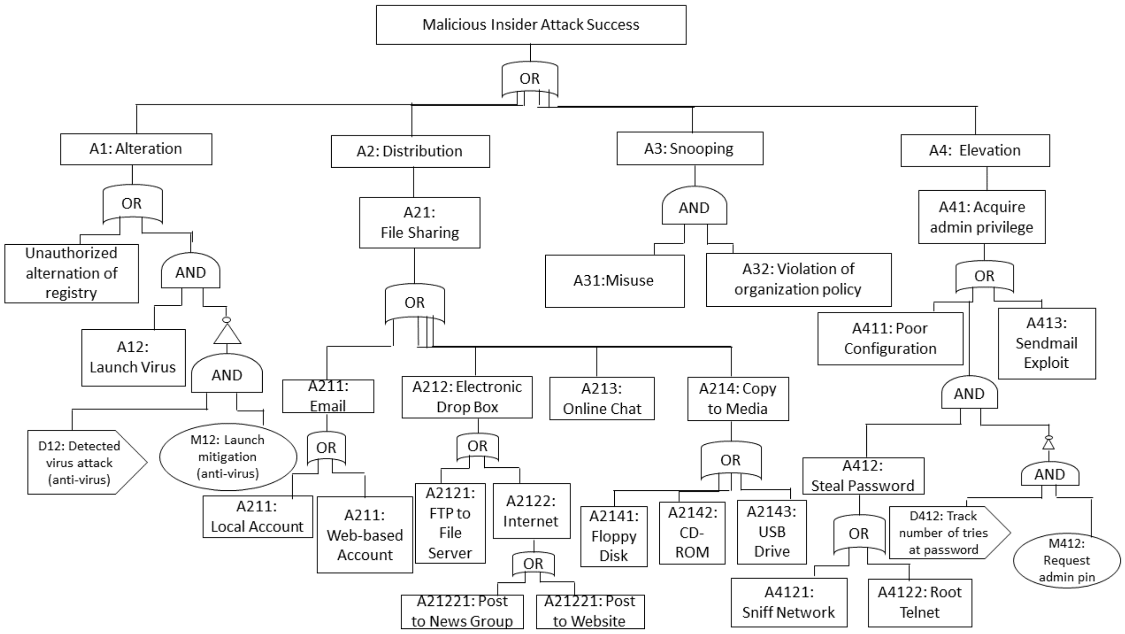


Figure 5.6: Attack Countermeasure Tree

5.3.5 Computing Node

Computing Cost as an attribute of an attack and defense system: This calculation is necessary to combine action costs whenever more than two transitions fire. These transitions can be related to malicious behaviors from attackers or countermeasures from defenders. When one of the transitions related to the combination gates (AND/OR) fires, along with changing the system's state, the cost of the actions is calculated by the transition called "computing transition". It receives two cost values from the place and returns the "sum"of the costs related to the activities.

In fact, the impact of each behavior provides another state of the system that depicts if the system is protected by a defense mechanism or intruded on by the attacker. Along with the system's state, the values regarding ca(i), cd(j), cm(k) (where i,j,k correspond to the actions) show the cost of the selected behavior of the attacker (Table **??**).

For instance, the computing node of attack cost of "A4121"and "A4122"is shown in Figure 5.8 by "CMP412". In this specific scenario, I assumed that all types of attacks initialized and proceed with a unique system (including humans) as it is introduced in the referenced scenario. As it is shown in Figure. 5.9, the computing nodes are transitions that make a sum for cost values for fired transitions (means taken and successful attacks). The details of the attack and defense analysis computed and produced by CPN Tools are given in Appendix B. Table 5.3 and 5.4 show the result of quantitative analysis of the cyber attack and defenses.

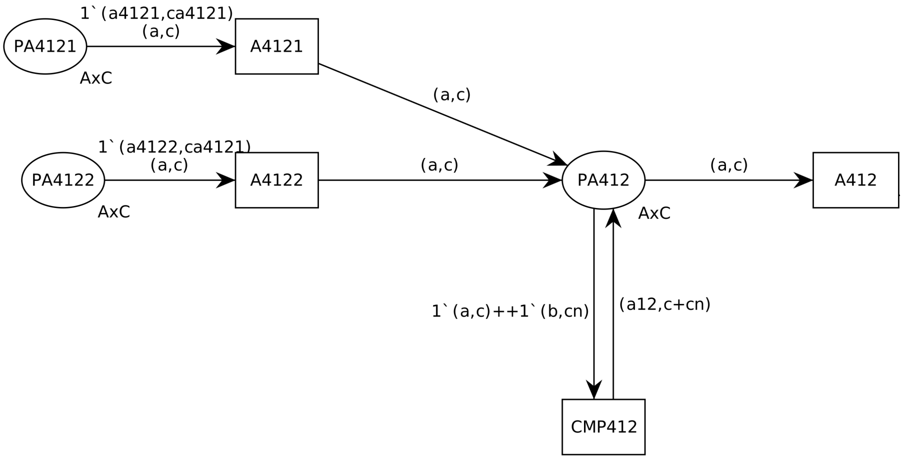


Figure 5.8: The Computing Node

Table 5.3: Running different Scenarios and Analysing Costs by CPN model - Cyber Attack

Attempt	Initial Attack	Cost	Impact	Dependency
no.1	PA21221	30	A2	N
no.2	PA21222	10	A2	N
no.3	PA31	30	A3	PA32
no.4	PA32	15	A3	PA31
no.5	PA4122	40	A4	N
no.6	PA12	60	A1	N
Total Cost		185		

Table 5.4: Running different Scenarios and Analysing Costs by CPN model- Defense

Attempt	Defense Systems Performance		Cost		Result
	Detection	Mitigation	Detection	Mitigation	
no.1	N	N			Compromised (A2)
no.2	N	N			Compromised (A2)
no.3	N	N			Compromised (A3)
no.4	N	N			
no.5	D412	M412	0	70	Attack stopped (A4122)
no.6	D12 Failed	M12	100	25	Compromised (A1)
Total Cost			100	95	195(Total)

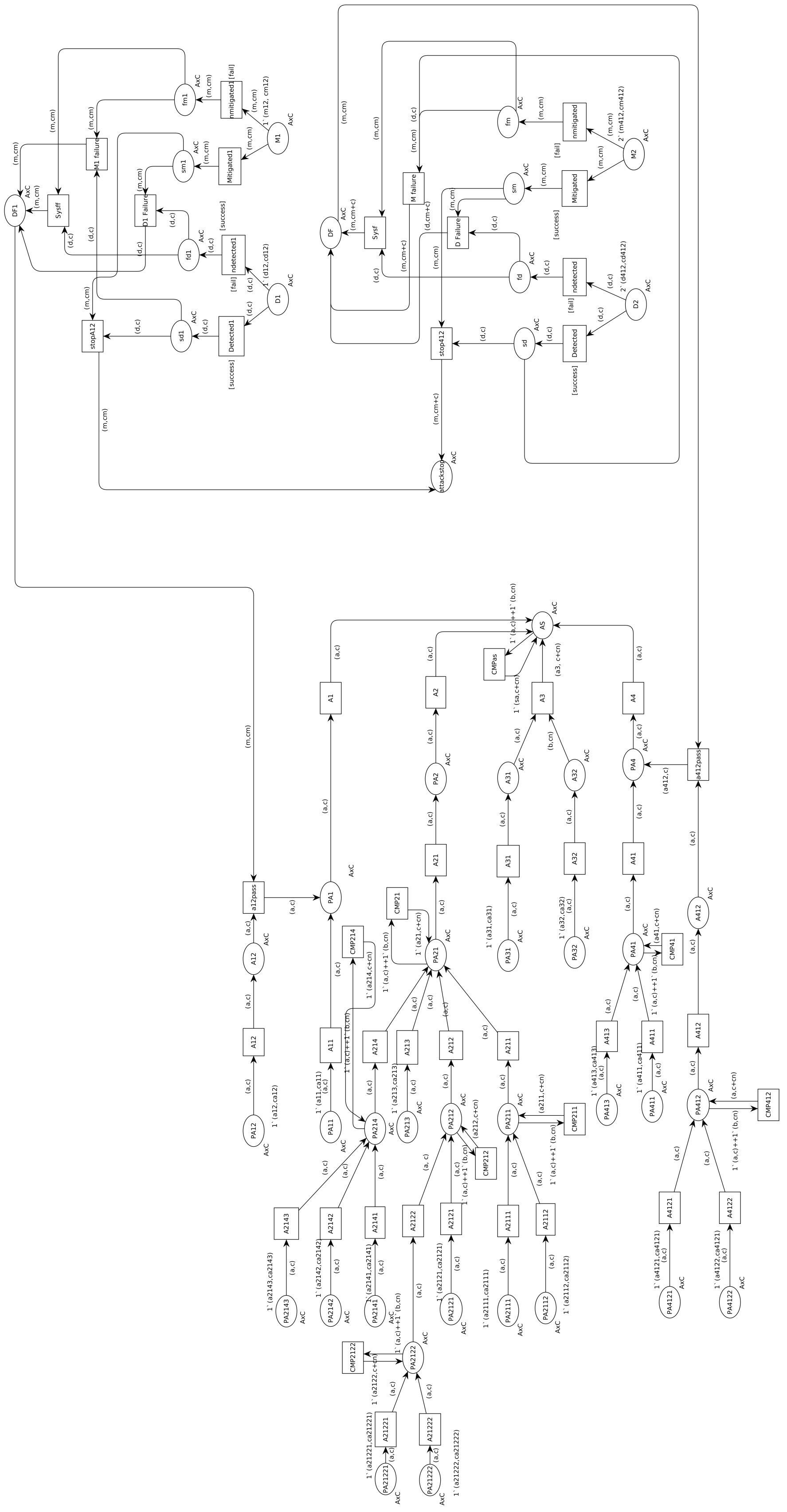


Figure 5.9: The CPN with Computing Nodes

5.4 Cyber-Resilience by CPN Notations

In chapter 2, Figure 2.4 shows that cyber resilience requires cyber security analysis. Therefore, GrSMs (which are tree-based models) are utilized as a potent tool to illustrate various scenarios related to system vulnerabilities, potential attack routes, as well as possible defense and response strategies. However, simulate all of the possible scenarios using CPN and/or CPN beneficial to the system´s resilience evaluation. The CPN model shows the impact of a potential attack on the performance and state of the system together with implemented defense strategies and recovery statutes. It means that cyber resilience evaluation requires to have information about the effects of the defense, response, and recovery strategies on the system performance.

The analysis of the system´s performance is the method that I use to measure resilience. In subsection 5.3.2, the preliminary of the proposed model for a CPSS is provided. In this regard, the characteristics of the CPN, such as its liveness and its safe behaviors, are what define which scenarios are successful. In normal performance and fully recovered systems or successfully absorbed attacks, it is necessary to check and make sure that the resources that are involved in the IDSs and Web services procedure will ultimately be carried out at least once. I have determined a time constraint for defenses and attacks.

As mentioned above, the framework can be described as $<V, \beta, M>$ Every $v \in V$ can be mapped to an input place to the system. Every $b \in \beta$ is a whole workflow described by a Petri net that defines the sequence of events needed to be taken if certain behavior $b \in \beta$ dominates. The mode $m \in M$ is a selection that dictates which set of behaviors will be activated and which are not. To give CPN model the capability to express the security properties of the modeled system and ensure its compatibility with the existing formalism in the following interpretation of the CPN components is proposed (a CPN which conforms to the conditions given below):

1. I determine an expected and desired interval time for transitions (events),

2. I consider a defense or recovery strategy successful if the interval time is fulfilled, or else the attack attempt is considered successful,

3. The performance analysis consists of time also cost these two parameters will be calculated in different protestations in beneficial of readability,

4. In the end, if the net is alive for all the normal tasks, then the system is resilient. But, it has to show deadlock for the attack attempts if the defense strategies are successful.

5.5 Chapter Summary

In this chapter, I provided an answer to **RQ2** that requires the set rules to translate existing non-state-based graphical models for the analysis of cyber security in the CPSS. It was also important to define computing rules for quantitative analysis purposes. In this chapter, I introduced six rules for specifying GrSMs translation to a CPN model that is applicable for GSPN too. I explained how CPN models are compatible with and complementary to GrSMs in sense of showing the dynamic of the attacks and defenses. I showed and explained the result with a concrete example from Attack Countermeasure Tree.

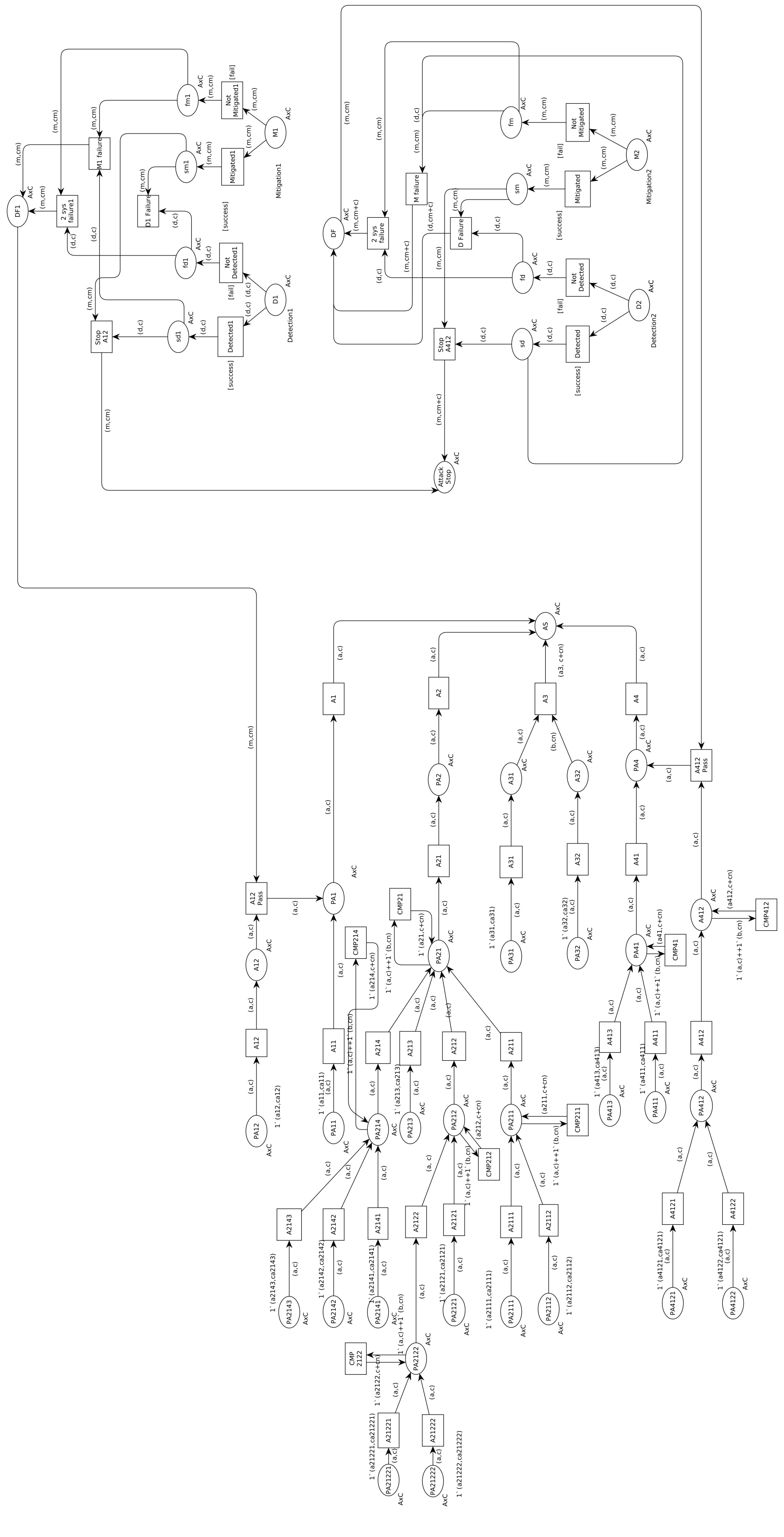


Figure 5.7: CPN mapped from ACT [74]

6

Design an experimental Attack Defense Simulator

We cannot solve our problems with the same thinking we used when we created them.
Albert Einstein (1879-1955)

6.1 Introduction

To validate and authenticate my research, I did the penetration test on the real use case and I used two separate methods to collect and examine data. The first approach entailed setting up a separate lab and conducting mock attacks, while the second entailed obtaining prior knowledge from our university's information technology department.

Designing a simulation environment for this work had two main challenges it must be isolated and we had to build a lab from scratch that should be adaptable to security scenarios in CPSS. It needs to point out that system users and the security team (red and blue team) are considered integral parts of both testing and risk assessment hence human facets play a notable role in cyber security incidents. In this regard, scenarios help explain and formulate these complex dependencies and relationships in the system components and associated tasks.

Scenarios are simulated or emulated networks comprising traffic as well as potential threats in the network layer (PAN, LAN, MAN, WAN), software, and hardware implemented through Virtual Machines (VMs), Containers, or Sandboxes. In a bid to comprehensively represent target networks, the scenario can also feature other system peripherals and appliances. The simulated network environment is injected with traffic representative of user activities e.g., web scanning, email phishing, and other server communications, and real-life attack scenarios such as in Control or Data centers are deployed. A predefined attack scenario library as well as custom-built scenarios are integral to the framework [192].

The rest of this chapter is organized as follows: Section 6.2 explains the framework of the designed experience to validate this thesis as well as three scenarios for three different types of attacks; then in section 6.3 the architecture and applied techniques to run the test are provided, also based on the tests the ADT is built and shown; and finally, in section 6.4 the summary of the chapter is provided.

6.2 Design Framework

The motivation scenario is related to web-based applications and services. To describe the idea, I borrowed an example from [193]. A web user (like a web commerce website) logins in a request receiving some information via the webpage- From the other side, the request passes Firewall and IDS. These prevention and detection systems are designed and used for the web services, to check the healthiness of the requests, and at the same time, the security administrations monitor and analyze the logs on the website network. The well-behaved request will pass to the web server. In the backend, there is a (MySQL/NoSQL) database that stores all the store's information, which includes product inventory, product description, customer account, and order history. The web server communicated with a database to send the requested information to the customer; customers receive the information at the end of the process. There is a possibility that the user is an attacker and can access the web server by some web hacking techniques, such as Buffer overflow, SQL injection, Social engineering, et al., and then can manipulate the web services. So, as a consequence, the system might be crashed, or the customer's and store's credentials are leaked and stolen. The introduced model follows the framework presented in the MITRE framework for use cases [59]. I created three scenarios and for each, I requested the experts to choose or define different actions regarding system security based on various conditions. I applied two indicators of abilities and organizational responsibility to classify human behavior. I considered cost and time as two criteria for measuring threats and defense impacts on the systems.

What I did to design the cyber-resilience by TCPN approach had a top-down concept. It means I created the high-level concept of all the scenarios and then unfold them in different sub-systems in the hierarchy TCPN to reduce the complexity and the net size. Another advantage of this approach is that changes in sub-systems do not have a huge impact on the whole designed model. It means that each mechanism's process is illustrated in different sub-pages of the net's high level.

Finally, based on the behavior of the net, the performance of the system can be divided into four levels:

Level 1: The attack is resolved and stopped. Systems are secured

Level 2: An attack is identified but the response system is failed to stop the attack/threat. System Awareness

Level 3: The attack is not distinguished and the system is disturbed partially. The system was interrupted but the performance is not under the threshold and recovering

Level 4: The attack is successful and system performance is not recovered

6.2.1 Simulation Characterises

For the objective of this work, I have modeled and applied snort architecture and detection mechanism as a networked-based IDS and Firewall as a first-layer defense system by CPNs in the application of SQL injection. The response system includes a set of actions that be taken by the SIEM administrator regarding the type of intrusions. The recovery phase in resilience consists of all the places and transitions after the intrusion/s. Considering this incident as a scenario, I can infer a list of broad scenario elements as follows.

- An attacker
- Users that the attacker targets initially
- A cyber system and data that the attacker targets
- System security personnel that detects the incident
- Interactions between the attacker, users, the system and the security personnel
- A wide network infrastructure that facilitates connection between cyber systems and people.

The above elements can be categorized under two groups: cyber systems (including data and wide network infrastructure), as observed in the Proxmox platform, and actors (attacker, user, and system security person).

The attacker is a vague term because it is an unknown party in the majority of cyber incidents. In this sense, an attacker may be an individual, a group, or a state-funded organization. Because of this ambiguity, attackers are frequently not explicitly represented in cyber-security simulation scenarios. Rather, their interactions with the cyber system are pre-programmed [194]. In my case, there is no difference between the parties but what is important is that each of the transitions contains a specific IP address with a specific behavior/action.

Simulators

Simulators for representing cyber vary from general-purpose simulation tools to those focused on the creation of networks and the evaluation of three types of cyber-attacks including DoS, Malicious code injection, and Email Phishing.

6.2.2 Classification and Data Extraction

Based on the work I have done in developing a cyber range and after the first screening of the literature, I The scenario describes and provides documentation, summaries, action orders, etc., to ensure the representative operational context supports

I used the MITRE use case resilience framework [37] to create scenarios which are depicted in figure 6.1.

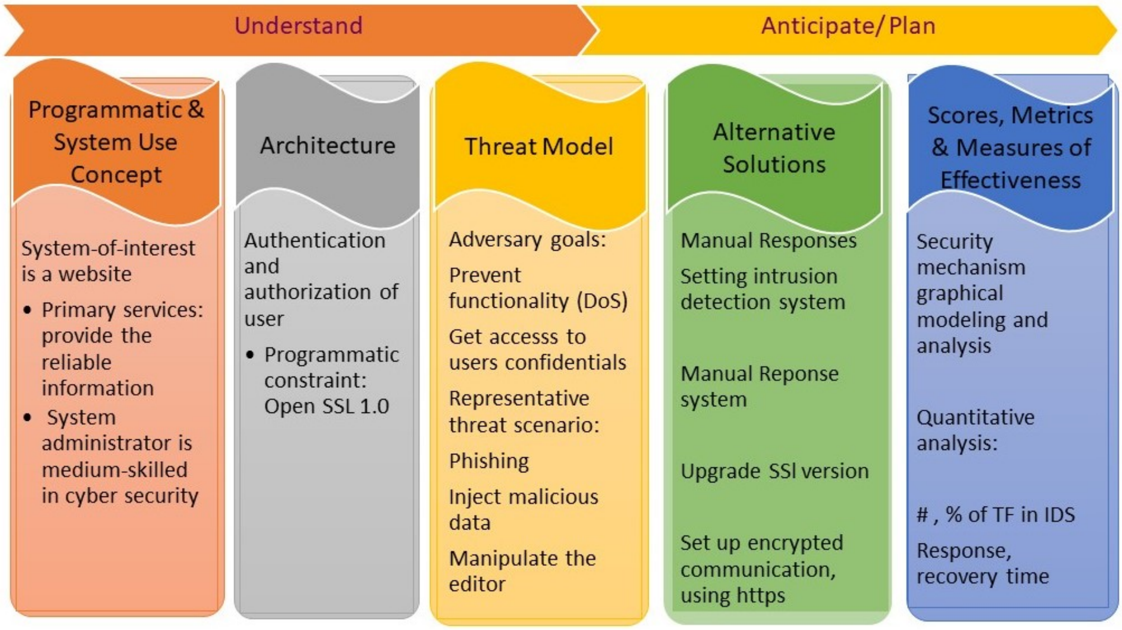

Understand
Anticipate/ Plan
Programmatic & System Use Concept
System-of-interest is a website
• Primary services: provide the reliable information
• System administrator is medium-skilled in cyber security
Architecture
Authentication and authorization of user
• Programmatic constraint: Open SSL 1.0
Threat Model
Adversary goals:
Prevent functionality (DoS)
Get accesss to users confidentials
Representative threat scenario:
Phishing
Inject malicious data
Manipulate the editor
Alternative Solutions
Manual Responses
Setting intrusion detection system
Manual Reponse system
Upgrade SSl version
Set up encrypted communication, using https
Scores, Metrics & Measures of Effectiveness
Security mechanism graphical modeling and analysis
Quantitative analysis:
# , % of TF in IDS
Response, recovery time

Figure 6.1: The MITRE Use-case Resilience Framework for the Proposed scenarios

6.2.2.1 System-of-Interest

The system of interest is a cloud-based tool chain offering a complete set of Petri net tools with a Web interface supporting digital controllers development. The tools include an interactive graphical Petri net editor, a model-checking subsystem composed of a state-space generator, state-space visualization, and a query system, and automatic code generation tools that produce software “C” code or VHDL hardware descriptions ready to be deployed into implementation platforms. All interactive tools are executed directly in the user’s Web Browser using AJAX principles, but file-storage and intensive processing operations are processed in the cloud. Take advantage of standard W3C technologies, such as SVG (Scalable Vector Graphics), AJAX (Asynchronous Javascript and XML), and XSLT (eXtensible Stylesheet Transformations), to offer full-featured edition capabilities inside standard compliant Web browsers, such as Chrome, and Firefox, Opera or Safari. Multiple users can perform collaborative work by sharing the clipboard contents. Parts of models can be copied to the clipboard and saved on the server, enabling other persons logged under the same user account, to download the shared clipboard contents and paste them on other models [195].

Architecture. Autonomous events are typically used in solutions composed of multiple hardware components, defined by several IOPT models or other hardware design formalisms, implemented in the same hardware platform or distributed GALS architectures [3]. The architecture of the tool is presented in Figure 6.2

Installation. To avoid any unwanted interruption in the performance of the system, I

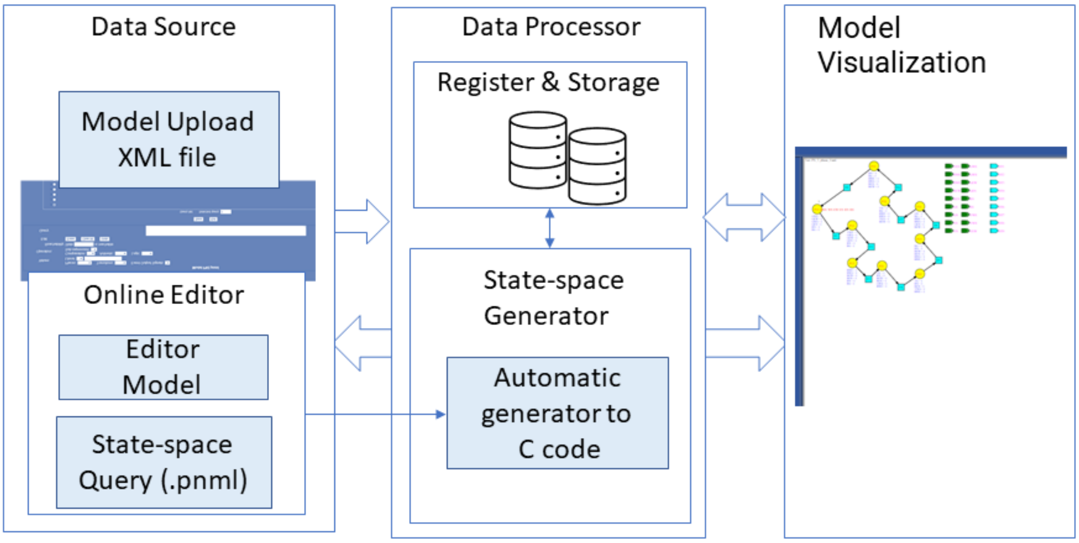


Figure 6.2: Victim System Architecture

duplicate the system on the virtual environment.

