UNIVERSITY OF BIRMINGHAM

RELIABILITY IN A SMART POWER SYSTEM WITH CYBER-PHYSICAL INTERACTIVE OPERATION OF PHOTOVOLTAIC SYSTEMS AND HEAT PUMPS

by

HASAN GUNDUZ

A thesis submitted to the University of Birmingham for the degree of

DOCTOR OF PHILOSOPHY

Department of Electronic, Electrical and Systems Engineering

College of Engineering and Physical Sciences

The University of Birmingham

May 2019

University of Birmingham Research Archive

e-theses repository

This unpublished thesis/dissertation is copyright of the author and/or third parties. The intellectual property rights of the author or third parties in respect of this work are as defined by The Copyright Designs and Patents Act 1988 or as modified by any successor legislation.

Any use made of information contained in this thesis/dissertation must be in accordance with that legislation and must be properly acknowledged. Further distribution or reproduction in any format is prohibited without the permission of the copyright holder.

Acknowledgements

I would like to express my sincere appreciation to my supervisor Dr. Dilan Jayaweera for his valuable advice, patience, and support during my PhD project. His encouragement on critical thinking helped me to understand my research project merits. Without his limitless guidance, and vision, my project cannot be accomplished.

I would also like to thank my colleagues from the Power and Control Group for their suggestions and helps during research period. Working with them has been a great experience for me.

Last but not the least, I would like to thank my beloved parents and siblings. Thank you so much for your love and limitless support throughout my whole study period.

Abstract

The connectivity of the power grid is increasing with the internet of things, and low carbon technologies being deployed to help enhance smart grid performance and reliability. Meanwhile, they also increase the digital complexity and dependency of cyber assets, which might be vulnerable to cyber-physical threats, and hence may impact the reliability of power systems. Due to cyber-threats' unpredictable nature, the interactive operation of low carbon technologies with cyber-physical systems is becoming a challenging task for smart grids. This thesis proposes novel mathematical frameworks to estimate the availability of photovoltaics and heat pumps with cyber-physical components. These frameworks are developed to quantify the level of risk posed by cyber-threats to the interactive operation of photovoltaics and heat pumps, using Markov-Chains. The availability framework considers the severity of random cyber-attacks on photovoltaics and the probability of cyber-threats with mean time to detection-time on heat pump operation. Sensitivities of the repair times of cyber-physical component for photovoltaics and sensitivities of cyber-attack-detection time for heat pumps are also evaluated. The impact of cyber threats on the interactive operation of photovoltaics and heat pumps are considerable and inconsistent, however the propagation of cyber-threats can be restricted by appropriate means of photovoltaics. For heat pumps, operational reliability substantially decreases due to the unavailability of their control panel. Contributions of this thesis include an availability model for photovoltaic configurations, an innovative approach to assess the reliability of a photovoltaic integrated power system with cyber-physical interactions, the availability estimation of heat pump with variable detection time, and an enhanced cyber-intrusion process model for reliability analysis of heat pumps. The findings offer insight into the impact of cyber-physical system availability and its importance on power system reliability.

Table of Contents

Chapter 1: Introduction 1

1.1 Status Quo of Power Systems 1

1.2 Status Quo of Low Carbon Technologies and ICT 4

1.3 Motivation and the Scope of the Research 7

1.4 Aim and Objectives 8

1.5 Contributions of the Thesis 8

1.6 Outline of the Thesis 9

Chapter 2: Literature Review 12

2.1 Introduction 12

2.2 Reliability Assessment of Engineering Applications 13

2.2.1 General Concept of Reliability in Engineering Systems 13
2.2.2 Reliability and Availability 14
2.2.3 Overview of Reliability Techniques in Engineering Systems 15

2.3 Reliability Assessment in Power Systems 22

2.3.1 Power System Reliability 22
2.3.2 Hierarchical Levels of Power Grid 24
2.3.3 Overview of Power System Reliability Studies 25

2.4 Power System Reliability Considering Low-Carbon Technologies 27

2.4.1 Electric Heat Pumps 28
2.4.2 Photovoltaic (PV) Powered Generation Systems 32

2.5 Power System Reliability Considering Information and Communication Technologies 36

2.6 Summary 42

Chapter 3: Power System Reliability Analysis without Cyber-Physical System Integration 43