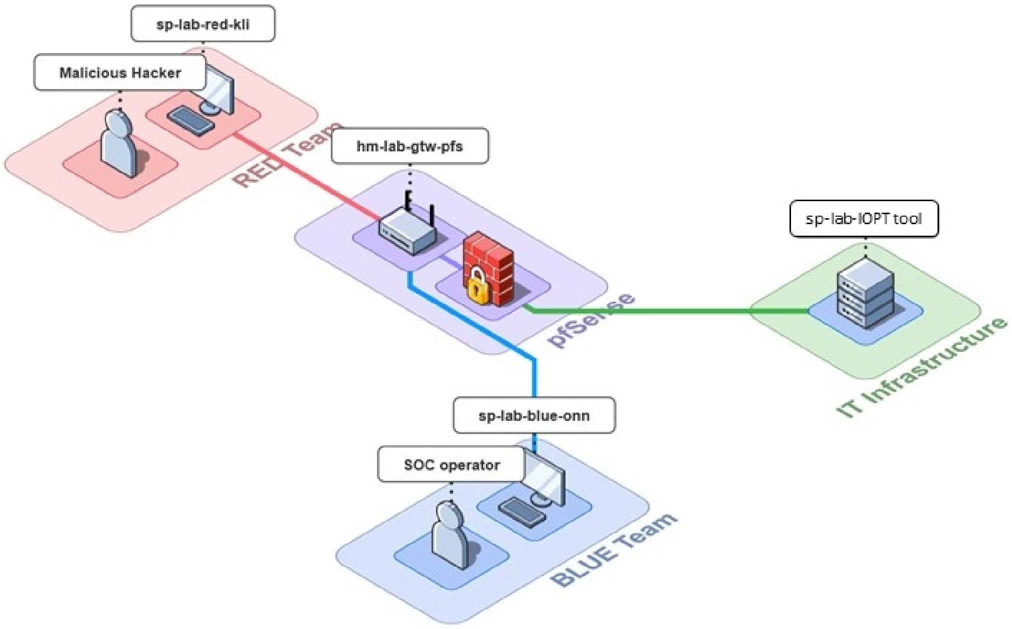
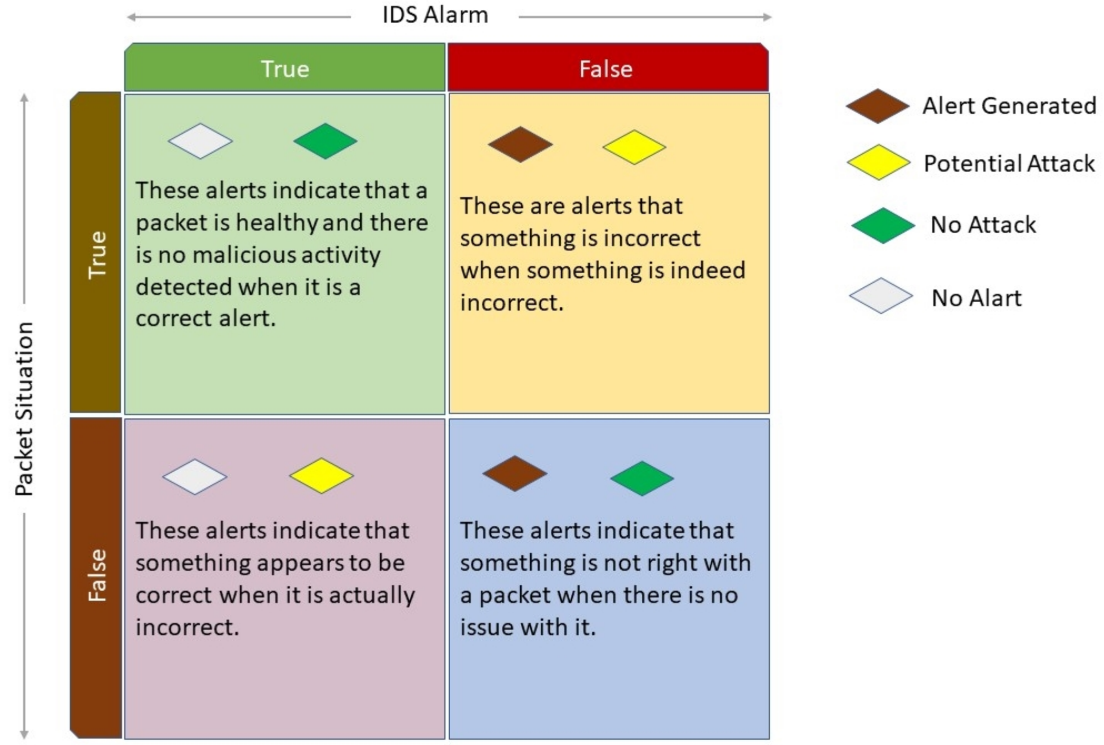


Figure 6.3: Isolated Lab High-level Conceptual Design and Components

6.2.2.2 Intrusion Detection/ Prevention Systems

Regardless of what program is designed or used for IDS/IPS, the alert result is categorized into four categories as it is shown and described in Figure 6.4.



Packet Situation	IDS Alarm: True	IDS Alarm: False
True	These alerts indicate that a packet is healthy and there is no malicious activity detected when it is a correct alert.	These are alerts that something is incorrect when something is indeed incorrect.
False	These alerts indicate that something appears to be correct when it is actually incorrect.	These alerts indicate that something is not right with a packet when there is no issue with it.

Figure 6.4: Intrusion Detection Systems / Intrusion Prevention Systems Performance

6.2.3 Scenario

The motivation scenario is related to web-based applications and services. A web user (like a web commerce website) logins in a request receiving some information via the webpage- From the other side, the request passes the firewall and IDS. These prevention and detection systems are designed and used for the web services, to check the healthiness of the requests, at the same time, the security administrations monitor and analyze the logs on the website network. In all the scenarios, defense and response strategies are applied for absorbing attacks and if they became successful the recovery plan would be implemented. All the absorb and recovery phases are a series of actions that be taken automatically by the system or manually by the security team(human).

The ultimate goal of attackers is to get access to the systems and can take control of it and in contrast, defenders' ultimate goal is not letting any unauthorized access to the system. In the following scenarios, three different techniques are considered.

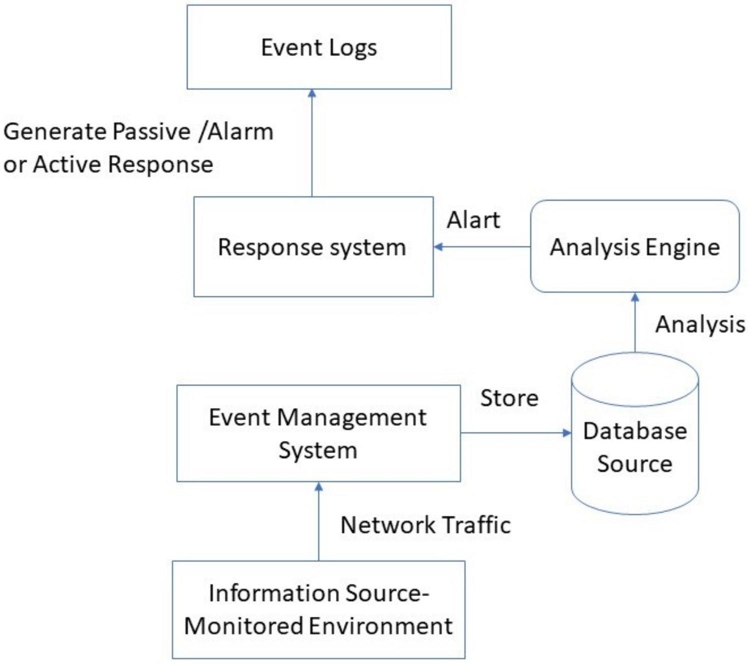


Figure 6.5: Intrusion Detection System Architecture

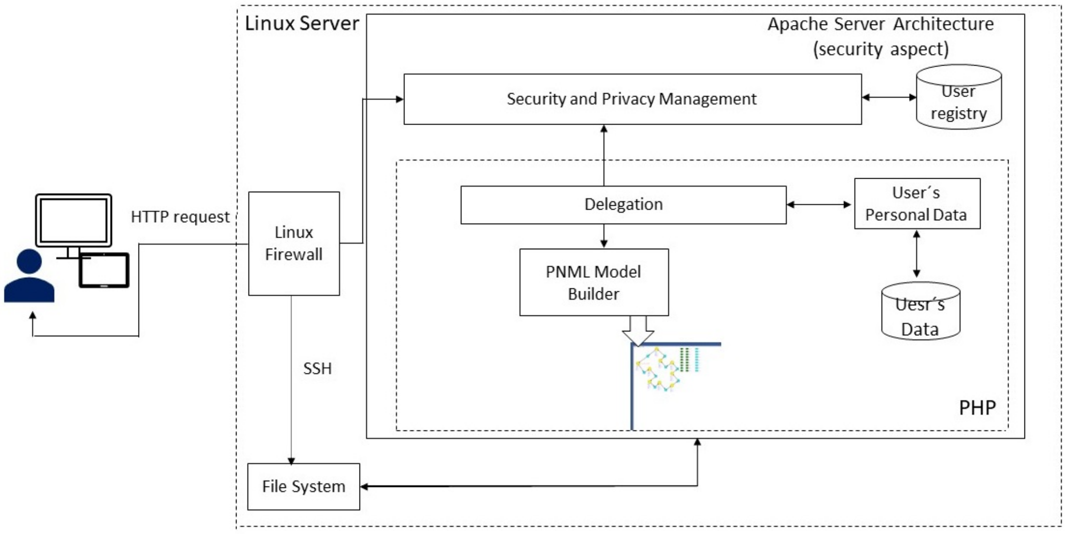


Figure 6.6: Security System in the System of the interest

6.2.3.1 Attacks

In this subsection, I describe all types of attacks that are modeled by TCPN and the applied defense/recovery plans if it is the case.

Attack 1. Compromised Database Server

Description of the attack process. The well-behaved request will pass to the web server. In the backend, there is a (MySQL/NoSQL) database that stores all the tool's information, which includes the tool´s services description, user account, and activities history. The web server communicates with a database to send the requested information to the users; users receive the information at the end of the process. There is a possibility that the user is an attacker and can access the web server by some web hacking techniques, such as Buffer overflow, SQL injection, Social engineering, et al., and then can manipulate the web services. So, as a consequence, the system might be crashed, or the user's and tool's credentials are leaked and stolen.

Scenario. A database administrator performs some off-hours maintenance on several production database servers. The administrator notices some suspicious and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator concludes that the server has been attacked and calls the incident response team for assistance. The team's investigation determines that the attacker successfully gained root access to the server.

Type of the detected attack: Remote malicious code injection.

Defense /Response Strategies: Block the suspicious IPs, Block port 443, and restart Apache.

Recovery: Load balancing and use of three servers

Attack 2. Denial of Service Attack

Description of the attack process. Considering a direct attack, an attacker arranges to send out a large number of attack packets directly toward a victim. Attack packet types can be TCP, ICMP, UDP, or a mixture of them [196].

Scenario. External users start having problems accessing one of the web services for delivering their project. Over the next hour, the problem worsens to the point where nearly every access attempt fails. Meanwhile, a networking staff responds to alerts from an Internet border router and determines that the organization's Internet bandwidth is being consumed by an unusually large volume of UDP packets to and from both the organization's public DNS servers. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address. Also, all the DNS requests from that address come from the same source port.

Type of attack: Denial of Services (DoS), direct attack.

Defense/Response Strategies [197]: Block the suspicious IP address and send it to the firewall, allow only whitelisted IPs, and Filter traffic to block the unwanted request.

To measure the traffic load on the TCPN, the following assumptions and configurations are needed.

Bandwidth network= 1 Gbps speed in Proxmox

The average volume of each package (length)for HTTP request: 150Kb

Recovery actions. Create a blacklist of IPs and abound them to reach the website. Create a White list and just filter IPs that have permission to pass.

Table 6.1: Formulate Threshold

Parameter	Average Maximum peak utilization	Maximum threshold value
Network bandwidth-Internet Link	50%	65%
DNS Traffic	5MB/h	8 MB/h

Table 6.2: Threshold for controlling DoS

Parameter	Average Maximum Packet/Hour	Maximum threshold packet/Second
Network bandwidth-Internet Link	500	650
DNS Traffic	27	44

In the scenarios, to ease the model, I assumed that all services after DoS are reachable again and the performance of infrastructures is back to the desired baseline. In this regard, two actions are needed for recovery: Access the end of the DoS situation, Restart stopped services. For measuring resilience, I consider the time for stopped services to start work as normal.

Attack 3. Phishing Email

Phishing is the most common type of attack which is easy to implement and potentially very effective. Phishing is an attack by email which normally include hyperlinks that redirect the recipient to faux net pages (clones) or malware that may be dispatched as an attachment or a download link.

Description of the attack process. An attacker send an email with this content to a victim: "HMRC: A tax rebate of 432.80 Euros has been issued to you for an overpayment in year 21/222. You can find a link to proceed: https://hmrc.taxbate.details-auth-sec.com."

Type of attack: Social Engineering (SE).

Response: Block the suspicious IPs.

For this type of attack, two different possibilities are considered based on SA present or absence. It means that the attack initiates or stops respectively.

6.3 Experimental lab set up

Within this section, I share various experimental studies conducted on susceptible systems to respond to the following research questions:

Q?How do the introduced cyber attacks and following defenses impact the performance of the system in terms of cyber security?

In this regard and based on the motivation of this thesis -Section 1.2-, the lab experience is designed following the scenario that is shown in Figure 6.7.

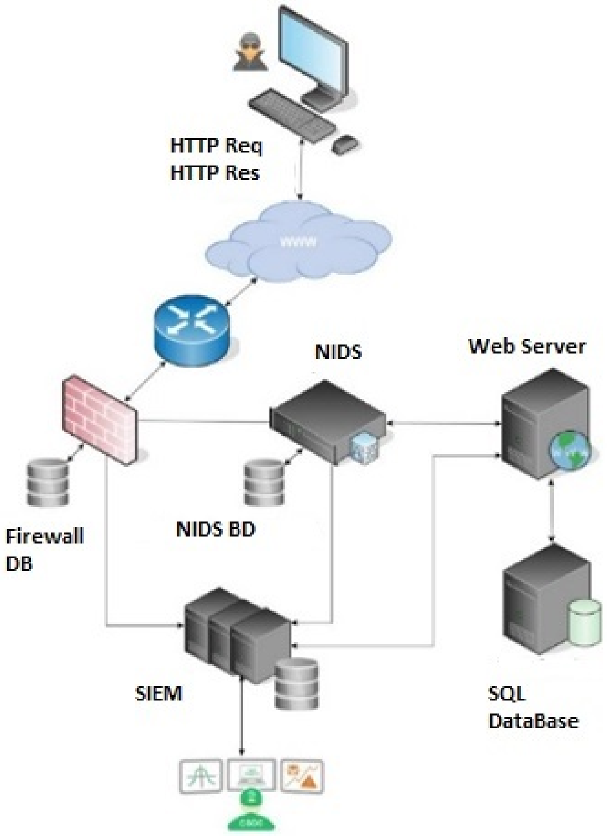
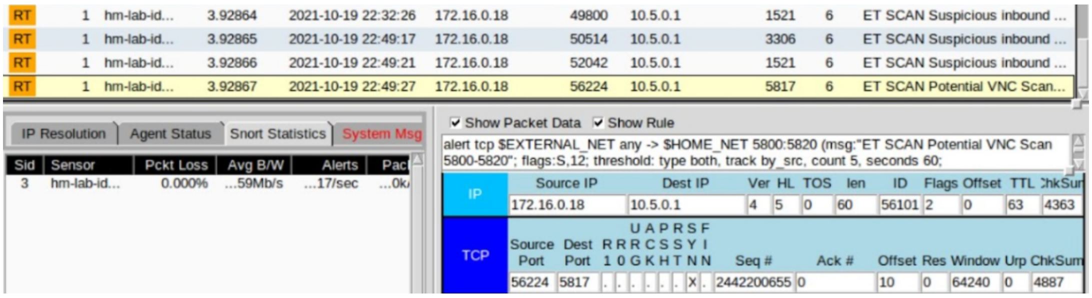


Figure 6.7: Motivating Scenario

6.3.1 IDS: Sguil by Security Onion

A packet can be malicious showing by False packet (F), or it is a healthy packet showing by True packet (T). Regarding the packet states, IDS alarms have four possibilities of True True (TT) which means the IDS recognizes the packet is Ok to pass and the packet is healthy, True False (TF) dedicated to a state the IDS recognizes the packet OK to pass but it is a malicious request and in the same way False True (FT) and False False (FF). In our scenario, I consider all the possibilities.



RT	1	hm-lab-id...	3.92864	2021-10-19 22:32:26	172.16.0.18	49800	10.5.0.1	1521	6	ET SCAN Suspicious inbound ...
RT	1	hm-lab-id...	3.92865	2021-10-19 22:49:17	172.16.0.18	50514	10.5.0.1	3306	6	ET SCAN Suspicious inbound ...
RT	1	hm-lab-id...	3.92866	2021-10-19 22:49:21	172.16.0.18	52042	10.5.0.1	1521	6	ET SCAN Suspicious inbound ...
RT	1	hm-lab-id...	3.92867	2021-10-19 22:49:27	172.16.0.18	56224	10.5.0.1	5817	6	ET SCAN Potential VNC Scan...

Sid	Sensor	Pckt Loss	Avg B/W	Alerts	Pac
3	hm-lab-id...	0.000%	...59Mb/s	...17/sec	...0k/

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan
5800-5820"; flags:S,12; threshold: type both, track by_src, count 5, seconds 60;
```

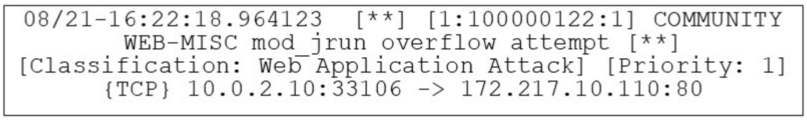
IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	172.16.0.18	10.5.0.1	4	5	0	60	56101	2	0	63	4363

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	56224	5817	.	.	.	.	.	.	X	.	2442200655	0	10	0	64240	0	4887

Figure 6.8: Seguil Alarm Message

Snort is not just a package sniffer also it is signature-based and checks the payloads.

The rules can be modified by the admin. All Snort rules follow a very simple format and define what Snort should watch for as it inspects packet header, payload, or both. Snort rules are divided into two logical sections, the rule header, and the ruling body. In Figure.6.9 a sample of a snort alarm is shown.



```
08/21-16:22:18.964123  [**] [1:100000122:1] COMMUNITY
        WEB-MISC mod_jrun overflow attempt [**]
[Classification: Web Application Attack] [Priority: 1]
      {TCP} 10.0.2.10:33106 -> 172.217.10.110:80
```

Figure 6.9: Snort Alarm Message

The message provides information on the source Internet Protocol (IP), destination IP, type of attack, time, and priority of the alarm. In the CPN model, I apply this information for validating the model. Considering the IDS (Snort) architecture, there are four main events/actions after capturing a suspicious packet. One of the most important requirements of the modeling approach is consistency with IDS principles. Therefore, it is important to define a generic IDS interface Figure.6.9 and Figure.6.8 for a resource before presenting the interface for the resource involved in our motivating scenario.

6.3.2 System Vulnerabilities and Threat Model

To proceed with the experimental test, as an initial step, I figured out the IOPT-Tools vulnerabilities by running some penetration tests. The penetration test results for system-in-interest are provided in the following list as a report from the red team.

- SSH is enabled on port 22 and there is no protection against brute force attacks. That means if you are a using weak password anyone can brute force it and get access to your server. configure your firewall and your server to block unsuccessful login requests.

- User “lab admin” can do a privilege escalation attack and become a root on that server. The reason is that you are using Apache 2.4.37. This version is outdated and vulnerable. CVE-2019-0215.

- Don’t ever trust user input. Looks like users are able to upload files. make sure they can upload only specific formats don’t let them upload whatever they want. If user input is not sanitized then the malicious attacker can upload a PHP reverse shell and get access to your server.

- Looks like you are using PHP 7.2.24 this version is outdated. This version is vulnerable to remote code execution. The stable version is 8.1.4. make sure you update your PHP

- HTTP TRACE method allowed on your server which means the attacker can gather sensitive header information about your server. It is better if you just disable it.

- I'm not sure what is going on on port 9090 but it looks like you're using Zeus-admin. The port is closed but if you ever going to use that web service make sure it is updated because that thing has a lot of vulnerabilities.

6.3.3 Attack Defense Tree of Three Types of Attacks

An intrusion, detection, and countermeasure scenario consists of the steps taken by an attempted attack from an intruder through different system gaps or vulnerabilities that are targeted at the website. The penetration test report provided in section 6.3.2 shows that how an attacker can make trouble for the system. This information helps to build the ADT and analysis the cyber security. It means the atomic actions that can be taken to proceed with the attacks based on the detected vulnerabilities are the leaves of the tree. For the given scenario associated with a set of detection systems and mitigation attempts, there are six alternatives to disturb the system including exploiting Apache mod buffer overflow, sending malicious email, creating several bots, HTTP Get/index.php,and resister flood. In Figure. 6.10 (check the end of the chapter) the ADT model for access and compromise Database is provided.

In the next chapter in Section. 7.4, I will translate this ADT to the TCPN model and evaluate the possible defense and countermeasure strategies to increase the resiliency of the system.

6.3.4 Human Behaviors in Context of Social System

Attack 3 in the section is designed to model human behavior as a victim in confrontation with an attacker behavior. Inspired by the mental model from Endsley 4.6 I created the scenario and asked random people to imagine the situation and respond how would be their reaction to the phishing scenario. Out of 10 people, 8 people had experienced a similar situation in the past and 5 of them were IT specialists. They also expressed it had happened in time or work stress, they had been trapped by phishing messages. According to the result, I categorized cognitive ability parameters which have an impact on human behavior in the process of decision-making into three groups: Skill, Experience, and Pressure. The important aspect of this modeling is how to design CPSS to raise awareness for this work in the cyber attack, then the resiliency of the system will increase.

As a result of this test, I learned when awareness increases the impact of malicious behavior decreases dramatically. In chapter 7, I will show the CPN model for the impact of human behavior on the systems in case of awareness and unawareness of potential cyber-attack.

6.4 Chapter Summary

In this chapter, I depicted and explained the experimental architecture and techniques to collect data to validate the proposed framework and model for our work. In order to design the lab configuration I considered a vulnerable system that can be visualized in an isolated lab. Also, to model human behavior, I designed an experiment based on human awareness and analyzed system logs to check the impact of the behavior on the system.

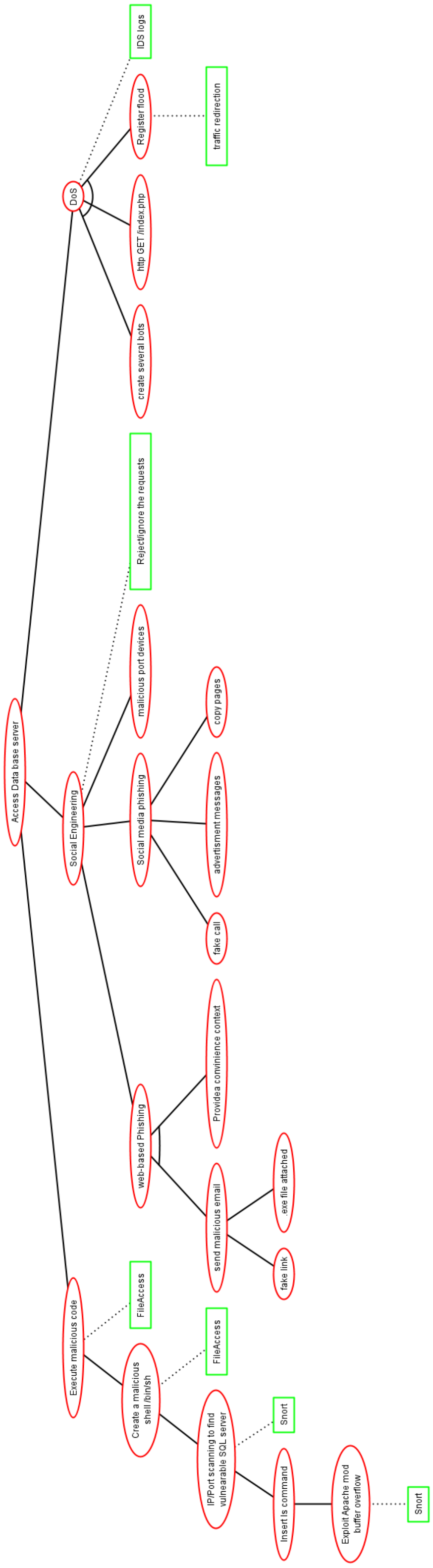


Figure 6.10: Attack-Defense Tree (ADT) for Access and control the web services

7

CPN model assessment and Hypothesis validation

Nothing is particularly hard if you divide it into small jobs.

Henry Ford

7.1 Introduction

In previous chapters, I proposed and showed the resilience evaluation framework for CPSS. I proposed to use CPN as a uniform model to describe attack paths, impacts, as well as defense and response system, impacts to mitigate the incidents in the system. I provide a simulation environment to examine our idea and acquire data to validate the proposed CPN model.

The main contributions of this chapter are to show the validity of the research hypotheses I have made in the introduction (chapter 1).In this chapter, I show how two key parts of the solution model are integrated to evaluate the resiliency of systems considering human behavior as a social component in a CPSS.

The outcome of this chapter will be CPN models for described scenarios in Chapter 6, the result of simulation by CPN Tool, and an analysis of the result of each action in sense and attacks and defense and recovery which shows the resiliency level of the system in each scenario.

The remainder of the chapter is structured as Section 7.2 provides the overall solution to evaluate cyber resilience using TCPN; Section 7.3 shows how to evaluate the performance of detection and defense systems by examining the behavior of IDS and firewall are which are modeled by CPN and show the system behavior in case of malicious injection; Therefore section 7.4 explains how to integrate time concept in the models and model the recovery plan by TCPN; In the section 7.5 focuses on modeling human behavior and creating TCPN model for DoS and SE scenarios; In section 7.6 the behavior of the system is analyzed and the level of the resiliency of a system in face of the three types of attacks is evaluated; In section 7.7 the hypothesis verification is explained and finally in the section 7.8 the conclusion of the chapter is provided.

7.2 An Overview of the Proposed Solution Framework

Our approach in this work to evaluate and model the system´s resiliency is shown in Figure 7.1. The business model to make a system cyber resilient is provided with many work groups as I mentioned in chapter 2. In this work, I proposed and examined the applicable technique to follow the standard framework. make systems resilient improving and examining at design time and improving during running time. Here I focus on the design part but the idea for simulation can be expanded to the run time as well. In this case, I test the functionality of systems in simulation time.

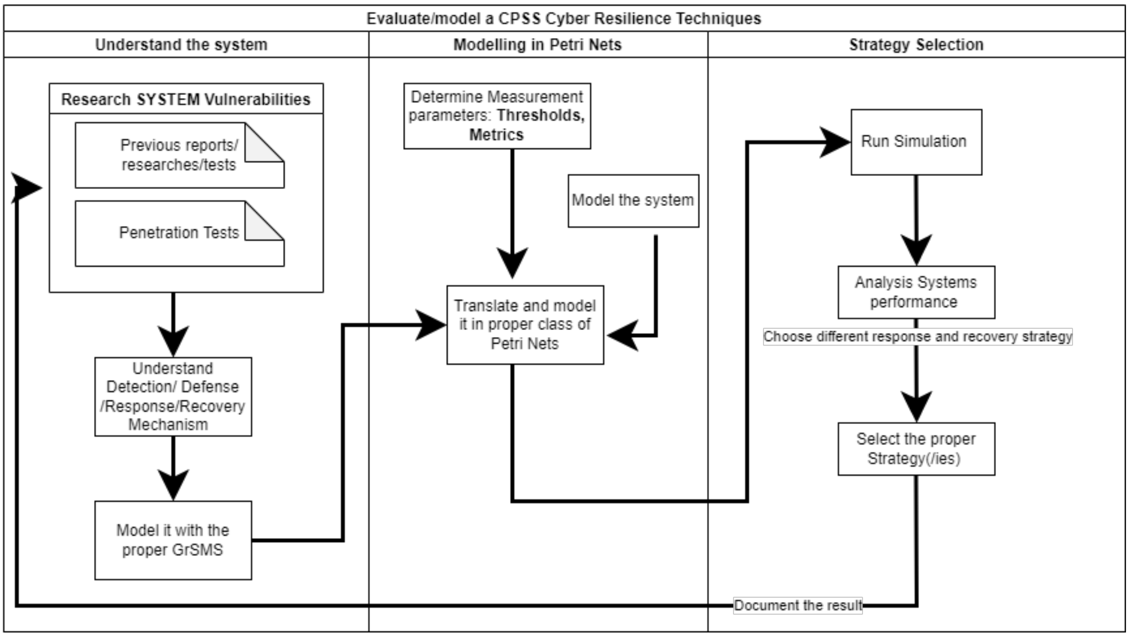

Evaluate/model a CPSS Cyber Resilience Techniques
Understand the system
Modelling in Petri Nets
Strategy Selection
Research SYSTEM Vulnerabilities
Previous reports/ researches/tests
Penetration Tests
Understand Detection/ Defense /Response/Recovery Mechanism
Model it with the proper GrSMS
Determine Measurement parameters: Thresholds, Metrics
Model the system
Translate and model it in proper class of Petri Nets
Run Simulation
Analysis Systems performance
Choose different response and recovery strategy
Select the proper Strategy(/ies)
Document the result

Figure 7.1: Resilience Evaluation Techniques and Framework

7.3 System Behavior Considering Intrusions by CPN

According to the proposed framework to design and evaluate a system´s resilience (Figure. 7.1, first I need to create the thereat model with ACT and translate it to CPN for validation and system performance regarding the defense strategies. To conduct that I did a penetration test and gathered information regarding the system-in-interest which is provided in Chapter 6, section 6.3. Following that ACT model was created and presented in Figure. 6.10.

To profile people in the CPN model, the following items are considered:

- Its identity, referred to as its id, is a name that is unique for every token
- Its position, the place where it resides
- Its value, the initial value of the token is known
- Timestamp, TS, is a non-negative number.

Any cyber attack in CPN is a tuple$\rangle ips, ipd, ps, pd, pro, com\rangle$ showing the malicious packet. In this work to ease the readability of the model for the SE scenario, I consider only the commands in describing and modeling human behaviors and their interactions.

7.3.1 CPN-based Approach for Cyber-Resilience

Using CPN modeling able us to analyze different behavioral properties of the compositions under disruptions. Modeling successful and failure scenarios for response-defense systems by CPN is key for modeling the resilience of the systems. In this regard, properties of the CPN such as liveness, and safe behaviors determine the successful scenarios. I need to verify that the resources involved in the IDS, and Web Services process will eventually be executed at least once.

7.3.2 Evaluation Detection Systems

In this section, the standard architecture of IDS is modeled by low-level Petri nets to show the high-level concept for designing the IDS and Firewalls. Regarding this goal, a scenario-based model is chosen. Based on this scenario, a sender sends a malicious request which in the first phase is not detectable by the firewall but by an IDS that I have chosen security onion, and by focusing on Snort logs will detect or not detect the cyber attack. The architecture of the firewall and snort mainly has five components after receiving a packet; these components work together to monitor and analyze all the network traffic and check for any matches sing of intrusions and then generate an alert and take action. Regarding this work's use case, these IDS are installed on the network and are not host-based.

On the network, the packet checked by the firewall looks for an intrusion in the payload and is defined as blocking or denying the suspicious request. If the packet header does not match with the rules, then NIDS in this work Snort rules in the Security Onion application will check the payload and content and analyze it with the signature-based database. NIDs generate an alert in the IDS admin logging system if the packet has questionable or intrusion content. Snort is a real-time monitoring system that monitors and analyzes network traffic.

If the packet does not have any malicious request, it will be passed in the network protocol. Places in the PNs model represent a state of the system, which shows components' behavior and the components. Events are shown by transitions and arcs, the connection and result of each event. In this PNs model, a requested packet is received by a firewall and will be checked with the defined rules in its database. The firewall takes the act of denying if one of the rules is matched with the packet header or letting the packet pass if any threat is detected. In Figure.7.2, using place/transition PNs, the firewall and IDS (NIDS) collaboration modeling by PNs is provided.

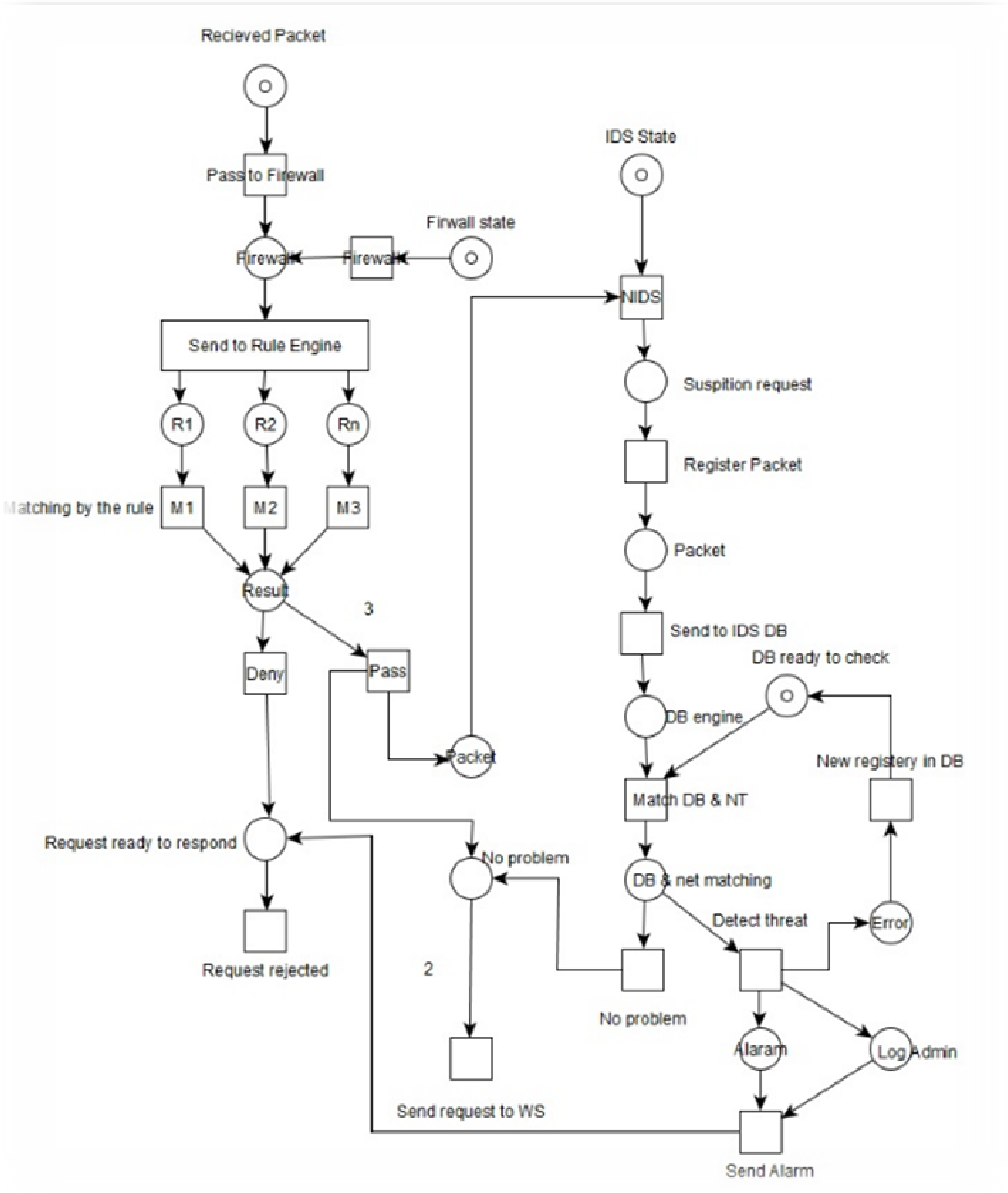


Figure 7.2: PNs demonstrating Firewall and Intrusion detection system dynamic

7.3.2.1 Firewall as Detection and Defense System

The first layer of the security mechanism in the systems is a firewall. A firewall is a technology of cybersecurity defense that regulates the packets flowing between two networks. The firewall’s main objective is to prevent attacks against the networked system by monitoring and controlling the inbound and outbound traffic on the network. It applies package filtering which is a mechanism that offers to handle and verify all the data passing through the firewall [198]. Firewalls have the same conceptual model as IDS with different analysis algorithms. Since there are many different security trust levels between networks, firewall rules are configured to filter out unnecessary traffic. The rule is written with the following criteria for acceptance or rejection:

- Type of protocol (here just HTTP/HTTPS)
- Incoming and outgoing traffic
- Specific port service
- Specific source and destination IP address

Calling these audit fields together as "header"are recorded in a firewall database and are used autonomously by the firewall engine to analyze malicious behavior or request. A resilient firewall should detect a threat with minimum rule-match-up timing and stop the anomaly packet from transmitting. The CPN model of the firewall is presented in Figure.7.3.

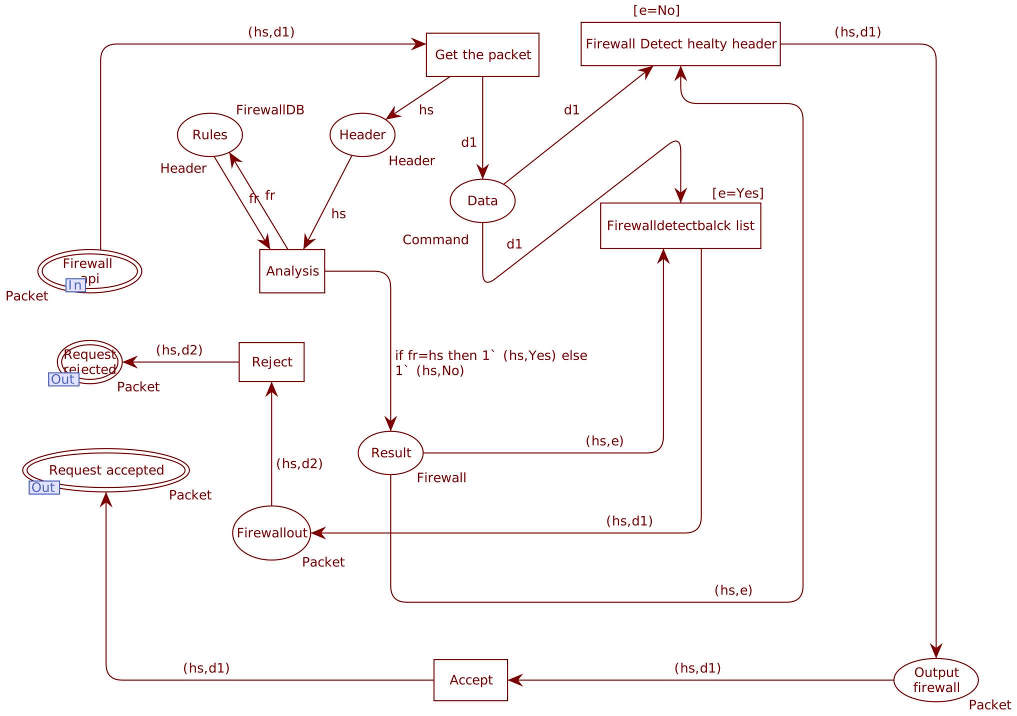


Figure 7.3: Firewall Coloured Petri Nets Model

Table 7.1: Firewall behavior

Firewall	**Behavior**
T1FW	Firewall analysis captured packet
T2FW	Analysis the header with set rules
T3FW	Generating the analysis result
T4FW	Let the packet pass
T5FW	Deny and stop the suspect's request

Table 7.2: Network Intrusion Detection System behavior

NIDS	**NIDS Behavior**
T1ids	Incoming package captured
T2ids	Analysis specious packet (rule-header: signature DB)
T3ids	Check the payload of the packet with signature (rule-body DB)
T4ids	Generate alerts and log entries as configured by the network administrator

The transitions related to five events happening while monitoring and analyzing inbound packets by a firewall are described in table 7.1.

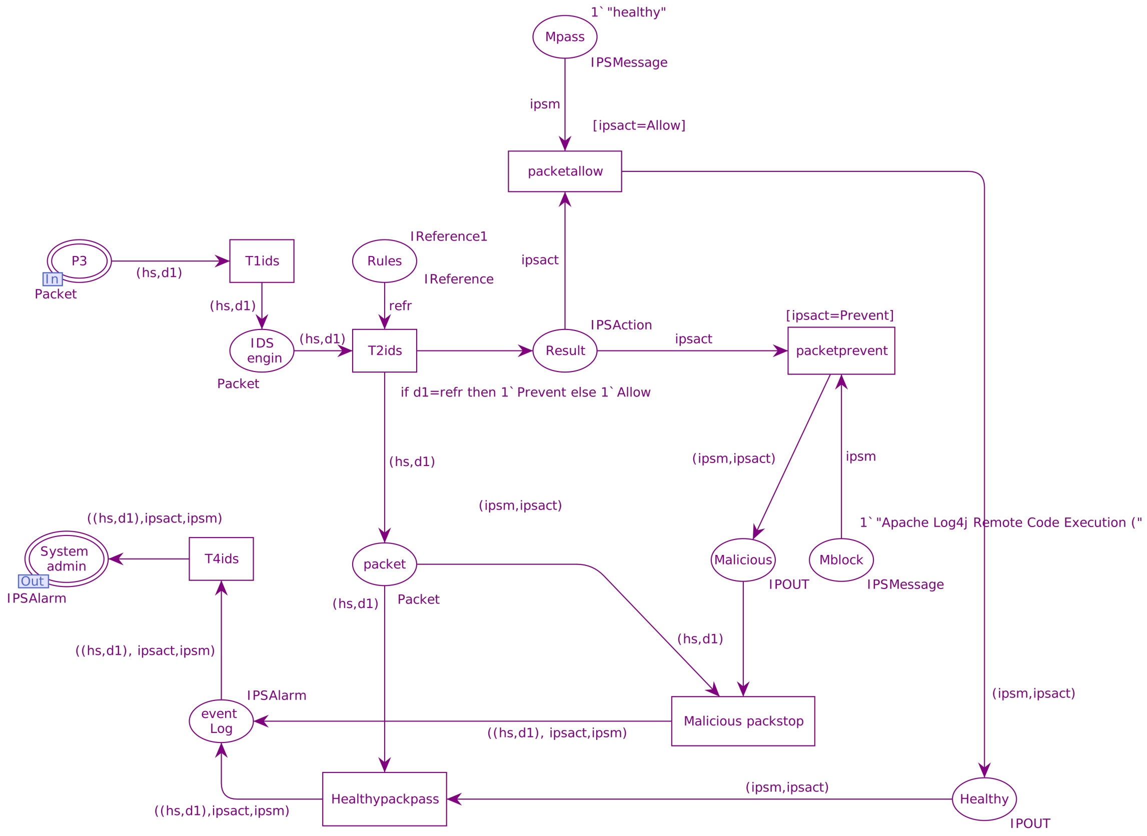


Figure 7.4: IDS behavior by CPN

7.3.3 Web Server and OPEN SSL

Web services are Internet-based software components that support Web server performance metrics including response time. OpenSSL is an open-source implementation of the Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS) protocols. It consists all-purpose cryptography library. It is applied in some web server modules to secure web sessions, such as the mod_ssl module in the Apache web server.

In the past, TLS/SSL protocol was considered one of the security protocols on the network, but according to reports in the last years, it has vulnerabilities considering Man-In-the-Middle (MITM) attacks. The remotely exploitable BoF vulnerability in OpenSSL servers, which exists in the released version before 0.9.6e and pre-release 0.9.7-beta 2 could lead to arbitrary code execution on the server.

The attack's impact is DoS, not availability, and lack of confidentiality and integrity in the services. In Figure 7.5 I present the CPN approach to model Open SSL and CA with five places and four events to show the impact of the attack and manipulating the web server.

The attacker's goal is to take over the victim's machine and execute arbitrary code on the target by hacking application control flow. By doing a penetration test on the server, the buffer size is recognized as "64", and the process of SQLI using the *Get* method is done using an automated tool.

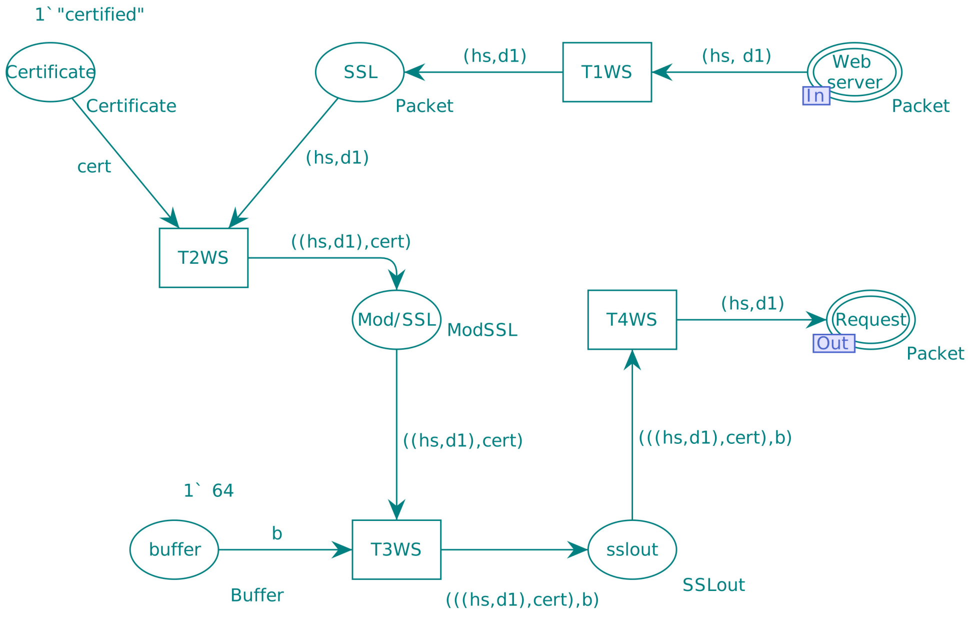


Figure 7.5: Web server composition by CPN

This model has an input node and an output node, which are the communication nodes with other sub-systems through the HTTP protocol on the network. In table.7.3 the four occurred events in the web-server are described when it is manipulated with SQLI. The places show the state of the system and each composition in the web server.

Table 7.3: Web-server behavior impacted by cyberattack

Webserver	**Web sever Behavior**
T1WS	Ask Trust CA
T2WS	Check Trusted Certificates
T3WS	Manipulated Modmod ssl confirm the malicious certificate
T4WS	Send the request to micro-service modules

7.3.4 Response System

In the IDS the input data is a malicious or neutral packet, and the output is the requested packet, and in anomaly detection, the alert message is included. These outputs in the systems equipped by Intrusion Response Systems (IRS) will be input.

Generally, IRS types are divided into three main categories based on their roles: notification, manual response systems, and automated response systems [199]. There are two types of configurations of types for offline and online architecture and controlled systems; preventive or proactive, which facilitate the system by detecting and mitigating cyber-attacks before they occur, and reactive response, respectively, which are simulating the game of attacker and defender behavior [200]. In our scenario, I chose the manual response systems and there are taken online. In this regard, eight types of response are defined so that system/security administrator (SIEM) can be applied considering the type of attack and its advancement. All of these responses presented in Table. 7.4 are dedicated to the one place node in the CPN model called *response* in Figure.7.10. The next event in the net depends on which action the SIEM is taken therefore the behavior and state of the system will differ.

Table 7.4: Response Systems

Response System Index	**Response system behavior**
R1	Block port 443 from the attacker's source IP
R2	Kill the apache privilege shell
R3	Block attacker's source IP
R4	Kill crontab process (kill process-name)
R5	Restart Apache (sudo service apache2 restart)
R6	Reboot Apache's host machine
R7	Deny access to crontab command and kill the process if it still running
R8	Set Apache's HTTP document directory to READONLY

7.3.5 Defense Mechanisms: Intrusion Detection and Response Systems

Any CPSS systems typically have specially designed firewall rules according to the system´s, organization's security mechanism as well as password policies to achieve a high level of network, and systems security. A firewall is a technology of cyber security defense and intrusion systems that regulates the packets flowing between two networks. A set of firewall rules is defined by security administrators to secure the communication transmission between two networks due to different security trust levels. These rules are configured to filter out suspicious or blacklisted packets (inbound traffics).

Service: any Source: from a network: Traffic from a particular IP address is translated at the source or destination as defined in the rule. Actions: Allow: allow access users based on the access rule. , Deny: deny access to users based on the access rule. the access rules are defined based on the following criteria [201, 202]:

- Type of protocol
- Inbound and Outbound Traffic
- Specific Port service
- Specific IP address: both IP source and IP destination

7.4 CPN Tools Model the Scenario

Modeling the system performance by the CPN defines a visual presentation of system states. It helps to understand the behavior of the system dynamically and also measures the performance of each sub-system's behaviors and impacts. It is also ideal for designers and developers to simulate their systems in advance.

CPN has the advantage that the modeling approach is independent of the data serialization format and allows the composition to explicitly process and display data types. In addition, by simulating the configuration process and examining various behavioral characteristics, CPNs can analyze the modeled configuration and examine its performance[203]. I validated how to use CPN Tools to implement the formal cyber resilience strategy based on CPNs in my experiment. The CPN Tools features such as editing, analyzing, and simulating Coloured Petri nets models are applied in this work.

Table 7.5: Cyber Physical Social System (CPSS) in the CPN model

System	Asset
Physical	Server, Firewall, Camera
Cyber	Web server, Database,IPS, Firewall,Packets(Data), Decisions
Social	Attacker, Victim, Incident Response Team

7.4.1 Recovery Plan

The objective of the CPN model in this work is to evaluate the recovery plan performance as well. In this regard, I designed two distinct recovery strategies for two types of attacks (DoS and compromised database, which means PHP or HTTP malicious code injection) as follows: for DoS, block IP, filter traffic, and pass the white list; and for compromised web-servers, design two backup web servers so that in the event of one server's failure, the other can pass the request. In Figure. 7.6 the absorb and recovery strategies for Dos are depicted by CPN.

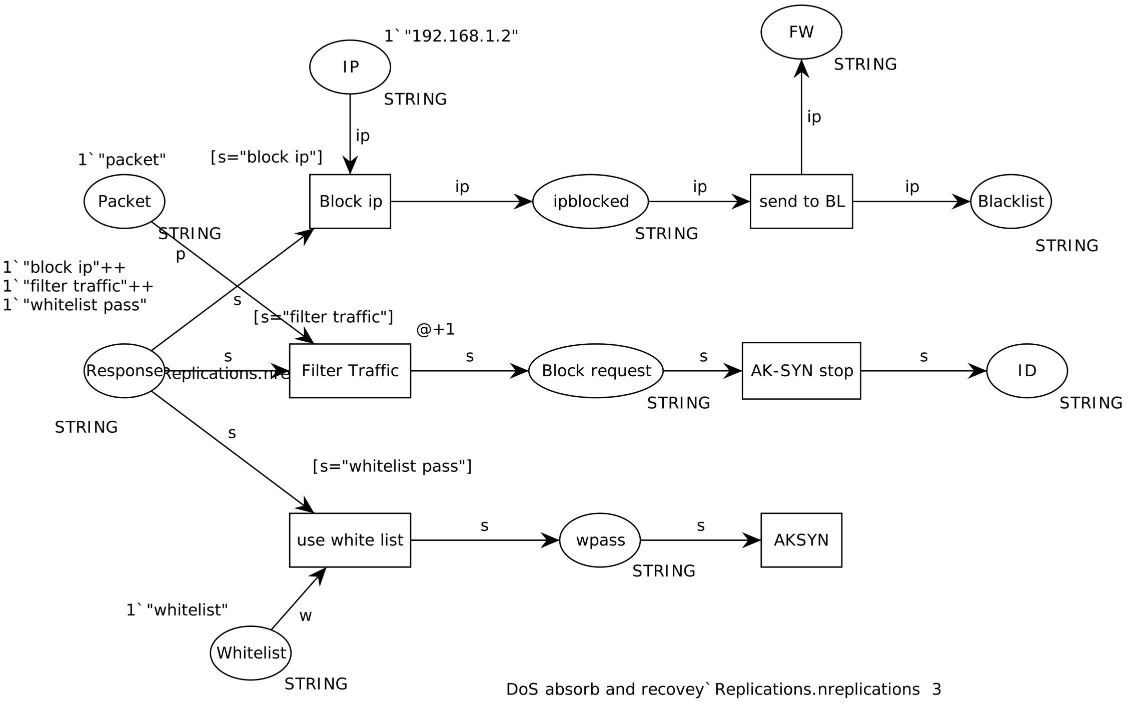


Figure 7.6: CPN modeling Recovery Plan

7.4.2 Timing in the CPN

The "time attribute" in our model is represented in two ways providing different information and presentations in the model as follows:

1. Timestamp: Used for Logs and registries. In Figure 7.4, the place "Timestamp"resembles the time attribute that related data receives from the system´s clock while the packet passes from IDS.
2. Timed Token: To control and indicate the required time to release a resource or change the system´s state. In Figure 7.13 and Figure 7.10 the decision-making process such as administer´s decision to respond to the threats/alarms shown by

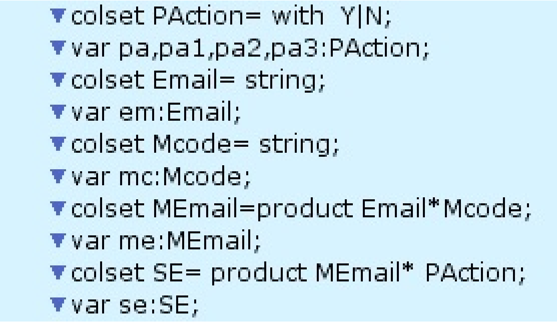
the "Response"transition. This transition has time attributes such as "time delay"for firing the transition which are determined by the "@+ "required or estimated time.

7.5 Human Behaviors in Social Systems: Profiling by CPN

As I discussed in Chapters 2 and 3, the CPSS threat is not limited to the physical and cyberspace but includes social space and can target people as the vulnerable and weak link of the chain. Considering the human mental model in the process of making decisions described in 4.6 in chapter 4, I can profile and outline the people's characteristics (mental and skill-ability) related to the attacker or defenders and apply in the dynamic of the attack-defense scenarios. Learning from the ACT, human behavior profiled in the CPN. I focus on situation awareness in understanding (plan phase) and incident response (absorb phase).

As I touched on the SA model in section 4.6, it is an important element in complex systems operations such as CPSS that comfort human factors practitioner. SA can be determined as a spectrum or binary. In this work, in the case of Social Engineering (SE), the victim´s SA caused the attack executed or not. So they are aware of it or not. By the CPN notation, the SE transitions fire if awareness=0 and stop if awareness=1. So, in the SE attack, I put human awareness in Boolean as a result of knowledge, training, personality, and experience. If awareness is true the attack stops and if be false, the attack is passed to the next level based on the attacker's activity. As in the response system, I determined human behavior as a place dedicated to a person (collective behavior of the blue team), each of the attackers and victims will be presented in place and their positional behavior as a data set. Because each behavior creates new data for the CPSS. The acted behavior will be shown by transitions which are conditional fire based on the interaction of people's behavior and the systems.

As I described in section 4.4.2, in a CPSS resources can be physical, cyber, or people. modeling human behavior in the context of SE, resources are people, network links, and threats (process incoming requests in a web server). In our CPN model, all resources are defined by places, and the attributes of the resources are taken into the account by tokens colsets (Table. 7.5) which Figure 7.7 shows the defined colset for those in CPN Tools.