3.1 Introduction 43

3.2 Load and Generation Profile Modelling 44

3.2.1 Load Modelling 44
3.2.2 PV Generation Modelling 47

3.3 Methodology for Power System Reliability Assessment without Considering Cyber-physical System Integration 50

3.3.1 The Procedure of Power System Reliability Assessment 51

3.4 Case Studies and Analysis 52

3.4.1 Case Study 1: Impact of Load Demand on Power System Reliability 53
3.4.2 Case Study 2: Effects of PV Power Generation on Power System Reliability 55
3.4.3 Case Study 3: Impacts of Load Demand versus PV Installation Capacity on Power System Reliability 58
3.4.4 Discussion 61

3.5 Summary 62

Chapter 4: Power System Reliability Analysis with Cyber-Physical Interactive Operations of PV Systems 63

4.1 Introduction 63

4.1.1 Status Quo of the Research Problem 64

4.2 The Mathematical Framework of Cyber-Physical Interactive Operations Considering PV Generating Units 66

4.2.1 Reliability Analysis Procedure of PV Systems 67
4.2.2 Reliability Analysis Procedure of Cyber-Physical Systems 71
4.2.3 The Procedure of Composite Power System Reliability Evaluation 76

4.3 Case Studies and Results Analysis 79

4.3.1 The Topology of Reliability Test Systems and Utilized Data for Case Studies 79
4.3.2 Case Study 1: Large-scale of PV Generating Unit Integration on Transmission System 84
4.3.3 Case Study 2: Comparison of PV and synchronous generator for IEEE RTS79 87
4.3.4 Case Study 3: Impact of power network topology on system reliability in IEEE RTS79 90
4.3.5 Case Study 4: Contingency Analysis 92
4.3.6 Case Study 5: Large-scale PV Generating Unit Integration on a Distribution System 94
4.3.7 Case Study 6: Comparison of PV and synchronous generator for RBTS 96

4.4 Summary 99

Chapter 5: Power System Reliability Analysis with Cyber-Physical Interactive Operation of Heat Pump Systems 100

5.1 Introduction 100

5.1.1 Status Quo of the research problem 101

5.2 The Mathematical Framework of Cyber-physical Interactive Operations Considering Heat Pump Systems 103

5.2.1 State Transition Model for Smart Grid 103
5.2.2 Calculation Procedure for Cyber Intrusion Process Times 105
5.2.3 Component-based Reliability Modelling for Heating System 112

5.2.4 Availability Analysis for Heating System with Cyber-physical Component 115
5.2.5 Power System Reliability Assessment in a Smart Grid 117

5.3 Case Studies and Analysis 120

5.3.1 Input Data for Cyber-Intrusion Process in Smart Grid 120
5.3.2 Scenario 1: Cyber-attack on HP during Peak Times 121
5.3.3 Scenario 2: Cyber-attack on Heat Pump through All Day 125

5.4 Summary 129

Chapter 6: Conclusions and Future Work 130

6.1 General Overview 130

6.2 Conclusion 132

6.2.1 Power System Reliability Assessment without CPS Interactive Operation 132
6.2.2 Availability model for PV systems with CPS operation in Power System Reliability 133
6.2.3 Availability model for HP systems with CPS operation in Power System Reliability 134

6.3 Recommendations for Future Work 135

Chapter 7: Appendix 138

7.1 The IEEE Reliability Test System (IEEE-RTS) 138

7.2 The Roy Billinton Test System (RBTS) 142

References 144

List of Figures

Chapter 1

Figure 1.1 A diagram of traditional power system with a unidirectional power flow 1

Figure 1.2 A diagram of a Smart grid with bidirectional power flows 2

Figure 1.3 Thesis Outline 10

Chapter 2

Figure 2.1 A Diagram for Engineering System Reliability Relation with Factors 14

Figure 2.2 Flowchart of Fault Tree Process Steps 16

Figure 2.3 A series configuration of a system network 18

Figure 2.4 A parallel configuration of a system network 19

Figure 2.5 Flowchart of Markov Chain Construction Steps 20

Figure 2.6 An overview of hierarchical levels for power system reliability [2] 25

Figure 2.7- A literature overview of power system reliability considering cyber-physical systems 39

Chapter 3

Figure 3.1 A Line diagram of Average Aggregated Load Profile of Consumers' Data Records [1] 46

Figure 3.2 A part of linearized (red dotted line) and raw (black solid line) load profiles [1] .. 47