```
▼colset PAction= with  Y|N;
▼var pa,pa1,pa2,pa3:PAction;
▼colset Email= string;
▼var em:Email;
▼colset Mcode= string;
▼var mc:Mcode;
▼colset MEmail=product Email*Mcode;
▼var me:MEmail;
▼colset SE= product MEmail* PAction;
▼var se:SE;
```

Figure 7.7: Colset Social Engineering

Human behavior is considered a result of cognitive decisions. I assumed that cognitive elements are resources for the behavior of a person. In this case, environmental elements such as time pressure, and people´s background knowledge viz skills and experience are shown with places with a Boolean value. It means I consider them as a crisp value (0,1) to show whether a person has an IT skill or the same experience in the past or is under time-social pressure (v=Y) or not (v=N). Each one of these places has two transitions possible to be fired. Along with the designed SE scenario by email phishing, the decision of the victim for clicking and opening the email or not relies on the accumulation of cogitative parameters. Based On Eldsy Situation Awareness, section 4.6, Awareness place is a set of Skill, Pressure, Experience. The transition *Not Click (NC)* fires if the value of *Skill = Y* AND *Pressure= N* AND *Experience=Y*. In the contrast action, transition *Click (N)* fires if the value of *Skill = N* OR *Pressure= Y* OR *Experience=N*. All the conditions for firing connected transitions should be indicated in the transition´s *guard*.

The place victim is a set of victims in Email phishing,

$$Victim = v_1, v_2, ..., v_n$$

, the Place Intruder

$$Intruder = Int_1, Int_2, ..., Int_m$$

where n, m >0, which they can communicate with each other. Each victim can make a decision independent of others or in a social context can talk with others before taking a decision. In this work, I assumed one-to-one interaction between a victim and an Intruder.

As it is shown in the ACT in Figure. 5.6, Phishing Email happens if both email contents be click-bate AND have a malicious link. Intruder place is a set of places Intruder= appealing email content, malicious link and the initial mark of both places are defined as colset Email and Mcode as string and place *victim's email* is a *product* of these two places, Figure 7.7. The Transition *Send email* is the intruder action to start the SE attack.

When the victim receives the phishing email declared by transition *Receive malicious email* the state of Awareness or Not Awareness changes the state of the SE attack. Both transitions *Block SE*, meaning that SE Stops and blocks, and transition *Intruder Access*, meaning that now the intruder has an access to the victim´s credential, can be fired if the connected places received the token. Here conflict transitions are shown by the CPN model as only one of these actions can be conducted simultaneously. Place *SE failure* shows the state of the attack which failed as a result of the customer´s awareness and the place *SE success* defines the state of the victim´s system hijacked by the attacker because of the victim´s unawareness of the possibility of being target with a malicious email. victim´s credentials as a resource of the cyber system (email) are denoted by place *User ´s Credentials* with colset *Authentication* which is Modeled as LDAP CPN Model is Figure. 7.13 as assigned to the subpage Authentication and in Figure. 7.8.

In figure 7.9, the SE CPN model considering human behavior as victim and intruder interaction is provided.

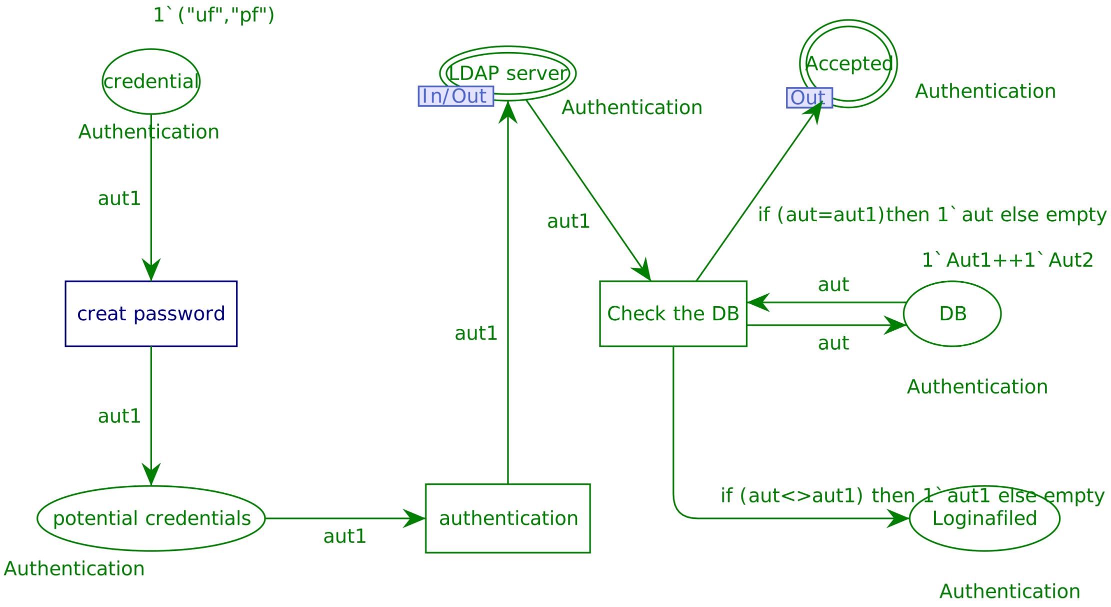


Figure 7.8: CPN modeling Authentication

The model validation criteria can enumerate as follow:

1. Scaleable: Applied for 3 different scenarios for different types of attacks,
2. For showing the resiliency the model can define a threshold to measure the resiliency and performance of the system,
3. Can apply Timestamp and delay,
4. Be able to show how the dynamic of GrSMs translates to the CPN model for all the models.

For all the model's deadlock transitions for attacker´s actions means the successful responses or intrusion detection and prevention.

7.6 Data Analysis

In chapter 5, section 5.3, I showed how by introducing the CPN model and computing transition we can examine the security of the systems and make a quantitative analysis (in this thesis, I provided attack and defense cost analysis). The result of the analysis showed the total cost of the different types of attacks and the impact of damages or troubles by them. Also, it gave information about the cost of defending against those attacks as well as their effectiveness to stop them. It explains that the states in the CPN model define the impact of the attack on the performance of the system as well as defense strategies. The argument here is how the result of security analysis shows the resilience of the system.

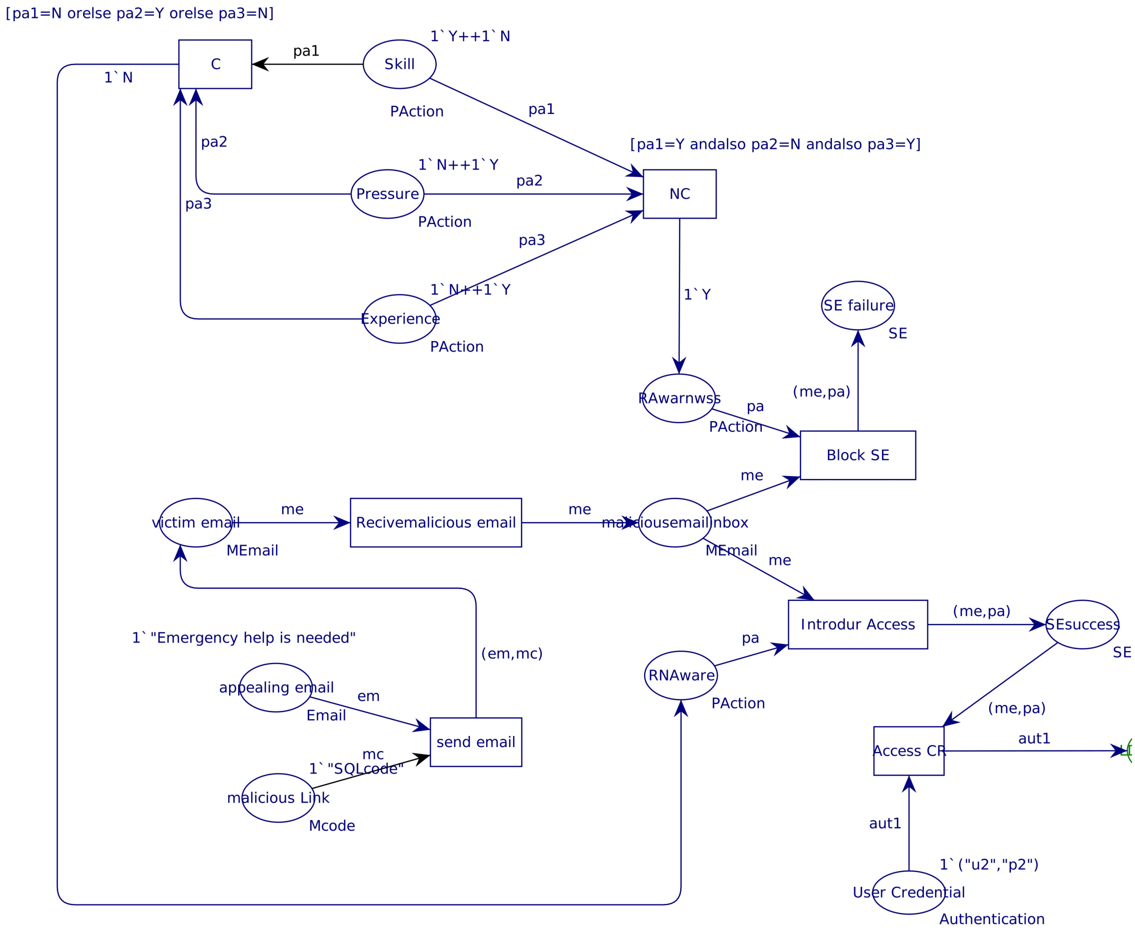


Figure 7.9: A CPN Model For Social Engineering Attack

In this section, besides the security analysis, I show resilience analysis by CPN considering response time as a measurement metric for evaluating system performance in terms of availability and the level of confidentiality and integrity. In section 7.4.2, I determined how to integrate the time property into the CPN model as a "timestamp"colset and transition delay. Using this idea, I examine the cyber resiliency of the systems taking into account the security metrics, CIA; as well as the system's response time and recovery time.

As I addressed the resiliency of the system in the chapter 2, the impact of the attack on the system has an inverse effect on the functionality (/performance), it means $F = \frac{1}{I}$. In subsection 2.3.2, where I described the resilience framework, we learned that the ability of a system to absorb and recover from disruption is an important parameter for resiliency. In this regard, I evaluate the performance of each security component (firewall, IDS, and defense system) to detect and absorb or stop cyber attacks.

To validate the model, two main data sources are used. As a first source, I imported the acquired data from the university's IT division which included the type of cyber attacks, the detection mechanisms and rules, the impact of the intruder´s action, and the impact of the defense or response system. This data is static and is used to test the model and set the detection rules for the second source of the data which was my isolated home lab. I integrated the data from my isolated lab for analysis of the impact of the attacks and defenses. The main purpose to use the lab data was to be able to test and monitor cyber attacks, SIEM behavior, and most important to be able to initiate the DoS and see the result.

Taking to account Figure. 7.4, I consider four categories for measuring the performance of the system as it is shown in Table. 7.6.

Table 7.6: IDS/IPS Performance

Performance	Range (%)
High	85-100
Medium	40-85
Low	10-40
Poor	0-10

It is noticeable that each type of attack has a different impact on the system and it is obvious that I need to analyze the behavior of the systems in different sub-nets.

CPN Model and Execution simulation by CPN Tool for scenario 1 (Injected Malicious Code).

In attack type 1, the number of times the sensitive information enclosures are shown as a state of the system with ”lack of Integrity” place; is marked by a token (and packet type). This place is designed to better readability of the model and the absence of that does not affect the system behavior.

I assumed that all the packets that are detected as TT, end in the normal packet (as I model the attack scenarios, TT is just for considering these possibilities and not for showing the communication part of the system). The successful attack in the scenario of a malicious code injection attack that compromises confidentiality and integrity ends up in the node "Lack Integrity". As described in the previous section, in the Log4j/malicious code injection attack, one of the recovery solutions is designing and applying web server backup. The recovery speed is critical to help the organization to avoid the temptation to pay the ransom. Continuous or frequent backups, as mentioned above, ensure almost no packet loss or drop. Most backup software today has a feature that enables the VMs and applications to mount on the backup storage device, saving the transfer time over the network to production storage.

In scenario 1, web server 1 and web server 2 are backups of the original web server. I assumed that when the web server was originally compromised, first web server 2 and if needed web server 3 as backups help the system not to lose the storage data and can decrease the data exposure. Those are designed as prevention and also recovery plan.

I evaluated their functionality and efficiency based on the number of lost/pass packets and the server's response time. The IDS goal is to reach the desired performance which means 100 % accuracy (in sense of 100% true detection of false packets). The higher accuracy causes a higher performance of the whole system and makes it secure against cyber attacks.

The performance of the defense system is measured by the total amount of numbers when the response system succeeds and the system can keep integrity/confidentiality. Based on Table 7.6, if the rate of stopping attacks by the defender is higher than 85% the quality of service in terms of CIA is high.

To show human behavior (as attackers) and the scalability of the model, I determined four senders (which means 4 initial places). Each of these senders uses different techniques to lunch the Log4j attack, but as it is shown in Figure. 7.10 the impact of all of them is the same on the behavior of the system. For instance, in this figure "sender 4"behavior shows applying the penetration test technique and "sender1” directly "POST"the malicious code.

In total 100 times simulation, it took almost 0.00 for the CPN Tools to simulate all the possibilities. I repeated the simulation three times and each time updated the firewall and IDS' rules and response strategies. As a result, for the first run, Out of 500 packets sent over the network ($total\ packet = initialpackets \times runningtimes$), 60.00% of the times the malicious codes were executed and the integrity of the system was compromised. That was because of the low performance of IDS and weak strategies taken by the defender that in this case, no actions from the defender side to stop the attack. In this case, while the average response time for the HTTP requests was 5 units (based on the TCP model (calculating delays)- which means the performance of the system was high- the total performance of the system was low as losing the integrity.

Figure 7.11 shows the number of steps in 100 times running scenario 1. The figure shows that the system was not crashed during its performance. That is a result of using the prevention and recovery solutions as explained at the beginning of the malicious code scenario in this chapter (using three web servers and load balancing strategies). But system integrity was compromised 60.00% of the time. The result of three of the firewall and IDS performance v.s impact of the cyber attack after three different simulations of this scenario is shown in Figure 7.12

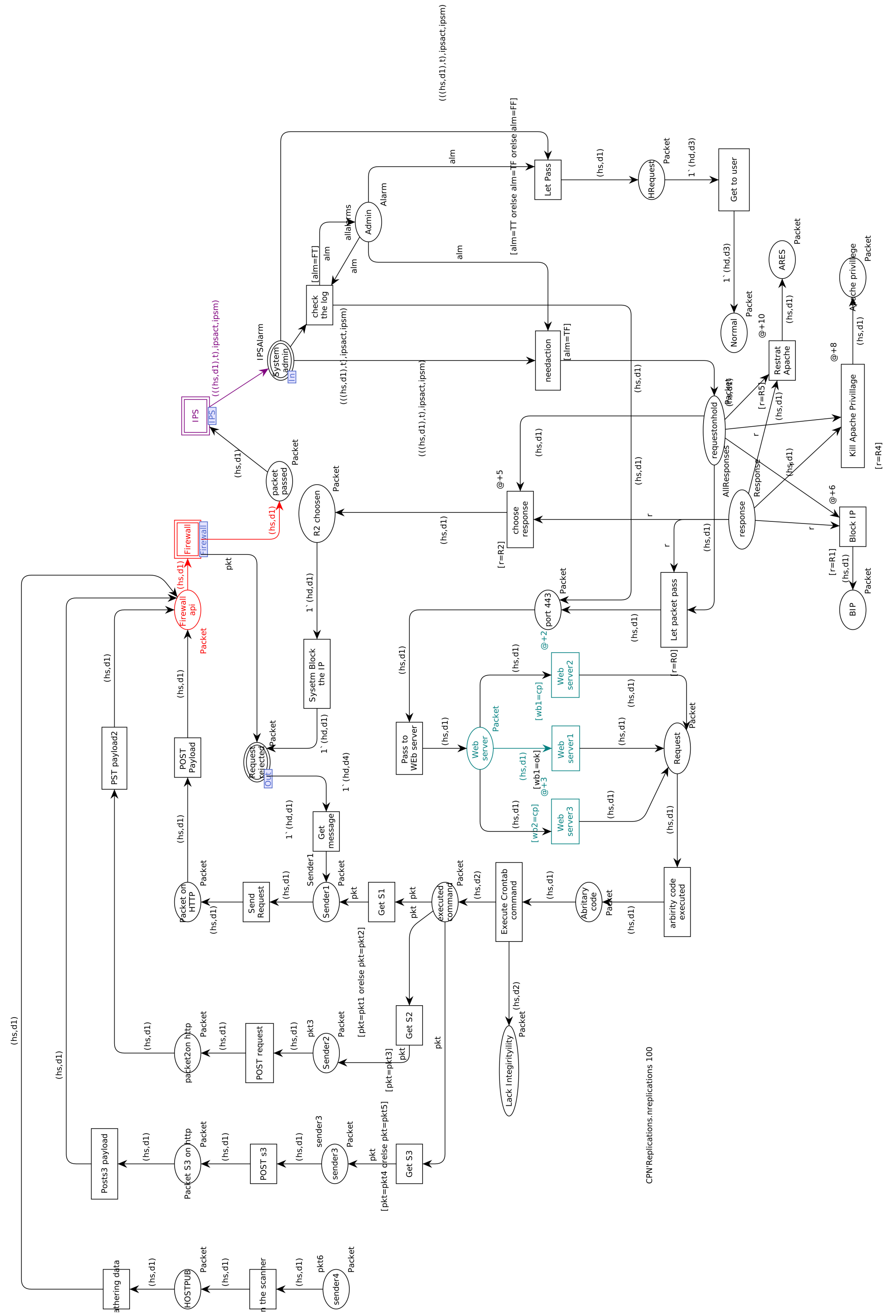


Figure 7.10: The CPN Model of Malicious Code Injection Attack, Response

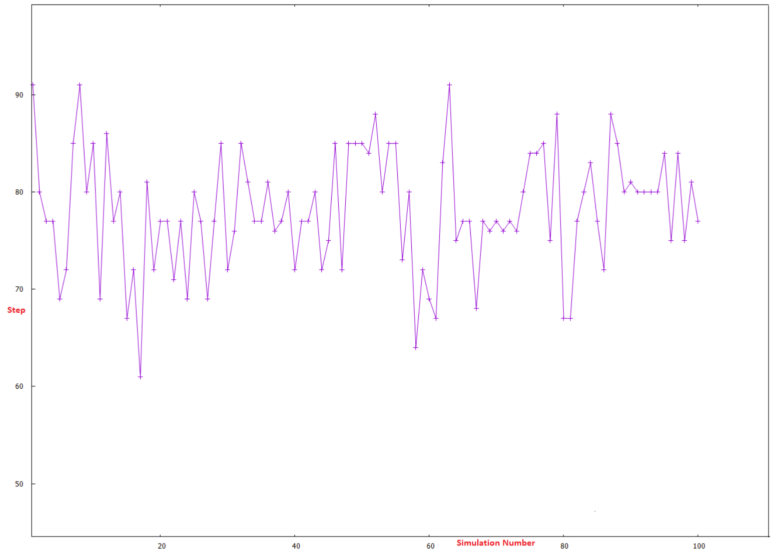


Figure 7.11: The Number of Steps in the Simulation

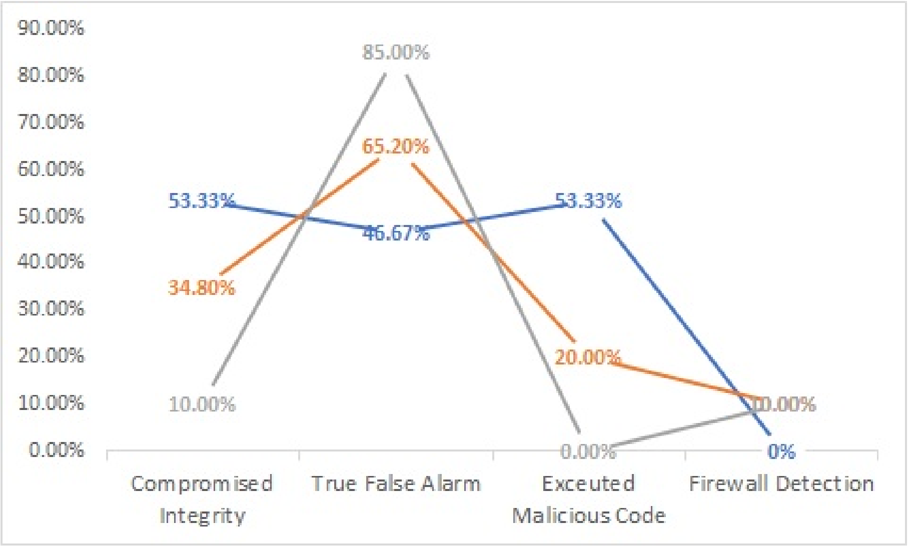


Figure 7.12: The Intrusion Detection Systems Performance vs. Malicious Code Injection Attack

In the second and third simulation runs, by changing all the detection system's rules and response strategies, the result of the performance regarding the time of response and CIA were different. In Table 7.7 the summary of the execution analysis is provided. In this specific scenario, two defense strategies of blocking suspicious IPs and killing the Apache privilege had better results than other strategies to stop the attack.

CPN Model and Execution simulation by CPN Tool for scenario 2 (DoS).

The type of attack in this scenario is the DoS. The assumption for the number of attackers is three who use different techniques for DoS, and besides the type of attack, I considered the recovery plan and actions which were introduced and modeled in 7.6.

Table 7.7: Scenario 1, Cr, M, N: Critical, Medium, Not effect Attack; H, M, L, N: High, Medium, Low, Poor Detection and Response System and Performance; C, I, A: Confidentiality, Integrity, and Availability reserved

Run no.	Response Strategy	Cr	M	N	H	M	L	N	C	I	A
Run 1	Detection and Mitigation Failure	Y						Y	N	N	Y
Run 2	Block the Suspicious IP	Y	Y			Y			Y	Y	Y
Run 3	Kill the Apache Privilege	Y	Y		Y				Y	Y	N

As it is shown in the table 7.8 when DoS happens and the system lost availability, the system back to normal functionality after RESTART the system which means the system crashed after DoS. To make the system resilient a new strategy was developed and the effects of that were evaluated by the CPN model again 7.6 this absorb strategy had a positive impact on the resiliency of the system.

Table 7.8: Scenario 2

Run no.	**Action**	Cr	M	N	H	M	L	N	C	I	A
Run 1	System Exhausted (SYN-FLOOD)	Y						Y	N	N	N
Run 2	Shutdown System	Y			Y			Y	N	Y	N
Run 3	Just Pass white list	Y			Y				Y	Y	Y
100 t	Absorb Attack	Y							Y	Y	Y

The strategy of ”just letting white list pass” had the problem of losing availability because of the lack of a completed white list in the database which also affected the response time and makes it slower. Table 7.9 shows a sample of how the result of performance analysis for the different defense and recovery plans is measured based on the TCPN model.

In this scenario, I defined "thresholds"by introducing a control loop (conditional transition) as a defense strategy. The thresholds determine the maximum traffic (here several packets) that allow passing the network. In this scenario, I defined a transition related to security administer action to decrease the impact of DoS or SYN-Flood.

CPN Model and Execution simulation by CPN Tools for scenario 3 (Email Phishing).

In Figure 7.13, and Figure 7.9, the impact of SE to access credentials on the system and the phishing techniques are provided respectively by CPN. The result of "Awareness"and "not being Aware"of phishing techniques leads to stop or proceed the attack. Awareness attributes are shown by places (Skill, Pressure, and Experience). The result of the simulation is shown in table 7.10.

Table 7.9: A sample of Data Analysis from the Time Coloured Petri Nets

Phase	**States**	**Fired Transitions**	**Impact**	**Response time**	**QoS (CIA)**
Detection	IDS Success	233	Detect and Prevent	28	High
Detection	Malicious packet not stopped	241	System Compromised	50.7	Low
Response	Malicious IP Blocked	5	System Defended	10.3	High
Response	Kill the Apache privilege shell	2	System Defended	10.3	High
Response	Restart Apache	2	System Defended	10.3	High
Response	Block Port 433	12	System Defended	10.3	High
Response	Kill crontab process	5	System Defended	10.3	High
Recovery of DoS	Restart and back to service	0	System restarted	1440	No Service
Recovery	White list pass	all	system recovered and defended	48.8	High
Recovery	Block black list IPs	all	System recovered and defended	30	High
Recovery	Filter traffics	all	System recovered and defended	35.8	High

Table 7.10: Scenario 3

Run no.	**Skill**	**Experience**	**Pressure**	**Confidentiality**
Run 1	Y	N	N	Y
Run 2	N	Y	Y	N
Run 3	N	N	N	N

The result of this analysis shows that for increasing awareness reducing the pressure (time, environment, and personal) has an important rule. In Figure 7.14 and Figure 7.15, the performance of the systems in the case of DoS is shown.

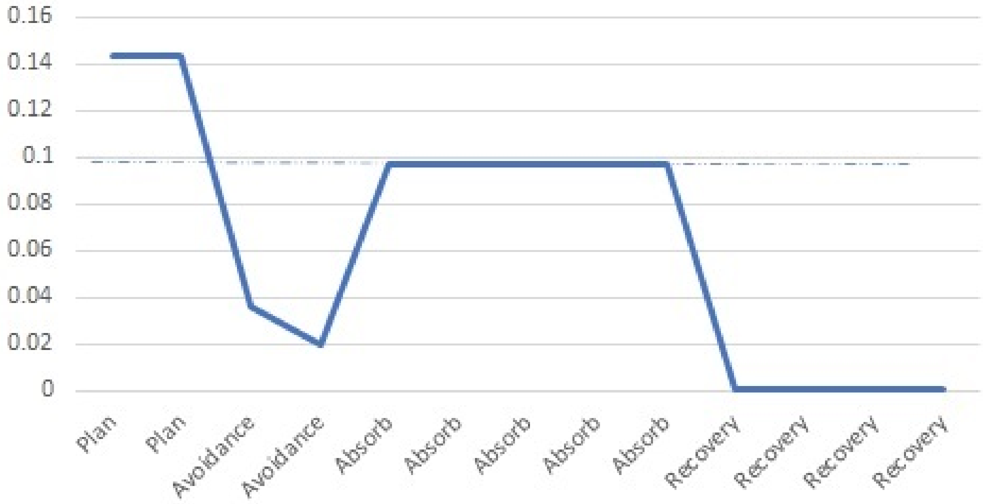


Figure 7.14: The cyber resilience performance under DoS

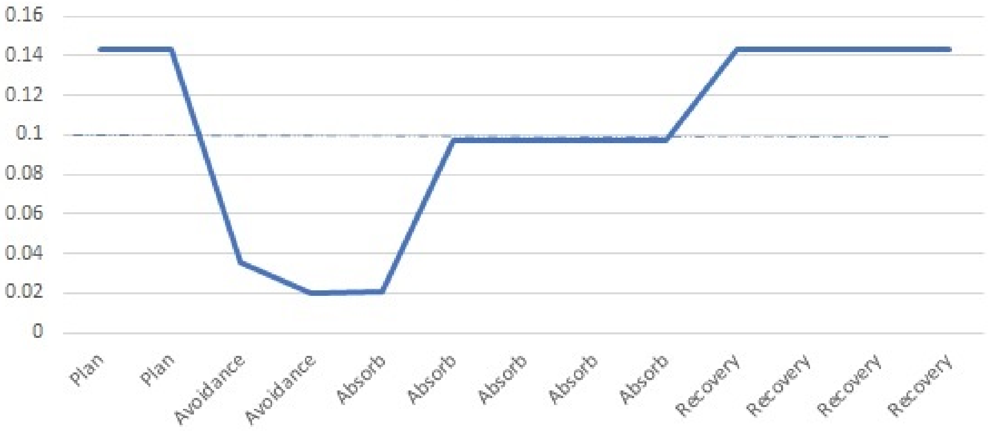


Figure 7.15: The cyber resilience performance In the DoS Profile, just white list let to pass

7.7 Hypothesis Verification

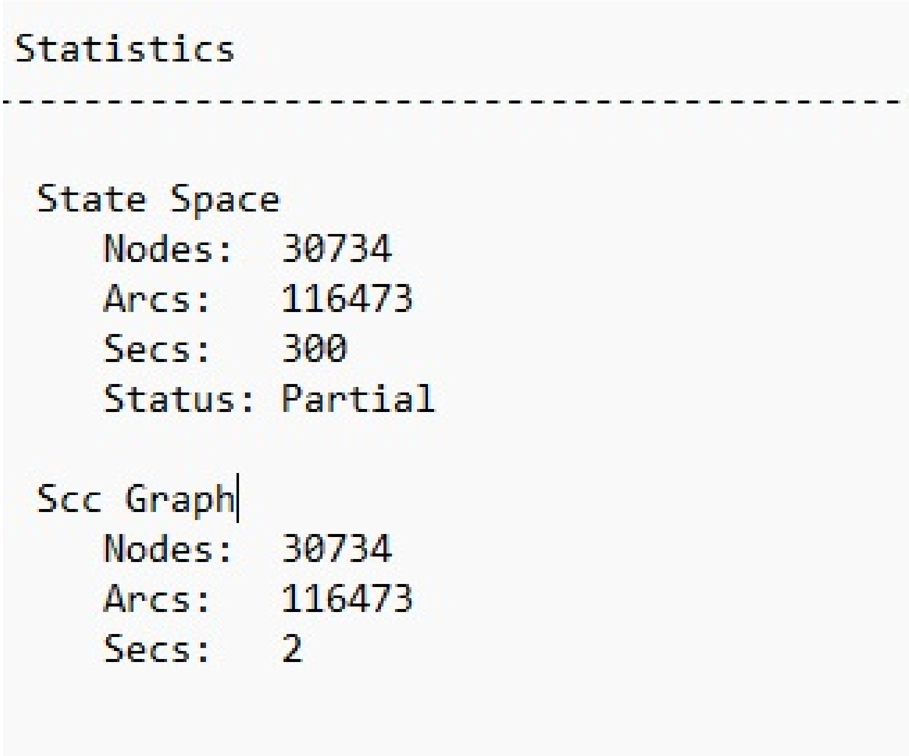
I showed how the proposed framework could ease the designing and evaluation of cyber resiliency in the systems and introduced CPSS as a system of interest that has more vulnerability because of the stochastic behavior of humans. I proved that CPN as a promising formalism could support GrSMs and be used as a uniform model to evaluate each phase of resiliency and assist decision-makers in providing proper recovery, response, and defense systems regarding different threats.

According to verifying the proposed CPN models, I provided the Reachability Graph (RG) of scenario 1 as follows.

Reachability Graph

In Figure 7.16 and Figure 7.17 the RG for the attack scenario of malicious code injection is provided. As shown in Figure 7.16, the CPN tool uses a special kind of graph derived from state spaces, called a Strongly Connected Component Graph (SCC-Graph). Also, the CPN tools have provided State Space Analysis (SS) as shown in Figure 7.17.

As I expected from the CPN analysis when the malicious code is injected, the first strategy for absorbing the attack-setting up Firewall- fails; the node "firewall detect black list"is deadlock which means it is not fired to stop the attack. On the other side, the defense strategy caused the "execute crontab command" to be deadlocked, which means that this attempt by the intruder failed and the related transition has not fired.

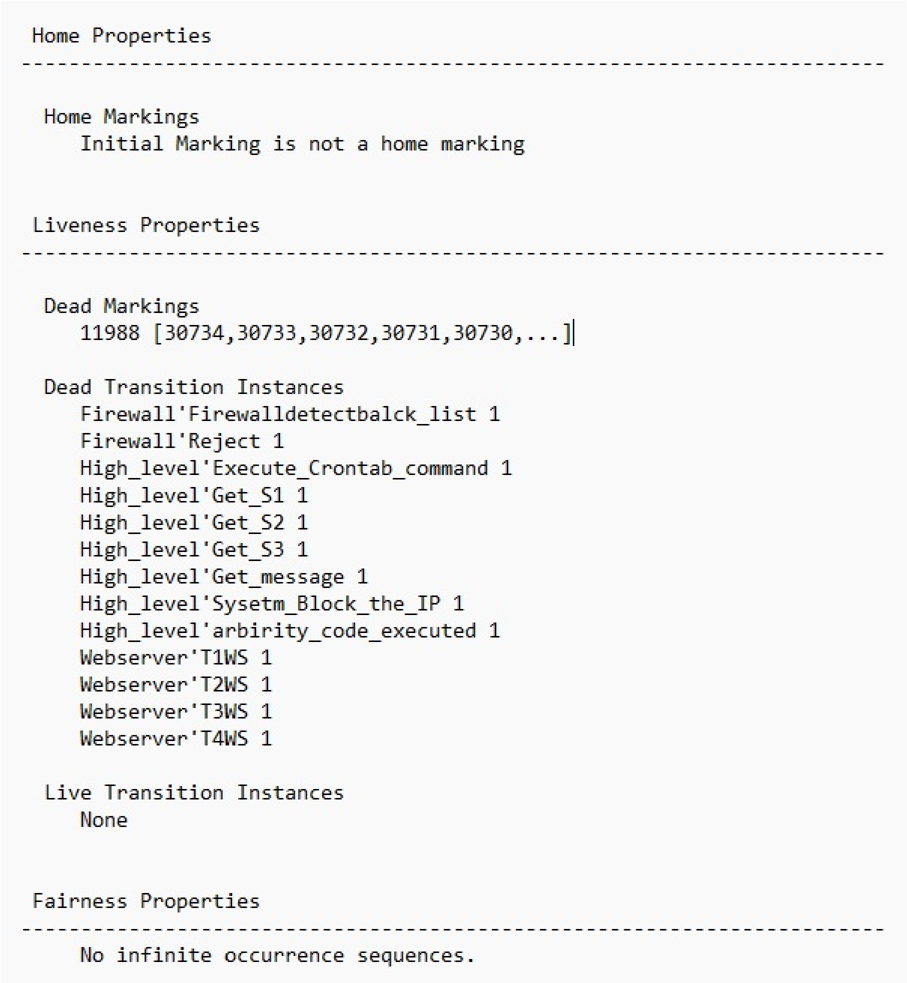


```
Statistics
----------------------------------------

 State Space
    Nodes:  30734
    Arcs:   116473
    Secs:   300
    Status: Partial

 Scc Graph
    Nodes:  30734
    Arcs:   116473
    Secs:   2
```

Figure 7.16:



```
 Home Properties
------------------------------------------------------------------------

  Home Markings
     Initial Marking is not a home marking


 Liveness Properties
------------------------------------------------------------------------

  Dead Markings
     11988 [30734,30733,30732,30731,30730,...]

  Dead Transition Instances
     Firewall'Firewalldetectbalck_list 1
     Firewall'Reject 1
     High_level'Execute_Crontab_command 1
     High_level'Get_S1 1
     High_level'Get_S2 1
     High_level'Get_S3 1
     High_level'Get_message 1
     High_level'Sysetm_Block_the_IP 1
     High_level'arbirity_code_executed 1
     Webserver'T1WS 1
     Webserver'T2WS 1
     Webserver'T3WS 1
     Webserver'T4WS 1

  Live Transition Instances
     None


 Fairness Properties
------------------------------------------------------------------------
     No infinite occurrence sequences.
```

Figure 7.17: Reachability Graph for Malicious Code Injection

7.8 Conclusion

In this chapter, I present the principal findings and results of the research evaluation. The main outcome of the chapter was evaluating the Resilience Evaluation frameworks and techniques. I applied the attack countermeasure tree and translated it to the Timed Coloured Petri Nets to evaluate the impact of each action/event on the system's resiliency. I evaluated the usability, adaptability, and scalability of Timed Coloured Petri nets to design, model, and analyze cyber security and cyber resilience in complex systems such as cyber physical social systems. I chose cyber physical social systems as complex systems, with homogeneous communication and control systems that consider stochastic and unpredictable human behavior modeling the system behavior is a very complex task.

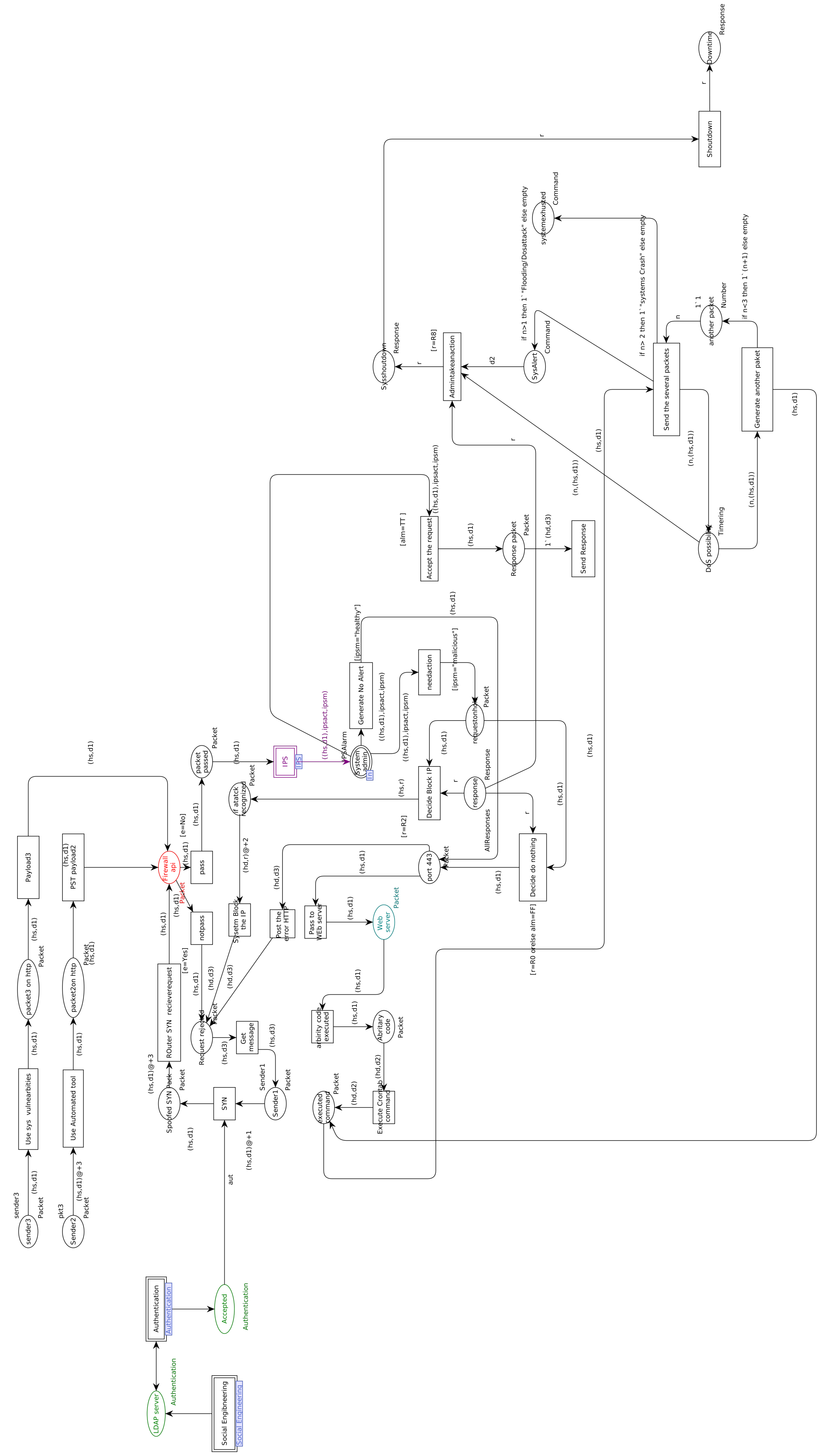


Figure 7.13: Denial of Service attack and Response System

8 Conclusion

The sweetest pleasure arises from difficulties overcome.

— *Publilius Syrus*

This chapter discusses the Ph.D. research work and the analysis of the finding. The results are analyzed from two perspectives: from problems to results and from research gaps/aimed contributions to results.

8.1 Rational on Research Result

The research problem that has been addressed was ambitious, considering the varied domains of science connected with it. The research work in different domains of science and engineering, viz biology, the environment, economics, civil engineering, and the theory of computation in intelligent and perceptional systems. To make bridges between concepts from such a confluence of research areas, section 1.4 provides a quick discussion, including the identified gaps and therefore the aimed contributions which will be made in each area. In Chapter 3, such diverse research areas are studied fully to produce a solid understanding of related areas and a discussion on past and ongoing research works. Existing scientific knowledge on cyber-resilience forms the basis of this research work.

On one hand, the problem of evaluating cyber resilience that is supported by cyber-security analysis methods is modeled using Timed Coloured Petri nets. The rules that govern the cyber physical social systems are satisfied by the system modeling under consideration. In addition, the CPN model could be translated to and verified by Graphical Security Analysis models of the different attack-defense scenarios to model the dynamic and impact of the attacker and defender behavior on the system.

On the other hand, assessing the resilience of a CPSS under cyber attack has been quantified using the MITRE and NIST cyber-resilience framework. This framework enables us to evaluate the resilience of individual designs, and then compare them. The side-by-side comparison enables us to select the design with better resilience attributes. However, what parameters influence the resilience attributes of a CPSS has not been fully investigated yet.

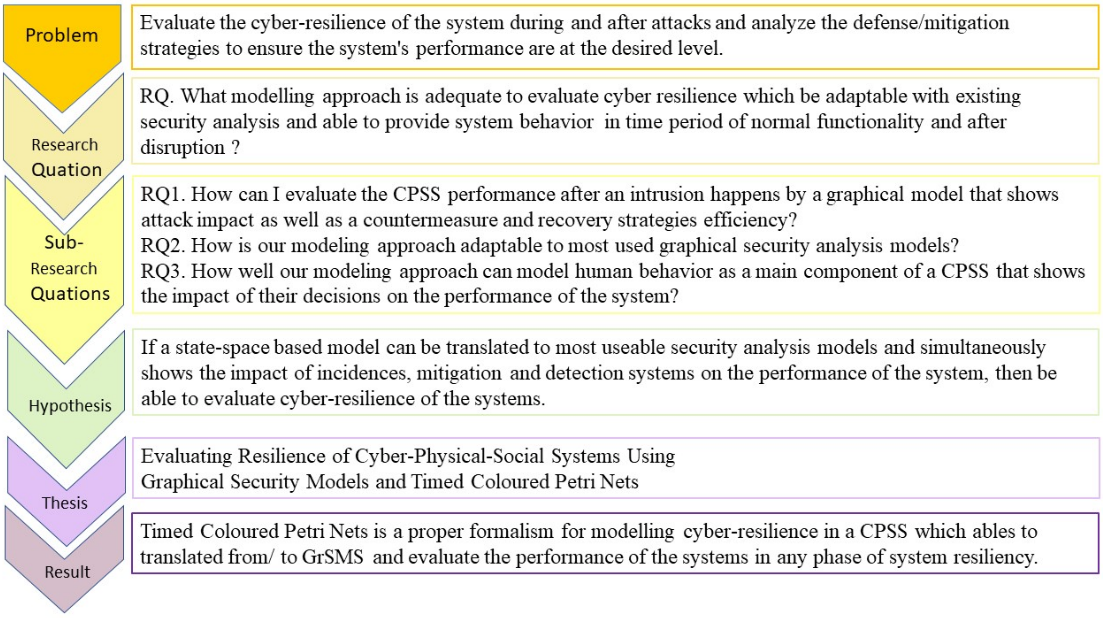
8.1.1 Research Summary: A Reminiscence

The research undertaken during this Ph.D. work has undergone a variety of cycles between theoretical and technical research. But it all started with the identification of problems associated with systems that are almost like living organisms – from the attitude that both need to handle the dynamic nature of the working environment. One of the critical concerns in complex systems is modeling human behavior as its stochastic behavior and performance insurance of the system in an uncertain environment. The CPSS was an adequate candidate to examine our hypothesis for modeling and evaluating the resilience of these types of complex systems considering human behavior. Besides, with the rapid usage and growth of Internet-connected CPSS devices and applications, a higher risk of cyber attacks occurs. In the course of cyber-resilience with cyber security scope, the main research question is divided into three sub-questions. Each question tries to find a solution to the detected problem, respond to it, and impact the solution (c.f. section 2.1).

These sub-questions are important ones to be answered for further enhancement of the state of the art of CPSS. In the domain of designing CPSS, the major problem is to meet the cyber-resilient requirement, which reflects a system's ability to manage uncertainty, dynamics, time, and concurrency in heterogeneous (interconnected) systems where the amount and complexity of intelligence (the cyber and social systems) are growing rapidly. In designing a CPSS, modeling resilience with a cyber-security approach takes care of the major portion of system design, validation, and ultimately verification. The research questions have captured this theme, paving a clear path for implementation (SQ1 and SQ2) and validation/assessment (SQ3). Figure. 8.1 shows the general flow of this Ph.D. work that started with a problem and ended with exploitable solutions. The next step was the formulation of hypotheses, the main highlight of which is the development of a learning mechanism over the
textcolorredbehavioral model of the system. If the behavioral model of the CPS can be formally modeled and represented along with the control mechanism based on events and actions, then systems adaptive loops can be used for learning to derive evolutionary paths

8.1.2 Research Challenges and Constrains

Despite the fact that Internet users and device connections are increasing, current IoT, IoP, and CPSS are still unable to integrate the human element into the entire system. There are both technical limitations and ethical issues such as security and privacy. As a consequence, we believe that these parameters build the reliability of a system, which is one of the major factors that unease the CPSS deployments in the real world. Critical infrastructures and industrial processes, medical data, or sensitive personal information need to be protected from unauthorized exploitation. Protecting confidential information is often not only a business requirement but, in many cases, also an ethical and legal



Evaluate the cyber-resilience of the system during and after attacks and analyze the defense/mitigation strategies to ensure the system's performance are at the desired level.

RQ. What modelling approach is adequate to evaluate cyber resilience which be adaptable with existing security analysis and able to provide system behavior in time period of normal functionality and after disruption ?

RQ1. How can I evaluate the CPSS performance after an intrusion happens by a graphical model that shows attack impact as well as a countermeasure and recovery strategies efficiency?
RQ2. How is our modeling approach adaptable to most used graphical security analysis models?
RQ3. How well our modeling approach can model human behavior as a main component of a CPSS that shows the impact of their decisions on the performance of the system?

If a state-space based model can be translated to most useable security analysis models and simultaneously shows the impact of incidences, mitigation and detection systems on the performance of the system, then be able to evaluate cyber-resilience of the systems.

Evaluating Resilience of Cyber-Physical-Social Systems Using
Graphical Security Models and Timed Coloured Petri Nets

Timed Coloured Petri Nets is a proper formalism for modelling cyber-resilience in a CPSS which ables to translated from/ to GrSMS and evaluate the performance of the systems in any phase of system resiliency.

Figure 8.1: The Thesis Flow

requirement. Reliable and consistent inference of a human's state is essential to the adaption of CPSS in real industrial, medical, or social scenarios. Incompetence to do so can have an extreme impact on the performance of the entire system. Secured and trustworthy Networking is also crucial for CPSS since these systems are often distributed and There is a need to exchange information among many people and devices.

In this research, our scope for evaluating cyber-resilience is tailored to cyber-security. The initial research challenge was to find interesting and useful lessons on how to design, model, and develop computing systems that will be deployed in a highly dynamic and uncertain environment. For that purpose, one obvious aspect to be studied is the methodology to capture real-time data and extract useful information such as events and situations, so that the system can take actions based on such observations. The reactions to such observed situations can lead to the accumulation of knowledge or experience of the nature of the system's environment and eventually lead to the evolution of functional behaviors. In this regard and with companies' concerns, gathering data from actual scenarios was the main challenge and led us to build an isolated and secure environment to simulate the scenarios and test the hypothesis. We limited the human decision-making factor to situation awareness about the specific technique (phishing by email) in SE. Regarding the response team, we chose limited (executable) incident responses to mitigate the attacks. We believe that narrowing down the elements helped us to understand the behavior of the systems and evaluate the impact of each action on the system's performance. By applying three different scenarios, we tested the scalability.

8.2 Integration with Fellow Research

As mentioned in this work motivation (section 1.1, the initial idea of this thesis was shaped based on a European project called DEFENDER. The DEFENDER aimed to adapt, integrate, upscale, deploy, and validate several different technologies and operational blueprints to develop a new approach to safeguard existing and future European CEI operations over cyber-physical-social threats, based on

a) novel protective concepts for lifecycle assessment, resilience, and self-healing offering "security by design" and

b) advanced intruder inspection and incident mitigation systems.

Moreover, DEFENDER created a culture of security, where trusted information exchange between trained employees and volunteers will complement cyber-physical protection while preserving the privacy of the citizens involved.

Two analysis models—GSPNs and attack trees—were used in this context to analyze cyber attacks and defenses. The task involved creating attack trees based on the risks and vulnerabilities of the system and analyzing them with GSPN. To do that, we introduced a set of rules for translating from AT to GSPN and applied them to the project scenarios.

8.3 Publications

Publication of research results is an important activity throughout the Ph.D. research. Results from the research work have been published in conference papers or journals addressing several areas that have been in the scope of the work. All the publications that were published throughout the time of this study are sorted by year of publication as follows:

Attack Tree Refinements Analysis and Verification by applying Coloured Petri Nets Conference: IECON 2022 Status: Accepted

This paper is my contribution to introducing a set of rules to translate GrSMs (tree-based) to CPN. In this work, the same example in Chapter 5 from ACT is translated to CPN considering the cost of attack and defenses. In this paper, for the first time, I provide a solution for uniforming all the notations regarding logical gates in GrSMs to a simple, AND, OR, and NAND in CPN. This model helps to analyze security in terms of the dynamic and efficiency of scenarios as well as quantitative analysis.

CYBER-PHYSICAL-SOCIAL SYSTEMS: TAXONOMY, CHALLENGES, AND OPPORTUNITIES

Journal: IEEE Access

Year:2022

This Paper is the outcome of state of an art literature review of existing knowledge and research in cyber-physical social systems. In this study, I provide a systematic review of the definition of CPSS and a uniform definition of CPSS. I propose a novel taxonomy to define CPSS to help future research and system design. The CPSS taxonomy aims to provide a comprehensive understating of CPSS characteristics and aspects from a system-to-system point of view. Furthermore, I discuss about social integration in CPSS and their relationships with CPS. I mention issues and opportunities in CPSS in the designing and implementing phases.

COVID-19 AND MITIGATION STRATEGIES: THE IMPACTOUR PILOTS COMMUNITY PERSPECTIVE

Proceeding: Tourism in South East Europe

Year:2021

This work as one of the applications of CPSS, works on the strategies such as technology application as one of the solutions for making social systems more resilient.

IMPROVING ATTACK TREES ANALYSIS USING PETRI NETS MODELING OF CYBER-ATTACKS

Proceeding: IEEE 28th International Symposium on Industrial Electronics (ISIE)

Year:2019

In this study, authors represented a new method for modeling one type of Cyber-attacks in I4.0 by using Attack trees assigned by Intrusion Detection Systems and then analysis behavior of the system (in this case 3D printer) by Generalized Stochastic Petri nets. This paper shows the application of GSPN as a promising tool for analysis and assessment security of Cyber Physical Systems.

MODELING CYBER PHYSICAL SOCIAL SYSTEMS USING DYNAMICS TIME PETRI NETS

Proceeding: Doctoral Conference on Computing, Electrical, and Industrial Systems

Year:2018

This work presents a Petri nets-based strategy supporting behavioral modeling as well as performance analysis of Cyber-Physical-Social Systems (CPSS) covering uncertainty situations when the social factor is also playing an effective role in the performance of these systems. The integration and interaction of system components including computation, physics, and social factors as a challenging part of these systems are considered. Petri nets models, augmented with dynamic time dependencies associated with transitions, are applied in a case study and validated as a promising tool for modeling and analysis of these kinds of systems.

8.4 Contributions

The rapid increase in the number of complex cyber attacks caused serious concerns about the damage they can cause to the government and private agencies. Meanwhile, the current technologies fall short to provide a comprehensive and reliable shield against cyber attacks. Therefore, a systematic design that helps systems endure cyber attacks and defenses looks extremely valuable and promising. This concept is commonly referred to as the resilience of a system to a certain cyber attack under particular conditions.

On one hand, the problem of evaluating cyber resilience that is supported by the attack countermeasure tree is modeled using Timed Coloured Petri Nets. The rules that govern the intrusion detection systems are satisfied by the systems designs under consideration.

On the other hand, assessing the resilience of an information processing enterprise has been quantified using the first (and the only) resilience framework available. This framework enables us to evaluate the resilience of individual designs, and then compare them. The side-by-side comparison enables us to select the design with better resilience attributes. However, what parameters influence the resilience attributes of an enterprise has not been investigated yet.

The principal contribution of this thesis is an approach for evaluating the cyber resilience of cyber physical social systems considering uncertainties in the system including human decisions and behaviors facing cyber-attacks. This main contribution incorporates several parts:

First, I provided a definition and taxonomy for cyber physical social systems for better understanding this new paradigm and distinguish it from similar concepts such as HiTLP CPS, IoP, and SIoT. It additionally describes social entity integration in the traditional CPS concept clearly.

Second, our analytical approach allowed us to translate several GrSMS to/from TCPN that facilitate these models to be compatible with state-space based models. I provided a set of translation rules that enables modelers to switch between these two approaches based on their needs.

Third, I applied the hierarchical concept in Coloured Petri Nets to solve the scalability problem in state-based graphical formalism. For that, I modeled and presented each component of the system in sub-models including intrusion detection systems, and defense/mitigation systems.

Fourth, I showed that the proposed CPN formalism for cyber resilience evaluation would support the human integration aspect in the CPSS and meet the situation awareness characteristics in the human decision-making process.

In addition to this primary contribution, this work makes a couple of secondary contributions that are also significant:

Systematic identification of CPSS characteristics and applications. I discussed The CPSS challenges and open issues in different domains from both technical and social aspects.

Findings on the experimental evaluations of the approach based on a new approach for designing the experimental isolated lab facilitated by virtual machines and security tools.

8.5 Final Consideration and Future Work

In this work, the control part of a CPSS was modeled by Petri nets, where the list of attributes that can be associated with transitions firing was augmented with a dynamic time attribute (extending Time Petri nets common execution semantics). This attribute is the result of a calculation involving specific input signals. In this sense, this proposal put together and reuses time dependencies, normally considered for performance analysis, also in the context of controller modeling, introducing this non-autonomous characteristic as an external value.

This Chapter provides a conclusion of this Ph.D. thesis dedicated to cyber resilience in cyber physical social systems. It likewise presents light on the future exploration and specialized exercises that can be embraced in the area of CPSS and cyber resilience. Toward the finish of this part, it is normal that the readers will have a comprehension of the exploration consequences of this Ph.D. work and inspirations for future exploration, and specialized headings that can be embraced toward accomplishing cyber resilient CPSS.

8.5.1 Future work

Throughout conducting this thesis, I have intermittently noted some areas in which further investigation would be necessary for elucidating open issues or advancing the state of knowledge regarding certain aspects. In this section, I enumerate some utmost future areas of work where I believe several significant research challenges remain and as a result, several perspectives for long-term study can be anticipated:

Extending modeling in the cyber-resilience phases to self-adaption phases as well. In this work, I considered the resilience phases including understanding, absorbing, and recovery. Integrating the adapting phase is an open area for future studies. By applying knowledge from previous experiences self-adapted and learning machines (smart systems and social systems) will be resilient and adaptive. However, one generalization of the work is to determine differently sets of adaptation rules at design time and switch between them.

Automate the process of translation. The proposed set of rules for translating GrSMs to/from TCPN is a starting point to develop a prototype for automated translations between these two models. It could be a new application or one augmented with existing tools for these graphical models. In this work, I illustrated the threat scenarios by AD Tool and CPN by CPN Tools version 4.0.1.

Consider other social characteristics and dynamics among social nodes In this thesis, I applied Endsley's mental model for studying situation awareness which impacts human behavior in one type of attack (Social Engineering- email phishing). This aspect of work can be studied further by considering social network activities and connections and profiling each node as I did with cyber systems in this work.

Extending to other application domains. The final front for extending this work is an application of TCPN to other application domains. I have already done this for the problem of cyber-resilience in web-based services. However, multiple other application domains can be extended to benefit from the contributions of this thesis such as management systems, and medical systems. Another domain that the proposed concepts and models in this work can fit perfectly is digital twins.

Bibliography

[1] F. Y. Wang. “The emergence of intelligent enterprises: From CPS to CPSS”. In: *IEEE Intelligent Systems* 25.4 (2010), pp. 85–88 (cit. on pp. 1, 43, 45).

[2] *cyber-physical-systems-cps*. URL: https://beta.nsf.gov/funding/opportunities/cyber-physical-systems-cpsf. (accessed: 2021) (cit. on p. 1).

[3] P. D. Castillo. *Shaping Europe’s digital future*. URL: https://www.europeanfiles.eu/digital/shaping-europes-digital-future. (accessed: 20.4.2021) (cit. on pp. 1, 48).

[4] F.-Y. Wang et al. “Social Computing: From Social Informatics to Social Intelligence”. In: *IEEE Intelligent Systems* 22.2 (2007), pp. 79–83. DOI: 10.1109/MIS.2007.41 (cit. on pp. 2, 51, 59).

[5] L. G. Anthopoulos. “Understanding the smart city domain: A literature review”. In: *Transforming city governments for successful smart cities* (2015), pp. 9–21 (cit. on pp. 2, 45, 54).

[6] I. Ashari. “Implementation of Cyber-Physical-Social System Based on Service Oriented Architecture in Smart Tourism”. In: *Journal of Applied Informatics and Computing (JAIC)* 4.1 (June 2020), pp. 66–73. DOI: 10.30871/jaic.v4i1.2077. URL: https://jurnal.polibatam.ac.id/index.php/JAIC/article/view/2077 (cit. on pp. 2, 48, 54, 55, 62).

[7] T. Ali, M. Gheith, and E. S. Nasr. “Socially intelligent computing — A survey of an emerging field for empowering crowd”. In: *2014 9th International Conference on Informatics and Systems*. 2014, PDC-102-PDC–108. DOI: 10.1109/INFOS.2014.7036685 (cit. on pp. 2, 58).

[8] I. Linkov and A. Kott. “Fundamental concepts of cyber resilience: Introduction and overview”. In: *Cyber resilience of systems and networks*. Springer, 2019, pp. 1–25 (cit. on p. 3).

[9] D. J. Bodeau et al. *Cyber resiliency engineering framework*. Tech. rep. MITRE CORP BEDFORD MA, 2011. URL: https://www.mitre.org/sites/default/files/pdf/11%5C_4436.pdf (cit. on pp. 3, 19, 27, 40).

[10] M. Barbeau et al. "Resilience Estimation of Cyber-Physical Systems via Quantitative Metrics". In: *IEEE Access* 9 (2021), pp. 46462–46475. DOI: 10.1109/ACCESS.2021.3066108 (cit. on p. 3).

[11] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez. "A review of definitions and measures of system resilience". In: *Reliability Engineering & System Safety* 145 (2016), pp. 47–61. URL: https://www.sciencedirect.com/science/article/pii/S0951832015002483 (cit. on pp. 4, 21).