Figure 3.3 An example PV Generation Profile for Belfast City (annual) [1] 49

Figure 3.4 A part of linearised (red dotted) and raw (black solid) PV generation profiles [1] 49

Figure 3.5 The Flowchart Diagram of Power System Reliability Evaluation Procedure [1] ...52

Figure 3.6 A Line chart of EENS considering with the scaling factor of different load demands [1] 54

Figure 3.7 A line chart of EENS for Centralised implementation of PV generating unit [1] ..55

Figure 3.8 A line chart of EENS for distributed implementation of PV generating unit [1] ...57

Figure 3.9 Line charts of EENS for Centralised PV generation considering Load capacity a. Maximum Load Capacity, b. Minimum Load Capacity [1] 58

Figure 3.10 Distributed PV generation under Maximum Loading Condition [1] 60

Chapter 4

Figure 4.1. A block diagram of PV generating units with cyber-physical systems [3].....67

Figure 4.2 A single block diagram of Markov chain operation[3].....68

Figure 4.3 Block diagram of Markov chain state transition of PV generating unit[3].....71

Figure 4.4 Procedure of Availability analysis of Cyber-physical system[3].....73

Figure 4.5 The procedure of the reliability assessment framework of PV generating units with CPS [3] 78

Figure 4.6 a) An example of the detailed architecture of the substation with ICT extension, b) Diagram of the extended version of IEEE RTS79 with PV systems and ICT [3].....80

Figure 4.7 Single line diagram of the extended version of RBTS with PV systems and ICT [3] 82

Figure 4.8 Graphs of EENS changes in IEEE RTS79 with centralised PV generating units-a) EENS for centralised PV generating units' integration in IEEE RTS79, b) EENS for centralised PV generating units' integration in IEEE RTS79 with ICT extensions [3] 84

Figure 4.9 Graphs of EENS changes in IEEE RTS79 with decentralised PV generating units- a) EENS for decentralised PV generating units' integration in IEEE RTS79, b) EENS for decentralised PV generating units' integration in IEEE RTS79 with ICT extensions [3] 86

Figure 4.10 EENS changes in centralised PV generation with different topology features [3], a) Centralised PV generating units' integration in IEEE RTS79, b) Centralised PV generating units' integration in IEEE RTS79 with ICT extensions [3]..... 88

Figure 4.11 EENS changes in decentralised PV generation with different topology features- a) Decentralised PV generating units' integration in IEEE RTS79 b) Decentralised PV generating units' integration in IEEE RTS79 with ICT extensions [3]..... 90

Figure 4.12 Comparison of EENS variation considering different generating units in Bus 9- a) PV Power Generation, b) Conventional Generation [3]..... 91

Figure 4.13 Graphs of EENS changes in RBTS with PV generating unit integrations- a) Centralised PV generating units' integration in RBTS, b) Centralised PV generating units' integration in RBTS with ICT extensions, c) Decentralised PV generating units' integration in RBTS, d)Decentralised PV generating units' integration in RBTS with ICT extensions [3] .. 95

Figure 4.14 EENS changes in RBTS considering conventional and PV powered generation- a) Centralised PV generating units' integration in RBTS, b) Decentralised PV generating units' integration in RBTS, c) Centralised PV generating units' integration in RBTS with ICT extensions, d) Decentralised PV generating units' integration in RBTS with ICT extensions [3] 97

Chapter 5

Figure 5.1 Generic attack tree graph for smart grid environment 103

Figure 5.2 Semi-Markov model for cyber-attack states 104

Figure 5.3 Comparison of calculation procedures of MTTA and $MTTC_{Cyber}$..... 107

Figure 5.4 Single Line Block Diagram of Generic Heating System Configuration..... 113

Figure 5.5 Single Line Blok Diagram of Generic Heat Pump's elements 114

Figure 5.6 Power system reliability calculation framework with cyber-intrusion process 119

Figure 5.7 Comparison of raw aggregated HP load profile and HP load profile with cyber-intrusion (cyber-intrusion only during the peak times) - a) $MTTD_{Cyber}$ is considered as a General Pareto random number, b) $MTTD_{Cyber}$ is considered as a Pareto random number... 122

Figure 5.8 Comparison of raw aggregated HP load profile and HP load profile with cyber-intrusion (cyber-intrusion only during the peak times) - a) $MTTD_{Cyber}$ is considered as a Gaussian random number, b) $MTTD_{Cyber}$ is considered as a Stable random number 123