[12] L. Atzori, A. Iera, and G. Morabito. "SIoT: Giving a Social Structure to the Internet of Things". In: *IEEE Communications Letters* 15.11 (2011), pp. 1193–1195. DOI: 10.1109/LCOMM.2011.090911.111340 (cit. on pp. 4, 50).

[13] J. B. Hong et al. "A survey on the usability and practical applications of Graphical Security Models". In: *Computer Science Review* 26 (2017), pp. 1–16. ISSN: 1574-0137. DOI: 10.1016/j.cosrev.2017.09.001. URL: https://www.sciencedirect.com/science/article/pii/S1574013716301083 (cit. on pp. 4, 30, 31, 33).

[14] Y. Y. Haimes. "On the Definition of Resilience in Systems". In: *Risk Analysis* 29.4 (2009), pp. 498–501. URL: https://EconPapers.repec.org/RePEc:wly:riskan:v:29:y:2009:i:4:p:498-501 (cit. on p. 5).

[15] K. Jensen and L. M. Kristensen. *Coloured Petri nets: modelling and validation of concurrent systems*. Springer Science & Business Media, 2009 (cit. on pp. 5, 73).

[16] L. M. Camarinha-Matos. *Scientific Research Methodologies and Techniques: RESEARCH METHOD*. 2016. URL: https://sites.google.com/a/uninova.pt/cam/teaching/srmt (cit. on p. 10).

[17] J. Zeng et al. "A survey: Cyber-physical-social systems and their system-level design methodology". In: *Future Gener. Comput. Syst.* 105 (2020), pp. 1028–1042 (cit. on pp. 16, 18, 43, 45, 59).

[18] Y. Zhu et al. "Cyber-physical-social-thinking modeling and computing for geological information service system". In: *International Journal of Distributed Sensor Networks* 12.11 (2016). DOI: 10.1177/1550147716666666 (cit. on pp. 16, 43, 49, 53, 58).

[19] J. Zeng et al. "System-Level Design Optimization for Security-Critical Cyber-Physical-Social Systems". In: *ACM Trans. Embed. Comput. Syst.* 16.2 (Apr. 2017). ISSN: 1539-9087. DOI: 10.1145/2925991. URL: https://doi.org/10.1145/2925991 (cit. on pp. 16, 18).

[20] S. Pasandideh, L. Gomes, and P. Maló. "Modelling Cyber Physical Social Systems Using Dynamic Time Petri Nets". In: *Doctoral Conference on Computing, Electrical and Industrial Systems*. Springer. 2018, pp. 81–89. ISBN: 978-3-319-78573-8. DOI: 10.1007/978-3-319-78574-5_8 (cit. on pp. 16, 18).

[21] L. Gomes et al. “The Input-Output Place-Transition Petri Net Class and Associated Tools”. In: *INDIN’2007 - 5th IEEE International Conference on Industrial Informatics*. 2007. DOI: 10.1109/INDIN.2007.4384809 (cit. on p. 16).

[22] F.-Y. Wang. “Toward a paradigm shift in social computing: The ACP approach”. In: *IEEE Intelligent Systems* 22.5 (2007), pp. 65–67 (cit. on p. 16).

[23] A. Smirnov, T. Levashova, and A. Kashevnik. “Ontology-based resource interoperability in socio-cyber-physical systems”. In: *Information Technology in Industry* 6.2 (2018) (cit. on pp. 17, 18).

[24] A. Smirnov et al. “Ontology for cyber-physical-social systems self-organisation”. In: *Proceedings of 16th Conference of Open Innovations Association FRUCT*. 2014, pp. 101–107. DOI: 10.1109/FRUCT.2014.7000933 (cit. on pp. 17, 18, 50, 51).

[25] A. Zimmermann, A. Lorenz, and R. Oppermann. “An Operational Definition of Context”. In: vol. 4635. Aug. 2007, pp. 558–571. ISBN: 978-3-540-74254-8. DOI: 10.1007/978-3-540-74255-5_42 (cit. on p. 17).

[26] A. Smirnov, A. Kashevnik, and A. Ponomarev. “Multi-level Self-organization in Cyber-Physical-Social Systems: Smart Home Cleaning Scenario”. In: *Procedia CIRP* 30 (2015). 7th Industrial Product-Service Systems Conference - PSS, industry transformation for sustainability and business, pp. 329–334. ISSN: 2212-8271. DOI: 10.1016/j.procir.2015.02.089 (cit. on pp. 17, 18, 55).

[27] P. Wang et al. “Data fusion in cyber-physical-social systems: State-of-the-art and perspectives”. In: *Information Fusion* 51 (2019), pp. 42–57 (cit. on pp. 17, 18, 57, 58, 62).

[28] B. Guo, Z. Yu, and X. Zhou. “A Data-Centric Framework for Cyber-Physical-Social Systems”. In: *IT Professional* 17.06 (Nov. 2015), pp. 4–7. ISSN: 1941-045X. DOI: 10.1109/MITP.2015.116 (cit. on pp. 17, 54, 62).

[29] S. De et al. “Cyber–Physical–Social frameworks for urban big data systems: A Survey”. In: *Applied Sciences* 7.10 (Oct. 2017), p. 1017. ISSN: 2076-3417. DOI: 10.3390/app7101017. URL: http://dx.doi.org/10.3390/app7101017 (cit. on pp. 18, 45, 47, 54, 55, 62).

[30] B. Yilma, H. Panetto, and Y. Naudet. “Systemic formalisation of Cyber-Physical-Social System (CPSS): A systematic literature review”. In: *Computers in Industry* 129 (Aug. 2021), p. 103458. DOI: 10.1016/j.compind.2021.103458 (cit. on pp. 18, 49, 51).

[31] G. Xiong et al. “Collaborative Optimization of Cyber Physical Social Systems for Urban Transportation Based on Knowledge Automation”. In: *IFAC-PapersOnLine* 53 (Jan. 2020), pp. 572–577. DOI: 10.1016/j.ifacol.2021.04.144 (cit. on pp. 18, 43).

[32] A. Sheth, P. Anantharam, and C. Henson. “Physical-Cyber-Social computing: An early 21st century approach”. In: *IEEE Intelligent Systems* 28.1 (2013), pp. 78–82. DOI: 10.1109/MIS.2013.20 (cit. on pp. 18, 45, 51).

[33] G. Chatzigeorgakidis et al. “FML-kNN: scalable machine learning on Big Data using k-nearest neighbor joins”. In: *Journal of Big Data* 5 (Feb. 2018). DOI: 10.1186/s40537-018-0115-x (cit. on p. 18).

[34] W. Zhang et al. “A Distributed Storage and Computation k-Nearest Neighbor Algorithm Based Cloud-Edge Computing for Cyber-Physical-Social Systems”. In: *IEEE Access* 8 (2020), pp. 50118–50130. DOI: 10.1109/ACCESS.2020.2974764 (cit. on p. 18).

[35] D. Ormrod and B. Turnbull. “Modeling and Simulation Approaches”. In: *Cyber Resilience of Systems and Networks*. Springer, 2019, pp. 171–193 (cit. on p. 19).

[36] R. Arghandeh et al. “On the definition of cyber-physical resilience in power systems”. In: *Renewable and Sustainable Energy Reviews* 58 (2016), pp. 1060–1069 (cit. on pp. 19, 24).

[37] D. J. Bodeau et al. *CYBER RESILIENCY METRICS AND SCORING IN PRACTICE– USE CASE METHODOLOGY AND EXAMPLES*. Nov. 2018. URL: https://www.mitre.org/publications/technical-papers/cyber-resiliency-metrics-and-scoring-in-practice-use-case-methodology (cit. on pp. 19, 85).

[38] S. Sheard. “A framework for system resilience discussions”. In: *INCOSE International Symposium*. Vol. 18. 1. Wiley Online Library. 2008, pp. 1243–1257 (cit. on p. 20).

[39] *PROTECTING CRITICAL INFRASTRUCTURE*. 2018. URL: https://www.cisa.gov/protecting-critical-infrastructure. (cit. on p. 20).

[40] A. Kott et al. “Approaches to enhancing cyber resilience: Report of the North Atlantic Treaty Organization (NATO) workshop IST-153”. In: (2018). arXiv: 1804.07651 [cs.CR] (cit. on p. 20).

[41] S. L. Cutter et al. “Disaster resilience: A national imperative”. In: *Environment: Science and Policy for Sustainable Development* 55.2 (2013), pp. 25–29 (cit. on pp. 20, 24).

[42] D. Nicol, W. Sanders, and K. Trivedi. “Model-based evaluation: from dependability to security”. In: *IEEE Transactions on Dependable and Secure Computing* 1.1 (2004), pp. 48–65. DOI: 10.1109/TDSC.2004.11 (cit. on p. 21).

[43] C.-W. Ten, G. Manimaran, and C.-C. Liu. “Cybersecurity for Critical Infrastructures: Attack and Defense Modeling”. In: *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 40.4 (2010), pp. 853–865. DOI: 10.1109/TSMCA.2010.2048028 (cit. on p. 21).

[44] A. Kott and I. Linkov. *Cyber resilience of systems and networks*. Springer, 2019 (cit. on pp. 21–23).

[45] Y. I. Khan, E. Al-Shaer, and U. Rauf. "Cyber resilience-by-construction: Modeling, measuring & verifying". In: *Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense*. 2015, pp. 9–14 (cit. on p. 21).

[46] K. Paridari et al. "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration". In: *Proceedings of the IEEE* 106.1 (2017), pp. 113–128 (cit. on p. 21).

[47] M. Kaâniche et al. "Modeling the resilience of large and evolving systems". In: *arXiv preprint arXiv:1211.5738* (2012) (cit. on p. 22).

[48] S. Natouri, C. Lac, and A. Serhrouchni. "Resilience design using the Challenge Countermeasure Tree (CCT) model". In: *2014 Applications and Innovations in Mobile Computing (AIMoC)*. IEEE. 2014, pp. 165–171 (cit. on p. 22).

[49] S. A. Zonouz et al. "RRE: A game-theoretic intrusion response and recovery engine". In: *IEEE Transactions on Parallel and Distributed Systems* 25.2 (2013), pp. 395–406 (cit. on p. 22).

[50] S. Pradhan et al. "Achieving resilience in distributed software systems via self-reconfiguration". In: *Journal of Systems and Software* 122 (2016), pp. 344–363 (cit. on p. 22).

[51] D. Liveri and A. Sarri. *An evaluation Framework for National Cyber Security Strategies*. Nov. 2014. URL: https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies (cit. on p. 22).

[52] A. Cardenas et al. "Challenges for securing cyber physical systems". In: *Workshop on future directions in cyber-physical systems security*. Vol. 5. 1. Citeseer. 2009 (cit. on p. 22).

[53] I. Linkov et al. "Resilience metrics for cyber systems". In: *Environment Systems and Decisions* 33.4 (2013), pp. 471–476 (cit. on p. 24).

[54] K. A. Ouedraogo, S. Enjalbert, and F. Vanderhaegen. "How to learn from the resilience of Human–Machine Systems?" In: *Engineering Applications of Artificial Intelligence* 26.1 (2013), pp. 24–34 (cit. on p. 24).

[55] B. A. Yilma, Y. Naudet, and H. Panetto. "Introduction to personalisation in cyber-physical-social systems". In: *OTM/IFAC/IFIP International Workshop on Enterprise Integration, Interoperability and Networking, EI2N 2018*. Ed. by C. Debruyne et al. Vol. 11231. On the Move to Meaningful Internet Systems. OTM 2018 Workshops. DOA Institute. La Vallette, Malta: Springer, Oct. 2018, pp. 25–35. DOI: 10.1007/978-3-030-11683-5_3. URL: https://hal.archives-ouvertes.fr/hal-02009913 (cit. on pp. 24, 54, 57).

[56] D. Bodeau et al. *Cyber resiliency engineering aid-the updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques*. Tech. rep. MITRE CORP BEDFORD MA BEDFORD United States, 2015 (cit. on pp. 24, 25).

[57] D. Henry and J. Emmanuel Ramirez-Marquez. "Generic metrics and quantitative approaches for system resilience as a function of time". In: *Reliability Engineering System Safety* 99 (2012), pp. 114–122. ISSN: 0951-8320. DOI: https://doi.org/10.1016/j.ress.2011.09.002. URL: https://www.sciencedirect.com/science/article/pii/S0951832011001748 (cit. on p. 26).

[58] H. R. Heinimann. *Future Resilient Systems: FRS Booklet*. URL: https://ethz.ch/content/dam/ethz/special-interest/dual/frs-dam/documents/FRS-Booklet.pdf (cit. on p. 26).

[59] D. J. Bodeau et al. *Cyber resiliency metrics and scoring in practice–use case METHODOLOGY AND EXAMPLES*. The MITRE Corporation, Sept. 2018 (cit. on pp. 27, 84).

[60] R. Ross et al. *Developing cyber resilient systems: a systems security engineering approach*. Tech. rep. National Institute of Standards and Technology, 2019 (cit. on p. 27).

[61] Y. I. Khan, E. Al-shaer, and U. Rauf. "Cyber Resilience-by-Construction: Modeling, Measuring Verifying". In: *Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense*. SafeConfig '15. Denver, Colorado, USA: Association for Computing Machinery, 2015, pp. 9–14. ISBN: 9781450338219. DOI: 10.1145/2809826.2809836. URL: https://doi.org/10.1145/2809826.2809836 (cit. on p. 29).

[62] A. Humayed et al. "Cyber-Physical Systems Security—A Survey". In: *IEEE Internet of Things Journal* 4.6 (2017), pp. 1802–1831. DOI: 10.1109/JIOT.2017.2703172 (cit. on p. 29).

[63] S. Nazir, S. Patel, and D. Patel. "Assessing and augmenting SCADA cyber security: A survey of techniques". In: *Computers Security* 70 (2017), pp. 436–454. ISSN: 0167-4048. DOI: 10.1016/j.cose.2017.06.010. URL: https://www.sciencedirect.com/science/article/pii/S0167404817301293 (cit. on p. 30).

[64] S. Pudar, G. Manimaran, and C.-C. Liu. "PENET: A practical method and tool for integrated modeling of security attacks and countermeasures". In: *Computers Security* 28.8 (2009), pp. 754–771. ISSN: 0167-4048. DOI: 10.1016/j.cose.2009.05.007. URL: https://www.sciencedirect.com/science/article/pii/S0167404809000522 (cit. on pp. 30, 37).

[65] L. M. Almutairi and S. Shetty. "Generalized stochastic Net model based security risk assessment of software defined networks". In: *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*. 2017, pp. 545–550. DOI: 10.1109/MILCOM.2017.8170813 (cit. on p. 30).

[66] V. Nagaraju, L. Fiondella, and T. Wandji. "A survey of fault and attack tree modeling and analysis for cyber risk management". In: *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*. 2017, pp. 1–6. DOI: 10.1109/THS.2017.7943455 (cit. on p. 30).

[67] B. Schneier. *Modeling security threats: Attack Tree*. Dec. 1999. URL: https://www.schneier.com/academic/archives/1999/12/attack%5C_trees.html (cit. on pp. 31, 39).

[68] M. Ajmone Marsan, A. Bobbio, and S. Donatelli. "Petri nets in performance analysis: An introduction". In: *Lectures on Petri Nets I: Basic Models: Advances in Petri Nets*. Ed. by W. Reisig and G. Rozenberg. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 211–256. ISBN: 978-3-540-49442-3. DOI: 10.1007/3-540-65306-6_17. URL: https://doi.org/10.1007/3-540-65306-6_17 (cit. on p. 31).

[69] K. S. Trivedi et al. "Dependability and security models". In: *2009 7th International Workshop on Design of Reliable Communication Networks*. 2009, pp. 11–20. DOI: 10.1109/DRCN.2009.5340029 (cit. on p. 31).

[70] S. Bistarelli, F. Fioravanti, and P. Peretti. "Defense trees for economic evaluation of security investments". In: *First International Conference on Availability, Reliability and Security (ARES'06)*. Vol. 8. 2006, p. 423. DOI: 10.1109/ARES.2006.46 (cit. on pp. 31, 39).

[71] K. Edge. "A Framework For Analyzing And Mitigating The Vulnerabilities Of Complex Systems Via Attack And Protection Trees". In: (July 2007), p. 219 (cit. on pp. 31, 40).

[72] S. A. Zonouz et al. "RRE: A game-theoretic intrusion Response and Recovery Engine". In: *2009 IEEE/IFIP International Conference on Dependable Systems Networks*. 2009, pp. 439–448. DOI: 10.1109/DSN.2009.5270307 (cit. on p. 32).

[73] K. Daley, R. Larson, and J. Dawkins. "A structural framework for modeling multi-stage network attacks". In: *Proceedings. International Conference on Parallel Processing Workshop*. 2002, pp. 5–10. DOI: 10.1109/ICPPW.2002.1039705 (cit. on p. 32).

[74] A. Roy, D. S. Kim, and K. S. Trivedi. "Cyber Security Analysis Using Attack Countermeasure Trees". In: *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*. CSIIRW '10. Oak Ridge, Tennessee, USA: Association for Computing Machinery, 2010. ISBN: 9781450300179. DOI:

10.1145/1852666.1852698. URL: 10.1145/1852666.1852698 (cit. on pp. 32, 39, 76, 82).

[75] B. Kordy et al. "Attack-Defense Trees and Two-Player Binary Zero-Sum Extensive Form Games Are Equivalent". In: *Proceedings of the First International Conference on Decision and Game Theory for Security*. GameSec'10. Berlin, Germany: Springer-Verlag, 2010, pp. 245–256. ISBN: 3642171966 (cit. on pp. 33, 40).

[76] B. Kordy et al. "ADTool: Security Analysis with Attack–Defense Trees". In: *Quantitative Evaluation of Systems Lecture Notes in Computer Science* (2013), pp. 173–176. DOI: 10.1007/978-3-642-40196-1_15 (cit. on pp. 33, 41).

[77] R. Kumar and M. Stoelinga. "Quantitative Security and Safety Analysis with Attack-Fault Trees". In: *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*. 2017, pp. 25–32. DOI: 10.1109/HASE.2017.12 (cit. on pp. 33, 40).

[78] H. Hermanns et al. "The Value of Attack-Defence Diagrams". In: *Proceedings of the 5th International Conference on Principles of Security and Trust - Volume 9635*. Berlin, Heidelberg: Springer-Verlag, 2016, pp. 163–185. ISBN: 9783662496343 (cit. on pp. 33, 40).

[79] J. P. McDermott. "Attack Net Penetration Testing". In: *Proceedings of the 2000 Workshop on New Security Paradigms*. NSPW '00. Ballycotton, County Cork, Ireland: Association for Computing Machinery, 2001, pp. 15–21. ISBN: 1581132603. DOI: 10.1145/366173.366183. URL: https://doi.org/10.1145/366173.366183 (cit. on p. 33).

[80] J. B. Hong and D. S. Kim. "Towards scalable security analysis using multi-layered security models". In: *Journal of Network and Computer Applications* 75 (2016), pp. 156–168. ISSN: 1084-8045. DOI: 10.1016/j.jnca.2016.08.024. URL: https://www.sciencedirect.com/science/article/pii/S1084804516301928 (cit. on pp. 33, 40).

[81] R. Zurawski and M. Zhou. "Petri nets and industrial applications: A tutorial". In: *IEEE Transactions on Industrial Electronics* 41.6 (1994), pp. 567–583 (cit. on p. 35).

[82] M. A. Holliday and M. K. Vernon. "A Generalized Timed Petri Net Model for Performance Analysis". In: *International Workshop on Timed Petri Nets*. USA: IEEE Computer Society, 1985, pp. 181–190. ISBN: 0818606746 (cit. on p. 35).

[83] Dalton et al. "Analyzing Attack Trees using Generalized Stochastic Petri Nets". In: *2006 IEEE Information Assurance Workshop*. 2006, pp. 116–123. DOI: 10.1109/IAW.2006.1652085 (cit. on pp. 35, 67).

[84] M. Ajmone Marsan, G. Conte, and G. Balbo. "A class of generalized stochastic Petri nets for the performance evaluation of multiprocessor systems". In: *ACM Transactions on Computer Systems (TOCS)* 2.2 (1984), pp. 93–122 (cit. on p. 36).

[85] T. Murata. "Petri nets: Properties, analysis and applications". In: *Proceedings of the IEEE* 77.4 (1989), pp. 541–580 (cit. on p. 37).

[86] L. Yao et al. "Network security analyzing and modeling based on Petri net and Attack tree for SDN". In: *2016 International Conference on Computing, Networking and Communications (ICNC)*. IEEE. 2016, pp. 1–5 (cit. on p. 37).

[87] R. Wu, W. Li, and H. Huang. "An attack modeling based on hierarchical colored Petri nets". In: *2008 International Conference on Computer and Electrical Engineering*. IEEE. 2008, pp. 918–921 (cit. on p. 37).

[88] W. H. Sanders and J. F. Meyer. "Stochastic activity networks: formal definitions and concepts". In: *School Organized by the European Educational Forum*. Springer. 2000, pp. 315–343 (cit. on p. 37).

[89] D. Codetta-Raiteri. "A Preliminary Application of Generalized Fault Trees to Security". In: *Proceedings of the 10th International Conference on Security and Cryptography - SECRYPT, (ICETE 2013)*. INSTICC. SciTePress, 2013, pp. 609–614. ISBN: 978-989-8565-73-0. DOI: 10.5220/0004612606090614 (cit. on p. 37).

[90] S. Pasandideh, L. Gomes, and P. Maló. "Improving Attack Trees Analysis using Petri Net modeling of Cyber-Attacks". In: *2019 IEEE 28th International Symposium on Industrial Electronics (ISIE)*. 2019, pp. 1644–1649. DOI: 10.1109/ISIE.2019.8781238 (cit. on pp. 37, 67, 68).

[91] B. Li et al. "On reliability analysis of smart grids under topology attacks: A stochastic Petri net approach". In: *ACM Transactions on Cyber-Physical Systems* 3.1 (2018), pp. 1–25 (cit. on p. 37).

[92] N. Yang et al. "Modeling and quantitatively predicting software security based on stochastic Petri nets". In: *Mathematical and Computer Modelling* 55.1-2 (2012), pp. 102–112 (cit. on p. 38).

[93] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford. "Petri net modeling of cyber-physical attacks on smart grid". In: *IEEE Transactions on smart grid* 2.4 (2011), pp. 741–749 (cit. on p. 38).

[94] M. Pflanz and A. Levis. "An approach to evaluating resilience in command and control architectures". In: *Procedia Computer Science* 8 (2012), pp. 141–146 (cit. on p. 38).

[95] B. Jasiul, M. Szpyrka, and J. Śliwa. "Malware Behavior Modeling with Colored Petri Nets". In: *13th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM)*. Ed. by K. Saeed and V. Snášel. Vol. LNCS-8838. Computer Information Systems and Industrial Management. Part 9: Various Aspects of Computer Security. Ho Chi Minh City, Vietnam: Springer, Nov. 2014, pp. 667–679. DOI: 10.1007/978-3-662-45237-0_60. URL: https://hal.inria.fr/hal-01405661 (cit. on p. 38).

[96] X. X. Yang Xu. “Modeling and Analysis of Security Protocols Using Colored Petri Nets”. In: *Journal of Computers* 6.1 (2011), pp. 19–27. DOI: 10.4304/jcp.6.1.19-27 (cit. on p. 38).

[97] X. Liu et al. “A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure”. In: *IEEE Transactions on Smart Grid* 6.5 (2015), pp. 2435–2443 (cit. on p. 38).

[98] L. Kahloul et al. “Modeling and verification of rbac security policies using colored Petri nets and cpn-tool”. In: *International Conference on Networked Digital Technologies*. Springer. 2010, pp. 604–618 (cit. on p. 38).

[99] K. Juszczyszyn. “Verifying enterprise’s mandatory access control policies with coloured Petri nets”. In: *WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003.* 2003, pp. 184–189. DOI: 10.1109/ENABL.2003.1231405 (cit. on p. 38).

[100] L. Kallab et al. “Using Colored Petri Nets for Verifying RESTful Service Composition”. In: *OTM Confederated International Conferences ”On the Move to Meaningful Internet Systems”*. Vol. 10573. On the Move to Meaningful Internet Systems. OTM 2017 Conferences Confederated International Conferences: CoopIS, C
TC, and ODBASE 2017, Rhodes, Greece, October 23-27, 2017, Proceedings, Rhodes, Greece, Oct. 2017, pp. 505–523. DOI: 10.1007/978-3-319-69462-7_32. URL: https://hal.archives-ouvertes.fr/hal-01592920 (cit. on p. 38).

[101] O. Dahl and S. Wolthusen. “Modeling and execution of complex attack scenarios using interval timed colored Petri nets”. In: *Fourth IEEE International Workshop on Information Assurance (IWIA’06)*. 2006, 12 pp.–168. DOI: 10.1109/IWIA.2006.17 (cit. on p. 38).

[102] A. E. Bouchti and A. Haqiq. “Modeling cyber-attack for SCADA systems using CoPNet approach”. In: *2012 IEEE International Conference on Complex Systems (ICCS)*. 2012, pp. 1–6. DOI: 10.1109/ICoCS.2012.6458588 (cit. on pp. 38, 39).

[103] J. N. Whitley et al. “Attribution of attack trees”. In: *Computers Electrical Engineering* 37.4 (2011), pp. 624–628. ISSN: 0045-7906. DOI: 10.1016/j.compeleceng.2011.04.010. URL: https://www.sciencedirect.com/science/article/pii/S0045790611000553 (cit. on p. 39).

[104] *GreatSPN*. URL: http://www.di.unito.it/~greatspn/index.html (cit. on p. 41).

[105] *Documentation*. URL: http://cpntools.org/category/documentation/ (cit. on p. 41).

[106] K. Jensen, L. M. Kristensen, and L. Wells. "Coloured Petri nets and CPN tools for modelling and validation of Concurrent Systems". In: *International Journal on Software Tools for Technology Transfer* 9.3-4 (2007), pp. 213–254. DOI: 10.1007/s10009-007-0038-x (cit. on p. 41).

[107] A. V. Ratzer et al. "CPN tools for editing, simulating, and analysing coloured Petri nets". In: *International conference on application and theory of Petri nets*. Springer. 2003, pp. 450–462 (cit. on p. 41).

[108] E. Lee. "The past, present and future of Cyber-Physical Systems: A focus on models". In: *Sensors* 15.3 (Feb. 2015), pp. 4837–4869. ISSN: 1424-8220. DOI: 10.3390/s150304837. URL: http://dx.doi.org/10.3390/s150304837 (cit. on pp. 43, 45).

[109] R. Dautov et al. "Data processing in Cyber-Physical-Social systems through edge computing". In: *IEEE Access* 6 (2018), pp. 29822–29835 (cit. on pp. 43, 58).

[110] K. Ding and P. Jiang. "Incorporating social sensors, cyber-physical system nodes, and smart products for personalized production in a social manufacturing environment". In: *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture* 232.13 (2018), pp. 2323–2338. ISSN: 20412975. DOI: 10.1177/0954405417716728 (cit. on pp. 43, 54, 56).

[111] C. G. Cassandras. "Smart cities as cyber-physical social systems". In: *Engineering* 2.2 (2016), pp. 156–158. ISSN: 2095-8099. DOI: 10.1016/J.ENG.2016.02.012. URL: https://www.sciencedirect.com/science/article/pii/S2095809916309420 (cit. on pp. 43, 49, 54, 62).

[112] G. Xiong et al. "Cyber-Physical-Social Systems for smart city: An implementation based on intelligent loop". In: *IFAC-PapersOnLine* 53.5 (2020). 3rd IFAC Workshop on Cyber-Physical Human Systems CPHS 2020, pp. 501–506. ISSN: 2405-8963. DOI: 10.1016/j.ifacol.2021.04.136. URL: https://www.sciencedirect.com/science/article/pii/S2405896321002603 (cit. on pp. 43, 54).

[113] G. Xiong et al. "Cyber-physical-social system in intelligent transportation". In: *IEEE/CAA Journal of Automatica Sinica* 2.3 (2015), pp. 320–333 (cit. on pp. 43, 54, 55, 59).

[114] J. Koh and Y. Kim. "Knowledge Sharing in Virtual Communities: An E-Business Perspective". In: *Expert Systems with Applications* 26 (Feb. 2004), pp. 155–166. DOI: 10.1016/S0957-4174(03)00116-7 (cit. on p. 44).

[115] M. Parameswaran and A. Whinston. "Social computing: An overview". In: *Communications of the Association for Information Systems* 19 (Jan. 2007), pp. 762–780. DOI: 10.17705/1CAIS.01937 (cit. on p. 44).

[116] H. B. El-Haouzi et al. “Social dimensions in CPS IoT based automated production systems”. In: *Societies* 11.3 (Aug. 2021), p. 98. ISSN: 2075-4698. DOI: 10.3390/soc11030098. URL: http://dx.doi.org/10.3390/soc11030098 (cit. on pp. 45, 48).

[117] M. Jirgl, Z. Bradac, and P. Fiedler. “Human-in-the-Loop issue in context of the cyber-physical systems”. In: *IFAC-PapersOnLine* 51.6 (2018). 15th IFAC Conference on Programmable Devices and Embedded Systems PDeS 2018, pp. 225–230. ISSN: 2405-8963. DOI: 10.1016/j.ifacol.2018.07.158. URL: https://www.sciencedirect.com/science/article/pii/S2405896318309042 (cit. on p. 45).

[118] G. Schirner et al. “The future of Human-in-the-Loop cyber-physical systems”. In: *Computer* 46.1 (2013), pp. 36–45. DOI: 10.1109/MC.2013.31 (cit. on pp. 45, 57).

[119] M. Tyworth et al. “A Human-In-The-Loop Approach to Understanding Situation Awareness in Cyber Defense Analysis”. In: *EAI Endorsed Transactions on Security and Safety* 13 (May 2013), pp. 1–10. DOI: 10.4108/trans.sesa.01-06.2013.e6 (cit. on p. 45).

[120] M. A. R. Garcia et al. “A human-in-the-loop cyber-physical system for collaborative assembly in smart manufacturing”. In: *Procedia CIRP* 81 (2019). 52nd CIRP Conference on Manufacturing Systems (CMS), Ljubljana, Slovenia, June 12-14, 2019, pp. 600–605. ISSN: 2212-8271. DOI: 10.1016/j.procir.2019.03.162. URL: https://www.sciencedirect.com/science/article/pii/S2212827119304676 (cit. on pp. 45, 58).

[121] Z. Su et al. “Incentive scheme for cyber physical social systems based on user behaviors”. In: *IEEE Transactions on Emerging Topics in Computing* 8.1 (2020), pp. 92–103. DOI: 10.1109/TETC.2017.2671843 (cit. on pp. 45, 51).

[122] X. Wang et al. “A Cloud-Edge Computing Framework for Cyber-Physical-Social Services”. In: *IEEE Communications Magazine* 55.11 (2017), pp. 80–85. DOI: 10.1109/MCOM.2017.1700360 (cit. on pp. 46, 51).

[123] G.-G. Wang et al. “High Performance Computing for Cyber Physical Social Systems by Using Evolutionary Multi-Objective Optimization Algorithm”. In: *IEEE Transactions on Emerging Topics in Computing* 8.1 (2020), pp. 20–30. DOI: 10.1109/TETC.2017.2703784 (cit. on pp. 46, 62).

[124] S. Dhawan. “Online Learning: A Panacea in the Time of COVID-19 Crisis”. In: *Journal of Educational Technology Systems* 49.1 (2020), pp. 5–22. DOI: 10.1177/0047239520934018. URL: https://doi.org/10.1177/0047239520934018 (cit. on pp. 47, 62).

[125] H. Ning et al. “Cybermatics: Cyber-physical-social-thinking hyperspace based science and technology”. In: *Future Generation Computer System* 56 (2016), pp. 504–522 (cit. on p. 47).

[126] F. Dressler. "Cyber Physical Social Systems: Towards Deeply Integrated Hybridized Systems". In: *2018 International Conference on Computing, Networking and Communications (ICNC)*. 2018, pp. 420–424. DOI: 10.1109/ICCNC.2018.8390404 (cit. on pp. 47, 49, 51, 55, 62).

[127] J. Feng et al. "Privacy-preserving computation in cyber-physical-social systems: A survey of the state-of-the-art and perspectives". In: *Information Sciences* 527 (2020), pp. 341–355 (cit. on pp. 48, 62).

[128] R. K. Ganti, Y.-E. Tsai, and T. F. Abdelzaher. "SenseWorld: Towards Cyber-Physical Social Networks". In: *Proceedings of the 7th International Conference on Information Processing in Sensor Networks*. IPSN '08. USA: IEEE Computer Society, 2008, pp. 563–564. ISBN: 9780769531571. DOI: 10.1109/IPSN.2008.48. URL: https://doi.org/10.1109/IPSN.2008.48 (cit. on p. 48).

[129] M. Conti, A. Passarella, and S. K. Das. "The Internet of People (IoP): A new wave in pervasive mobile computing". In: *Pervasive and Mobile Computing* 41 (2017), pp. 1–27. ISSN: 1574-1192. DOI: 10.1016/j.pmcj.2017.07.009. URL: https://www.sciencedirect.com/science/article/pii/S1574119217303723 (cit. on p. 49).

[130] L. Atzori et al. "The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization". In: *Computer Networks* 56.16 (2012), pp. 3594–3608. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2012.07.010. URL: https://www.sciencedirect.com/science/article/pii/S1389128612002654 (cit. on pp. 49, 50).

[131] F. Xia and J. Ma. "Building Smart Communities with Cyber-Physical Systems". In: *Proceedings of 1st International Symposium on From Digital Footprints to Social and Community Intelligence*. SCI '11. Beijing, China: Association for Computing Machinery, 2011, pp. 1–6. ISBN: 9781450309257. DOI: 10.1145/2030066.2030068. URL: 10.1145/2030066.2030068 (cit. on p. 49).

[132] A. M. Ortiz et al. "The Cluster Between Internet of Things and Social Networks: Review and Research Challenges". In: *IEEE Internet of Things Journal* 1.3 (2014), pp. 206–215. DOI: 10.1109/JIOT.2014.2318835 (cit. on p. 50).

[133] J. Perno and C. W. Probst. "Behavioural Profiling in Cyber-Social Systems". In: *Human Aspects of Information Security, Privacy and Trust*. Ed. by T. Tryfonas. Cham: Springer International Publishing, 2017, pp. 507–517. ISBN: 978-3-319-58460-7 (cit. on pp. 51, 54, 62).

[134] E. Griffor et al. *Framework for Cyber-Physical Systems: Volume 1, Overview*. en. June 2017. DOI: b10.6028/NIST.SP.1500-201 (cit. on pp. 51, 53, 62).

[135] J. S. Dahmann. "Systems of systems characterization and types". In: *Systems of Systems Engineering for NATO Defence Applications (STO-EN-SCI-276)* (2015), pp. 1–14 (cit. on p. 51).

[136] S. Pasandideh, P. Pereira, and L. Gomes. “Cyber-Physical-Social Systems: Taxonomy, Challenges, and Opportunities”. In: *IEEE Access* 10 (2022), pp. 42404–42419. DOI: 10.1109/ACCESS.2022.3167441 (cit. on p. 51).

[137] L. Yan, M. Katherine, and F. Simon. *Current Standards Landscape for Smart Manufacturing Systems*. en. Feb. 2016. DOI: 10.6028/NIST.IR.8107 (cit. on p. 53).

[138] F. Kolini and L. J. Janczewski. “Cyber Defense Capability Model: A Foundation Taxonomy”. In: *CONF-IRM*. 2015, p. 32 (cit. on p. 53).

[139] S. M. M. Rahman. “Cyber-physical-social system between a humanoid robot and a virtual human through a shared platform for adaptive agent ecology”. In: *IEEE/CAA Journal of Automatica Sinica* 5.1 (2018), pp. 190–203. DOI: 10.1109/JAS.2017.7510760 (cit. on p. 54).

[140] L. Nisiotis, L. Alboul, and M. Beer. “A Prototype that Fuses Virtual Reality, Robots, and Social Networks to Create a New Cyber–Physical–Social Eco-Society System for Cultural Heritage”. In: *Sustainability* 12.2 (Jan. 2020), p. 645. ISSN: 2071-1050. DOI: 10.3390/su12020645. URL: http://dx.doi.org/10.3390/su12020645 (cit. on pp. 54, 55).

[141] P. Jiang, K. Ding, and J. Leng. “Towards a cyber-physical-social-connected and service-oriented manufacturing paradigm: Social Manufacturing”. In: *Manufacturing Letters* 7 (2016), pp. 15–21. ISSN: 2213-8463. DOI: 10.1016/j.mfglet.2015.12.002. URL: https://www.sciencedirect.com/science/article/pii/S221384631500022X (cit. on pp. 54, 55).

[142] *68% of the world population projected to live in urban areas by 2050, says UN*. Last accessed 20 September 2021. 2018. URL: https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html (cit. on p. 54).

[143] Y. Yoshihito et al. “Hitachi’s Vision of the Smart City”. In: *Hitachi Review* 61.3 (2012), pp. 111–118 (cit. on p. 54).

[144] M. Angelidou. “Smart cities: A conjuncture of four forces”. In: *Cities* 47 (2015). Current Research on Cities (CRoC), pp. 95–106. ISSN: 0264-2751. DOI: 10.1016/j.cities.2015.05.004. URL: https://www.sciencedirect.com/science/article/pii/S0264275115000633 (cit. on p. 54).

[145] A. Puliafito et al. “Smart Cities of the Future as Cyber Physical Systems: Challenges and Enabling Technologies”. In: *Sensors* 21.10 (May 2021), p. 3349. ISSN: 1424-8220. DOI: 10.3390/s21103349. URL: http://dx.doi.org/10.3390/s21103349 (cit. on p. 54).

[146] N. Mitton et al. "Combining Cloud and sensors in a smart city environment". In: *EURASIP Journal on Wireless Communications and Networking* 2012.1 (2012), p. 247. DOI: 10.1186/1687-1499-2012-247. URL: https://hal.inria.fr/hal-00784397 (cit. on p. 54).

[147] J. Stübinger and L. Schneider. "Understanding Smart City—A Data-Driven Literature Review". In: *Sustainability* 12.20 (Oct. 2020), p. 8460. ISSN: 2071-1050. DOI: 10.3390/su12208460. URL: http://dx.doi.org/10.3390/su12208460 (cit. on p. 55).

[148] M. J. Kim, M. E. Cho, and H. J. Jun. "Developing Design Solutions for Smart Homes Through User-Centered Scenarios". In: *Frontiers in Psychology* 11 (2020), p. 335. ISSN: 1664-1078. DOI: 10.3389/fpsyg.2020.00335. URL: https://www.frontiersin.org/article/10.3389/fpsyg.2020.00335 (cit. on p. 55).

[149] K. Boes, D. Buhalis, and A. Inversini. "Conceptualising smart tourism destination dimensions". In: *Information and communication technologies in tourism 2015*. Springer, 2015, pp. 391–403 (cit. on p. 55).

[150] S. Tian et al. "Smart healthcare: making medical care more intelligent". In: *Global Health Journal* 3.3 (2019), pp. 62–65. ISSN: 2414-6447. DOI: 10.1016/j.glohj.2019.07.001. URL: https://www.sciencedirect.com/science/article/pii/S2414644719300508 (cit. on p. 56).

[151] T. Poongodi et al. "IoT Sensing Capabilities: Sensor Deployment and Node Discovery, Wearable Sensors, Wireless Body Area Network (WBAN), Data Acquisition". In: *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*. Springer International Publishing, 2020, pp. 127–151. ISBN: 978-3-030-33596-0. DOI: 10.1007/978-3-030-33596-0_5. URL: https://doi.org/10.1007/978-3-030-33596-0_5 (cit. on pp. 56, 62).

[152] Y. Zhang et al. "Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data". In: *IEEE Systems Journal* 11.1 (2017), pp. 88–95. DOI: 10.1109/JSYST.2015.2460747 (cit. on p. 56).

[153] S. A. Haque, S. M. Aziz, and M. Rahman. "Review of Cyber-Physical System in Healthcare". In: *International Journal of Distributed Sensor Networks* 10.4 (2014), p. 217415. DOI: 10.1155/2014/217415. URL: https://doi.org/10.1155/2014/217415 (cit. on p. 56).

[154] Y. Xue and X. Yu. "Beyond smart grid—cyber–physical–social system in energy future (point of view)". In: *Proceedings of the IEEE* 105.12 (2017), pp. 2290–2292. DOI: 10.1109/JPROC.2017.2768698 (cit. on pp. 56, 62).

[155] S. A. Camtepe and B. Yener. "Modeling and detection of complex attacks". In: *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*. IEEE. 2007, pp. 234–243 (cit. on p. 56).

[156] N. Gati et al. "Differentially private data fusion and deep learning Framework for Cyber–Physical–Social Systems: State-of-the-art and perspectives". In: *Information Fusion* 76 (Dec. 2021), pp. 298–314. DOI: 10.1016/j.inffus.2021.04.017 (cit. on pp. 56, 57, 62).

[157] T. Sharma, J. C. Bambenek, and M. Bashir. "Preserving privacy in cyber-physical-social systems: An anonymity and access control approach". In: *Proceedings of the 1st Workshop on Cyber-Physical Social Systems*. ceur-ws, 2020 (cit. on p. 56).

[158] X. Zheng et al. "Follow But No Track: Privacy Preserved Profile Publishing in Cyber-Physical Social Systems". In: *IEEE Internet of Things Journal* PP (Mar. 2017), pp. 1–1. DOI: 10.1109/JIOT.2017.2679483 (cit. on p. 56).

[159] D. Blazquez and J. Domenech. "Big Data sources and methods for social and economic analyses". In: *Technological Forecasting and Social Change* 130 (2018), pp. 99–113 (cit. on p. 57).

[160] R. K. Ganti, F. Ye, and H. Lei. "Mobile crowdsensing: current state and future challenges". In: *IEEE Communications Magazine* 49.11 (2011), pp. 32–39. DOI: 10.1109/MCOM.2011.6069707 (cit. on p. 57).

[161] J. Ai and A. A. Abouzeid. "Coverage by directional sensors in randomly deployed wireless sensor networks". In: *Journal of Combinatorial Optimization* 11.1 (2006), pp. 21–41 (cit. on p. 57).

[162] S. Zhang et al. "A tensor-network-based big data fusion framework for Cyber–Physical–Social Systems (CPSS)". In: *Information Fusion* 76 (2021), pp. 337–354. ISSN: 1566-2535. DOI: 10.1016/j.inffus.2021.05.014. URL: https://www.sciencedirect.com/science/article/pii/S1566253521001147 (cit. on pp. 57, 62).

[163] M. J. Hall, C. Hall, and T. Tate. "Removing the HCI Bottleneck: How the Human-Computer Interface (HCI) Affects the Performance of Data Fusion Systems". In: vol. 2. 2001, pp. 89–104 (cit. on p. 58).

[164] X. Chen. "Chapter 2 - Point coverage analysis". In: *Randomly Deployed Wireless Sensor Networks*. Ed. by X. Chen. Elsevier, 2020, pp. 15–33. ISBN: 978-0-12-819624-3. DOI: 10.1016/B978-0-12-819624-3.00007-0. URL: https://www.sciencedirect.com/science/article/pii/B9780128196243000070 (cit. on p. 58).

[165] V. Moysiadis et al. "Smart Farming in Europe". In: *Computer Science Review* 39 (2021), p. 100345. ISSN: 1574-0137. DOI: 10.1016/j.cosrev.2020.100345. URL: https://www.sciencedirect.com/science/article/pii/S1574013720304457 (cit. on p. 58).

[166] A. A. Nazarenko and G. A. Safdar. "Survey on security and privacy issues in cyber physical systems". In: *AIMS Electronics and Electrical Engineering* 3.2 (2019), pp. 111–143. DOI: 10.3934/ElectrEng.2019.2.111 (cit. on p. 58).

[167] J. Yli-Huumo et al. “Where Is Current Research on Blockchain Technology?—A Systematic Review”. In: *Plos One* 11.10 (2016). DOI: 10.1371/journal.pone.0163477 (cit. on p. 58).

[168] G. Cabour, É. Ledoux, and S. Bassetto. *A Work-Centered Approach for Cyber-Physical-Social System Design: Applications in Aerospace Industrial Inspection*. 2021. arXiv: 2101.05385 (cit. on p. 59).

[169] B. Liu et al. “A survey of model-driven techniques and tools for cyber-physical systems”. In: *Frontiers of Information Technology & Electronic Engineering* 21.11 (2020), pp. 1567–1590 (cit. on p. 59).

[170] C. V. Lozano and K. K. Vijayan. “Literature review on Cyber Physical Systems Design”. In: *Procedia Manufacturing* 45 (2020). Learning Factories across the value chain – from innovation to service – The 10th Conference on Learning Factories 2020, pp. 295–300. ISSN: 2351-9789. DOI: 10.1016/j.promfg.2020.04.020. URL: https://www.sciencedirect.com/science/article/pii/S2351978920310581 (cit. on p. 59).

[171] S. Wang et al. “Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach”. In: *IEEE Transactions on Computational Social Systems* 5.4 (2018), pp. 942–950. DOI: 10.1109/TCSS.2018.2865526 (cit. on p. 59).

[172] *How important is your cyber security?* Oct. 2017. URL: https://theect.org/importance-cyber-security/. (cit. on p. 59).

[173] URL: https://www.schneier.com/crypto-gram/archives/2000/1015.html#1 (cit. on p. 59).

[174] A. Humayed et al. “Cyber-physical systems security—A survey”. In: *IEEE Internet of Things Journal* 4.6 (2017), pp. 1802–1831 (cit. on p. 60).

[175] D. Lupton. “The Internet of Things: Social dimensions”. In: *Sociology Compass* 14.4 (2020). DOI: 10.1111/soc4.12770 (cit. on p. 62).

[176] L. Cheng et al. “Parallel Cyber-Physical-Social Systems Based Smart Energy Robotic Dispatcher and Knowledge Automation: Concepts, Architectures, and Challenges”. In: *IEEE Intelligent Systems* 34.2 (2019), pp. 54–64. DOI: 10.1109/MIS.2018.2882360 (cit. on p. 62).

[177] W. Li et al. “Multi-Objective Optimization for Cyber-Physical-Social Systems: A Case Study of Electric Vehicles Charging and Discharging”. In: *IEEE Access* 7 (2019), pp. 76754–76767. DOI: 10.1109/ACCESS.2019.2921716 (cit. on p. 62).

[178] Y. Qu et al. “A Hybrid Privacy Protection Scheme in Cyber-Physical Social Networks”. In: *IEEE Transactions on Computational Social Systems* 5.3 (2018), pp. 773–784. DOI: 10.1109/TCSS.2018.2861775 (cit. on p. 62).

[179] M. Hussein. “Transition to Web 3.0: E-Learning 3.0 opportunities and challenges”. In: *EELU 2014 EELU INTERNATIONAL CONFERENCE ON E-LEARNING*. June 2014 (cit. on p. 62).

[180] D. Janssen et al. “Virtual Environments in Higher Education – Immersion as a Key Construct for Learning 4.0”. In: *International Journal of Advanced Corporate Learning (iJAC)* 9.2 (2016), p. 20. DOI: 10.3991/ijac.v9i2.6000 (cit. on p. 62).

[181] F. J. García-Peñalvo, Á. Fidalgo-Blanco, and M. L. Sein-Echaluce. “An adaptive hybrid MOOC model: Disrupting the MOOC concept in higher education”. In: *Telematics and Informatics* 35.4 (2018), pp. 1018–1030. ISSN: 0736-5853. DOI: 10.1016/j.tele.2017.09.012. URL: https://www.sciencedirect.com/science/article/pii/S0736585317303453 (cit. on p. 62).

[182] J. Predd et al. “Insiders behaving badly”. In: *IEEE Security & Privacy* 6.4 (2008), pp. 66–70 (cit. on p. 62).

[183] S. L. Pfleeger and D. D. Caputo. “Leveraging behavioral science to mitigate cyber security risk”. In: *Computers Security* 31.4 (2012), pp. 597–611. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2011.12.010. URL: https://www.sciencedirect.com/science/article/pii/S0167404811001659 (cit. on p. 62).

[184] M. A. Sasse and I. Flechais. “Usable Security: Why Do We Need It? How Do We Get It?” In: 2005 (cit. on p. 63).

[185] M. Endsley. “Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), 32-64”. In: *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37 (Mar. 1995), pp. 32–64. DOI: 10.1518/001872095779049543 (cit. on p. 63).

[186] L. M. Almutairi and S. Shetty. “Generalized stochastic Petri net model based security risk assessment of software defined networks”. In: *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*. IEEE. 2017, pp. 545–550 (cit. on p. 67).

[187] M. Wu et al. “Establishment of intrusion detection testbed for CyberManufacturing systems”. In: *Procedia Manufacturing* 26 (2018), pp. 1053–1064 (cit. on p. 70).

[188] S. Mauw and M. Oostdijk. “Foundations of Attack Trees”. In: *Information Security and Cryptology - ICISC 2005*. Ed. by D. H. Won and S. Kim. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 186–198. ISBN: 978-3-540-33355-5 (cit. on p. 73).

[189] B. Kordy et al. “Attack-defense trees”. In: *Journal of Logic and Computation* 24 (Feb. 2014). DOI: 10.1093/logcom/exs029 (cit. on p. 73).

[190] A. Roy, D. S. Kim, and K. S. Trivedi. “Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees”. In: *Security and Communication Networks* 5.8 (2012), pp. 929–943 (cit. on p. 73).

[191] S. Pasandideh, P. Pereira, and L. Gomes. “Attack Tree Refinements Analysis and Verification by Applying Coloured Petri Nets”. In: IECON´22. IEEE, 2022 (cit. on p. 74).

[192] E. Ukwandu et al. “A Review of Cyber-Ranges and Test-Beds: Current and Future Trends”. In: *Sensors* 20.24 (2020). ISSN: 1424-8220. DOI: 10.3390/s20247148. URL: https://www.mdpi.com/1424-8220/20/24/7148 (cit. on p. 83).

[193] B. Foo et al. “ADEPTS: adaptive intrusion response using attack graphs in an e-commerce environment”. In: *2005 International Conference on Dependable Systems and Networks (DSN’05)*. 2005, pp. 508–517. DOI: 10.1109/DSN.2005.17 (cit. on p. 84).

[194] S. Hamilton and W. Hamilton. “Adversary Modeling and Simulation in Cyber Warfare”. In: vol. 278. Sept. 2008. ISBN: 978-0-387-09698-8. DOI: 10.1007/978-0-387-09699-5_30 (cit. on p. 85).

[195] F. Pereira, F. Moutinho, and L. Gomes. “IOPT-tools — Towards cloud design automation of digital controllers with Petri nets”. In: *2014 International Conference on Mechatronics and Control (ICMC)*. 2014, pp. 2414–2419. DOI: 10.1109/ICMC.2014.7232002 (cit. on p. 86).

[196] G. Carl et al. “Denial-of-service attack-detection techniques”. In: *IEEE Internet Computing* 10.1 (2006), pp. 82–89. DOI: 10.1109/MIC.2006.5 (cit. on p. 90).

[197] C. P. Suryawanshi. *Playbook for DDOS Security Response*. May 2017. URL: https://www.cisoplatform.com/profiles/blogs/response-strategy-for-ddos (cit. on p. 90).

[198] D. Rountree. “3 - Network Security”. In: *Security for Microsoft Windows System Administrators*. Ed. by D. Rountree. Boston: Syngress, 2011, pp. 71–107. ISBN: 978-1-59749-594-3. DOI: https://doi.org/10.1016/B978-1-59749-594-3.00003-X. URL: https://www.sciencedirect.com/science/article/pii/B978159749594300003X (cit. on p. 101).

[199] A. Shameli-Sendi et al. “Intrusion response systems: survey and taxonomy”. In: *Int. J. Comput. Sci. Netw. Secur* 12.1 (2012), pp. 1–14 (cit. on p. 104).

[200] L. F. Cómbita et al. “Response and reconfiguration of cyber-physical control systems: A survey”. In: *2015 IEEE 2nd Colombian Conference on Automatic Control (CCAC)*. IEEE. 2015, pp. 1–6 (cit. on p. 104).

[201] G. N. Ericsson. “Cyber security and power system communication—essential parts of a smart grid infrastructure”. In: *IEEE Transactions on Power delivery* 25.3 (2010), pp. 1501–1507 (cit. on p. 105).

[202] L. Phiri and S. Tembo. *Petri Net-Based (PN) Cyber Risk Assessment and Modeling for Zambian Smart Grid (SG) ICS and SCADA Systems*. Jan. 2022. DOI: 10.5923/j.computer.20221201.01 (cit. on p. 105).

[203] L. Kallab et al. “Using colored Petri nets for verifying restful service composition”. In: *OTM Confederated International Conferences"On the Move to Meaningful Internet Systems"*. Springer. 2017, pp. 505–523 (cit. on p. 105).

A

The Home Lab Design and system logs

Architectures plays a critical role in the design, evaluation, and analysis of complex systems (e.g., System of Systems). Consequently, the first phase of any system's development is the architecture design. The second phase, after the design of the architecture, is the evaluation and analysis phase. Based on the development design paradigm used, e.g., spiral method, these two phases may repeat for some iterations. However, adherence to the original requirements requires a rigorous methodology for both design and evaluation. The design phase usually relies on modeling languages such as the Unified Modeling Language (UML), the System Modeling Language (SysML), and many others. The evaluation phase is mainly based on executable models based on Petri Nets and their analysis capabilities such as Computational Tree Logic (CTL) for State Space Analysis (SSA). The SSA could be used to investigate the properties of the design such as potential deadlocks, reachability, and so forth. As a result of these analyses, the architecture could be further enhanced. This appendix presents the architecture design process used in this work. In addition, the evaluation method with which the architecture is evaluated is elaborated.

A.0.1 Design the Architecture

The applied technologies to build the lab are described in Figure A.1.

Figure A.2 shows the architecture of the home lab.

A.0.2 system logs: results

In Figure. A.3 a result of scanning vulnerable ports by Nmap is provided. This is an example to show what type of information is provided by Nmap.

Here is the result of the simulation in the TCPN model for DoS (scenario 2 in Chapter 7). The simulation is done for all the scenarios that the summary and description of the results are provided in section 7.6.

1 0.0 C @ (1:High$_{l}evel$)
$-pa1 = Y$
$-pa2 = N$
$-pa3 = N$

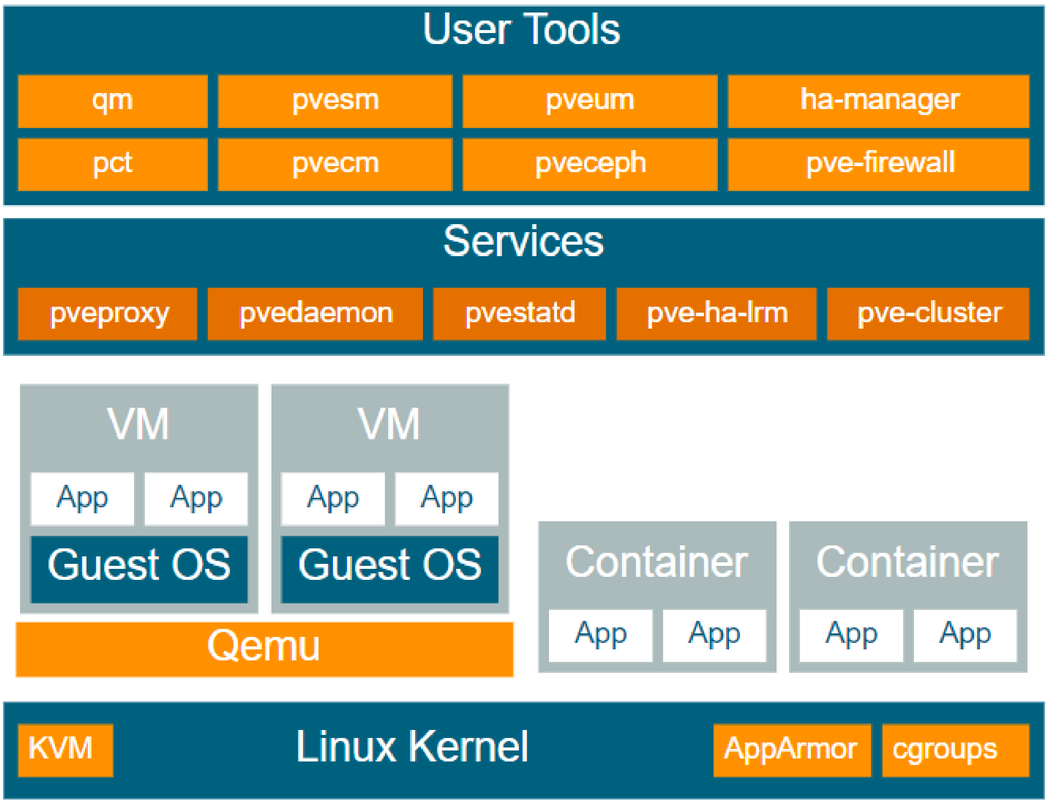


Figure A.1: Proxmox Architecture

$20.0creat_{p}assword@(1:High_{l}evel)$

$-aut1=("uf","pf")$

$30.0send_{e}mail@(1:High_{l}evel)$

$-mc="SQLcode"$

$-em="Emergencyhelpisneeded"$

$40.0Use_{s}ys_{v}ulnearbities@(1:High_{l}evel)$

$-hs=("88.80.186.144","192.168.140.34",TCP6,https,46978,443)$

$-d1="CVE-2014-0346"$

$50.0Use_{A}utomated_{t}ool@(1:High_{l}evel)$

$-hs=("101.0.4.62","192.168.140.21",TCP6,http,33250,80)$

$-d1="CVE-2020-26728"$

$60.0Use_{s}ys_{v}ulnearbities@(1:High_{l}evel)$

$-hs=("88.80.186.144","192.168.56.72",TCP6,https,41816,443)$

$-d1="CVE-2014-0346"$

$70.0C@(1:High_{l}evel)$

$-pa1=N$

$-pa2=Y$

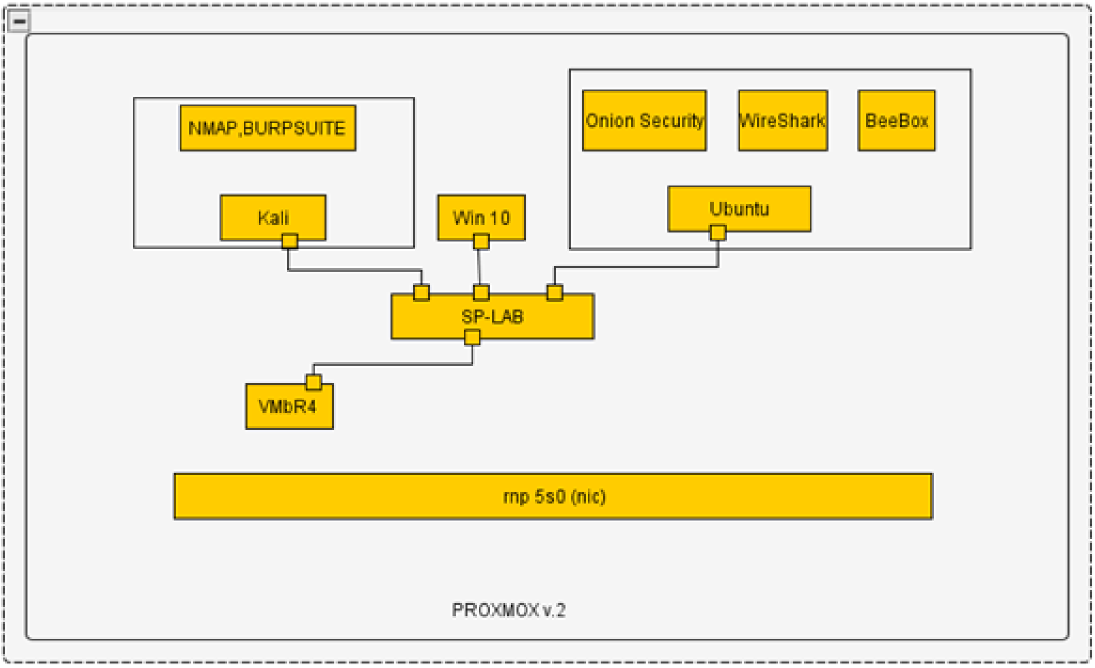
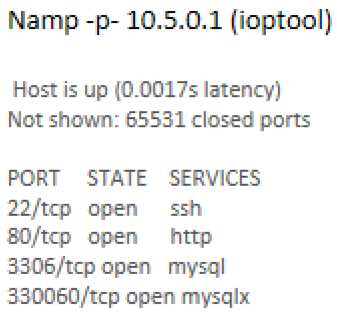


Figure A.2: The isolated home lab diagram