Figure 5.9 Comparison of raw aggregated HP load profile and HP load profile with cyber-intrusion (all day along) - a) $MTTD_{Cyber}$ is considered as a General Pareto random number, b) $MTTD_{Cyber}$ is considered as a Pareto random number..... 126

Figure 5.10 Comparison of raw aggregated HP load profile and HP load profile with cyber-intrusion (all day along) - a)$MTTD_{Cyber}$ is considered as a Gaussian random number, b) $MTTD_{Cyber}$ is considered as a Stable random number..... 127

Appendix

Figure 7.1 IEEE Reliability Test System (IEEE-RTS-24 bus)..... 138

List of Tables

Chapter 3

Table 3.1 Comparison of linearised PV and original PV profiles on the system reliability [1] 60

Chapter 4

Table 4.1 Reliability data for PV system, ICT components and CPS repair time strategies[3] 83

Table 4.2 Contingency Analysis of the IEEE RTS79 for Critical Components [3] 93

Chapter 5

Table 5.1 Reliability Data for Heat Pump System [186] 120

Table 5.2 Utilized Time Intervals for a Smart Distribution Systems 121

Table 5.3 EENS Changes for Scenario 1 124

Table 5.4 EENS Changes for Scenario 2 128

Appendix

Table 7.1 Generator reliability data for IEEE-RTS 139

Table 7.2 Bus load data for IEEE-RTS 139

Table 7.3 Branch Data for the IEEE-RTS 140

Table 7.4 Branch Reliability Data for the IEEE-RTS 141

Table 7.5 Load data for the RBTS 142

Table 7.6 Line Data for the RBTS 143

Table 7.7 Generator data for the RBTS 143

List of Abbreviations

AMI	Advance Metering Infrastructure
ASHP	Air-source Heat Pump
CPS	Cyber-physical System
COP	Coefficient of Performance
COP_{ideal}	Coefficient of Performance (ideal)
DER	Distributed Energy Resources
DSM	Demand-side Management
GSHP	Ground-source Heat Pump
EDNS	Expected Demand Not Supplied
EENS	Expected Energy Not Supplied
ES	Ethernet Switch
HP	Heat Pump
ICT	Information and Communication Technology
IEEE RTS79	IEEE Reliability Test System-79
MTTA	Mean Time to Attack
$MTTC_{Cyber}$	Mean Time to Compromise for Cyber-attack
$MTTD_{Cyber}$	Mean Time to Detection for Cyber-attack
MU	Merging Unit

$P_{Cyber\text{-}attack}$	The probability of cyber-intrusion
PMU	Phasor Measurement Unit
PV	Photovoltaic
RBTS	Roy Billinton Test System
SCADA	Supervisory Control and Data Acquisition
TTR	Time to Repair
WSHP	Water-source Heat Pump
A, U	Availability/Unavailability of system indicators
P_{f_X}, P_{r_X}	Failure/Repair state probability of component X (series)
$\lambda_{system}, \mu_{system}$	Failure/Repair rate of system
$\lambda^{k}{}_{Panel}, \mu^{k}{}_{Panel}$	Failure/Repair rate of kth PV panel
λ_{CC}, μ_{CC}	Failure/Repair rate of Charge Controller
λ_{BB}, μ_{BB}	Failure/Repair rate of Battery Bank
λ_{MI}, μ_{MI}	Failure/Repair rate of Micro-inverter
$\lambda_{String_k}, \mu_{String_k}$	Failure/Repair rate of kth String
$P^{X}_{f_{String}}, P^{X}_{r_{String}}$	Failure/Repair state probability of component X (parallel)
$\lambda_{Cyber}, \mu_{Cyber}$	Failure/Repair rate of Cyber-physical system
$\lambda^{X}_{Y}, \mu^{X}_{Y}$	Failure/Repair rate of Y element related to X system

T_L	Outdoor Temperature (K)
T_H	Indoor Temperature (K)
W_i	The waiting (sojourn) time at each phase
W_{input}	Input Energy Demand
$[\tau_{a,i}, \tau_{a,i}^{max}]$	Lower-upper boundary limits of normal attack agent
$[\tau_{s,i}^{min}, \tau_{s,i}^{max}]$	Lower-upper boundary limits of smart attack agent
X_i^n	The normal attack time needed during *i*-th phase of cyber intrusion for attack agent
X_i^s	The smart-attack time needed during *i*-th phase of cyber intrusion for smart-attack agent
Y_i	The detection time of the cyber intrusion during *i*-th phase for detection agent
randp	Pareto random number generator
randn	Gaussian random number generator
gprnd	General pareto random number generator
stblrnd	Stable random number generator
λ_C, μ_C	Failure/Repair rate of heating system's control panel
λ_{Str}, μ_{Str}	Failure/Repair rate of heating system's storage
λ_{HP}, μ_{HP}	Failure/Repair rate of heat pump
$\lambda_{Switch}, \mu_{Switch}$	Failure/Repair rate of switch

λ_{AH}, μ_{AH}	Failure/Repair rate of auxiliary heater
λ_{Eva}, μ_{Eva}	Failure/Repair rate of evaporator
$\lambda_{Comp}, \mu_{Comp}$	Failure/Repair rate of compressor
$\lambda_{Cond}, \mu_{Cond}$	Failure/Repair rate of condenser
$\lambda_{Evalve}, \mu_{Evalve}$	Failure/Repair rate of expansion valve
M_4	4-state stochastic transition matrix for heating system
M_8	8-state stochastic transition matrix for heating system
F_{Cyber}	The number of successful cyber-intrusion attempts
$A_{succesful}$	Successful cyber-intrusion attempt

List of Publications

1. Hasan Gunduz, Dilan Jayaweera, “Reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems,” International Journal of Electrical Power and Energy Systems, vol. 101, pp. 371-384, 2018. *(Published journal paper)*
2. Hasan Gunduz, Zafar A. Khan, Abdullah Altamimi, Dilan Jayaweera, “An Innovative Methodology for Load and Generation Modelling in a Reliability Assessment with PV and Smart Meter Readings,” 2018 IEEE Power & Energy Society (PES) General meeting, Portland, 2018. *(Published conference paper)*
3. Hasan Gunduz, Dilan Jayaweera, “Power System Reliability Evaluation with Cyber-Intrusion on Heat Pump Systems”. (*Submitted to IEEE Transactions on Power Systems)*
4. Bader Alharbi, Hasan Gunduz, Dilan Jayaweera, "Risk Assessment in a Smart Power System with Dynamic Thermal Limits and Strategic Connection of PV Systems" Smart Grid Conference in Saudi Arabia (SASG) December 2018. *(Published conference paper)*
5. Zafar A. Khan, Dilan Jayaweera and Hasan Gunduz, "Smart meter data taxonomy for demand side management in smart grids," 2016 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Beijing, 2016, pp. 1-8. (Published conference paper)

Chapter 1: Introduction

1.1 Status Quo of Power Systems

The principal goal of a power system is to supply electricity to customers with the high quality, secure, and uninterrupted level of service, which is as affordable as possible. The power system is considered as a critical infrastructure and it needs continuously adapt to necessary technological developments for hi-performance with regards to operation and reliability [4]. Nevertheless, due to the complexity of power systems with its enormous size, the adaptation of electricity grid into new technological innovations has proceeded slowly. Power system operation with a traditional structure would lead to reduce the system efficiency, increase difficulties in operation, and challenges to maintain forthcoming electricity demand. Future electricity demand is expected to reach high levels, whereas the current generation systems may not fully meet the projected demand. This status is likely to affect the system limits [5-7]. As the system demand keeps on growing with similar projections [5, 6], power system is forced to operate with its boundary limits, and its reliability has evolved into a critical problem.

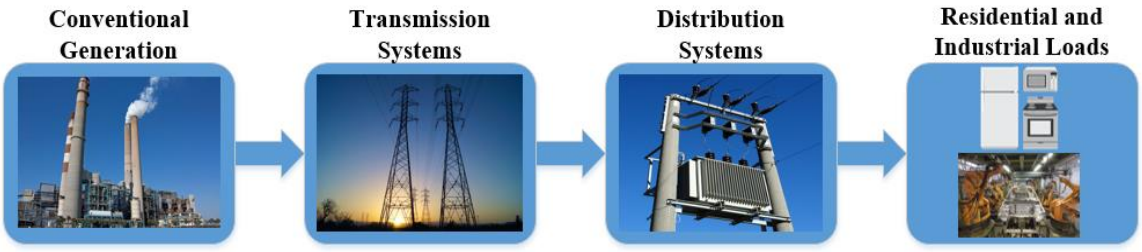


Figure 1.1 A diagram of traditional power system with a unidirectional power flow