```
Namp -p- 10.5.0.1 (ioptool)

 Host is up (0.0017s latency)
Not shown: 65531 closed ports

PORT     STATE   SERVICES
22/tcp   open    ssh
80/tcp   open    http
3306/tcp open   mysql
330060/tcp open mysqlx
```

Figure A.3: A sample of Scanning Vulnerable Port in the System of Interest

$-pa3 = Y$

$80.0authentication@(1 : High_level)$

$-aut1 = (''uf'', ''pf'')$

$90.0Recivemalicious_email@(1 : High_level)$

$-me = (''Emergencyhelpisneeded'', ''SQLcode'')$

$100.0PST_payload2@(1 : High_level)$

$-hs = (''101.0.4.62'', ''192.168.140.21'', TCP6, http, 33250, 80)$

$-d1 = ''CVE-2020-26728''$

$110.0notpass@(1 : High_level)$

$-e = Yes$

$-hs = (''101.0.4.62'', ''192.168.140.21'', TCP6, http, 33250, 80)$

$- d1 = ”CVE - 2020 - 26728”$

$120.0Check_{t}he_{D}B@(1 : High_{l}evel)$

$- aut1 = (”uf”, ”pf”)$

$- aut = (”u2”, ”p2”)$

$130.0Introdur_{A}ccess@(1 : High_{l}evel)$

$- pa = N$

$- me = (”Emergencyhelpisneeded”, ”SQLcode”)$

$140.0Access_{C}R@(1 : High_{l}evel)$

$- aut1 = (”u2”, ”p2”)$

$- me = (”Emergencyhelpisneeded”, ”SQLcode”)$

$- pa = N$

$150.0Payload3@(1 : High_{l}evel)$

$- hs = (”88.80.186.144”, ”192.168.140.34”, TCP6, https, 46978, 443)$

$- d1 = ”CVE - 2014 - 0346”$

$160.0Payload3@(1 : High_{l}evel)$

$- hs = (”88.80.186.144”, ”192.168.56.72”, TCP6, https, 41816, 443)$

$- d1 = ”CVE - 2014 - 0346”$

$170.0Check_{t}he_{D}B@(1 : High_{l}evel)$

$- aut1 = (”u2”, ”p2”)$

$- aut = (”u1”, ”p1”)$

$180.0pass@(1 : High_{l}evel)$

$- e = No$

$- hs = (”88.80.186.144”, ”192.168.140.34”, TCP6, https, 46978, 443)$

$- d1 = ”CVE - 2014 - 0346”$

$190.0notpass@(1 : High_{l}evel)$

$- e = Yes$

$- hs = (”88.80.186.144”, ”192.168.56.72”, TCP6, https, 41816, 443)$

$- d1 = ”CVE - 2014 - 0346”$

$200.0T1ids@(1 : IPS)$

$- hs = (”88.80.186.144”, ”192.168.140.34”, TCP6, https, 46978, 443)$

$- d1 = ”CVE - 2014 - 0346”$

$210.0T2ids@(1 : IPS)$

$- hs = (”88.80.186.144”, ”192.168.140.34”, TCP6, https, 46978, 443)$

$- d1 = ”CVE - 2014 - 0346”$

$- refr = ”CVE - 2021 - 44228”$

$220.0packetallow@(1 : IPS)$

$- ipsact = Allow$

$- ipsm = ”healthy”$

$230.0Healthypackpass@(1 : IPS)$

$- ipsm = ”healthy”$

$- ipsact = Allow$

$-hs = (''88.80.186.144'', ''192.168.140.34'', TCP6, https, 46978, 443)$

$-d1 = ''CVE - 2014 - 0346''$

$240.0T4ids@(1 : IPS)$

$-hs = (''88.80.186.144'', ''192.168.140.34'', TCP6, https, 46978, 443)$

$-ipsm = ''healthy''$

$-d1 = ''CVE - 2014 - 0346''$

$-ipsact = Allow$

$250.0Generate_N o_A lert@(1 : High_l evel)$

$-hs = (''88.80.186.144'', ''192.168.140.34'', TCP6, https, 46978, 443)$

$-ipsm = ''healthy''$

$-d1 = ''CVE - 2014 - 0346''$

$-ipsact = Allow$

$260.0Pass_t o_W Eb_s erver@(1 : High_l evel)$

$-hs = (''88.80.186.144'', ''192.168.140.34'', TCP6, https, 46978, 443)$

$-d1 = ''CVE - 2014 - 0346''$

$270.0arbirity_c ode_e xecuted@(1 : High_l evel)$

$-hs = (''88.80.186.144'', ''192.168.140.34'', TCP6, https, 46978, 443)$

$-d1 = ''CVE - 2014 - 0346''$

$280.0Execute_C rontab_c ommand@(1 : High_l evel)$

$-d2 = ''CVE - 2014 - 0346''$

$-hd = (''88.80.186.144'', ''192.168.140.34'', TCP6, https, 46978, 443)$

$290.0Send_t he_s everal_p ackets@(1 : High_l evel)$

$-hs = (''88.80.186.144'', ''192.168.140.34'', TCP6, https, 46978, 443)$

$-d1 = ''CVE - 2014 - 0346''$

$-n = 1$

$300.0Generate_a nother_p aket@(1 : High_l evel)$

$-n = 1$

$-hs = (''88.80.186.144'', ''192.168.140.34'', TCP6, https, 46978, 443)$

$-d1 = ''CVE - 2014 - 0346''$

$310.0Send_t he_s everal_p ackets@(1 : High_l evel)$

$-hs = (''88.80.186.144'', ''192.168.140.34'', TCP6, https, 46978, 443)$

$-d1 = ''CVE - 2014 - 0346''$

$-n = 2$

$320.0Admintakeanaction@(1 : High_l evel)$

$-r = ''Shoutdownthesystems''$

$-n = 2$

$-hs = (''88.80.186.144'', ''192.168.140.34'', TCP6, https, 46978, 443)$

$-d1 = ''CVE - 2014 - 0346''$

$-d2 = ''Flooding/Dosattack''$

$330.0Shoutdown@(1 : High_l evel)$

$-r = ''Shoutdownthesystems''$

B

The Computing node

B.0.1

CPN Tools simulation report for quantitative analysis of attack and defense cost based on Figure.5.9. The computation is done by CPN Tools.

```
1 0.0 A21221 @ (1:computing)
- c = 30
- a = a21221
2 0.0 Detected1 @ (1:computing)
- d = d12
- c = 100
- success = true
3 0.0 A2112 @ (1:computing)
- c = 0
- a = a2112
4 0.0 A2141 @ (1:computing)
- c = 25
- a = a2141
5 0.0 A2122 @ (1:computing)
- c = 30
- a = a21221
6 0.0 Mitigated1 @ (1:computing)
- m = m12
- cm = 25
- success = true
7 0.0 A31 @ (1:computing)
- c = 30
- a = a31
8 0.0 Mitigated @ (1:computing)
- m = m412
- cm = 70
- success = true
9 0.0 A11 @ (1:computing)
- c = 50
- a = a11
10 0.0 A4121 @ (1:computing)
- c = 40
- a = a4121
11 0.0 A32 @ (1:computing)
- c = 15
- a = a32
12 0.0 A213 @ (1:computing)
- c = 15
- a = a213
13 0.0 ndetected @ (1:computing)
- d = d412
- c = 0
- fail = true
14 0.0 A3 @ (1:computing)
- c = 30
- a = a31
- b = a32
- cn = 15
15 0.0 A411 @ (1:computing)
- c = 0
- a = a411
16 0.0 A1 @ (1:computing)
- c = 50
- a = a11
17 0.0 DFailure @ (1:computing)
- d = d412
- c = 0
- m = m412
- cm = 70
18 0.0 Mitigated @ (1:computing) - m = m412
- cm = 70
- success = true
19 0.0 A2142 @ (1:computing)
- c = 25
- a = a2142
20 0.0 A2121 @ (1:computing)
- c = 20
- a = a2121
21 0.0 stopA12 @ (1:computing)
- m = m12
- cm = 25
- d = d12
- c = 100
22 0.0 A412 @ (1:computing)
- c = 40
- a = a4121
23 0.0 Detected @ (1:computing)
- d = d412
- c = 0
- success = true
24 0.0 a412pass @ (1:computing)
- c = 40
- a = a4121
- m = d412
- cm = 70
25 0.0 A41 @ (1:computing)
- c = 0
- a = a411
26 0.0 CMP212 @ (1:computing)
- c = 30
- b = a2121
- a = a21221
- cn = 20
27 0.0 CMPas @ (1:computing)
- c = 50
- b = a3
- a = a11
- cn = 45
28 0.0 A21 @ (1:computing)
- c = 15
- a = a213
29 0.0 A211 @ (1:computing)
- c = 0
- a = a2112
30 0.0 A4 @ (1:computing)
- c = 0
- a = a411
31 0.0 A21222 @ (1:computing)
```

```
- c = 10
- a = a21222
32 0.0 A12 @ (1:computing)
- c = 60
- a = a12
33 0.0 CMPas @ (1:computing)
- c = 0
- b = sa
- a = a411
- cn = 95
34 0.0 A214 @ (1:computing)
- c = 25
- a = a2142
35 0.0 A4122 @ (1:computing)
- c = 40
- a = a4122
36 0.0 A21 @ (1:computing)
- c = 0
- a = a2112
37 0.0 A2111 @ (1:computing)
- c = 0
- a = a2111
38 0.0 stop412 @ (1:computing)
- m = m412
- cm = 70
- d = d412
- c = 0
39 0.0 A2143 @ (1:computing)
- c = 50
- a = a2143
40 0.0 A413 @ (1:computing)
- c = 5
- a = a413
41 0.0 A21 @ (1:computing)
- c = 25
- a = a2142
42 0.0 A41 @ (1:computing)
- c = 5
- a = a413
43 0.0 A212 @ (1:computing)
- c = 50
- a = a212
44 0.0 A2 @ (1:computing)
- c = 15
- a = a213
45 0.0 A21 @ (1:computing)
- c = 50
- a = a212
46 0.0 A2122 @ (1:computing)
- c = 10
- a = a21222
47 0.0 A4 @ (1:computing)
- c = 5
- a = a413
48 0.0 A214 @ (1:computing)
- c = 50
- a = a2143
49 0.0 CMPas @ (1:computing)
- c = 5
- b = sa
- a = a413
- cn = 95
50 0.0 CMPas @ (1:computing)
- c = 15
- b = sa
- a = a213
- cn = 100
51 0.0 A4 @ (1:computing)
- c = 40
- a = a412
52 0.0 A211 @ (1:computing)
- c = 0
- a = a2111
53 0.0 A2 @ (1:computing)
- c = 50
- a = a212
54 0.0 A21 @ (1:computing)
- c = 50
- a = a2143
55 0.0 CMPas @ (1:computing)
- c = 115
- b = a212
- a = sa
- cn = 50
56 0.0 A2 @ (1:computing)
- c = 0
- a = a2112
57 0.0 CMPas @ (1:computing)
- c = 0
- b = a412
- a = a2112
- cn = 40
58 0.0 A21 @ (1:computing)
- c = 0
- a = a2111
59 0.0 A412 @ (1:computing)
- c = 40
- a = a4122
60 0.0 A2 @ (1:computing)
- c = 50
- a = a2143
61 0.0 CMPas @ (1:computing)
- c = 165
- b = sa
- a = sa
- cn = 40
62 0.0 CMPas @ (1:computing)
- c = 205
- b = a2143
- a = sa
- cn = 50
63 0.0 A2 @ (1:computing)
- c = 0
- a = a2111
64 0.0 A212 @ (1:computing)
- c = 10
- a = a21222
65 0.0 CMPas @ (1:computing)
- c = 0
- b = sa
- a = a2111
- cn = 255
66 0.0 A2 @ (1:computing)
```

```
- c = 25
- a = a2142
67 0.0 CMPas @ (1:computing)
- c = 255
- b = a2142
- a = sa
- cn = 25
68 0.0 A214 @ (1:computing)
- c = 25
- a = a2141
69 0.0 CMP21 @ (1:computing)
- c = 10
- b = a2141
- a = a21222
- cn = 25
70 0.0 A21 @ (1:computing)
- c = 35
- a = a21
71 0.0 A2 @ (1:computing)
- c = 35
- a = a21
72 0.0 CMPas @ (1:computing)
- c = 280
- b = a21
- a = sa
- cn = 35
```