A traditional power system (Figure 1.1) is centralised in nature, from the perspective of controllability and transmissibility of power. Traditional power systems operate from

centralised generators throughout transmission and distribution infrastructure towards end-users with a unidirectional concept. Thus, a malfunction or a physical failure in any section of traditional power systems could affect many consumers and their assets due to cascading collapse, and even great deals of economic loss. According to [8], power systems have experienced ten major blackouts around the globe during last decade. Most of power outages have occurred due to the reasons of the tripping of assets, overloading during peak time, and a lack of self-monitoring on operational status [8]. As a solution to conventional and ageing power infrastructure, an increasing amount of DER with ICT might diminish the impact of power outages, and also increase the operability, controllability, and manageability of power systems.

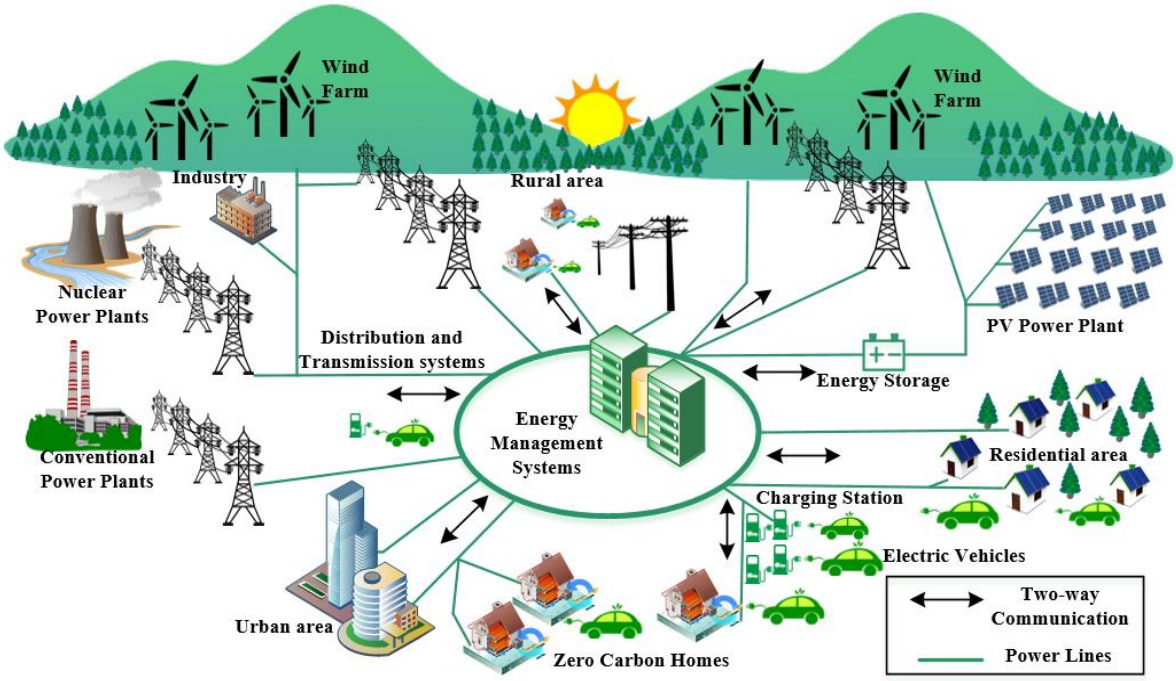


Figure 1.2 A diagram of a Smart grid with bidirectional power flows

The existing electricity grid is undergoing a transformation called "*Smart Grid"*, and is gradually becoming more technologically intelligent than before [9]. Smart grid can be defined

as a modernised power grid that supplies electricity to end-users by utilising digital control and monitoring mechanisms [9].

Smart grid (Figure 1.2) is digitalized in nature owing to its bidirectional communication, as it has sensors throughout, two-way energy flows, decentralised generations, many consumer choices, and pervasive control loads [9]. Due to environmental legislations, low carbon technologies are pushing power systems more into the direction of smarter grid systems [10]. Therefore, the smart grid has become a product of highly complex architecture with self-monitoring characteristics. As a result, it allows end-users to be prosumers and to interact energy management systems in order to regulate their energy consumption as well as to minimise utilised electricity costs [9]. The concept of smart grid includes self-healing features that mitigates sudden failures [9]. It forecasts imminent actions and stabilises operating conditions in optimum levels [9].

Besides the benefits gained by coupling smart grids with controllability criteria, smart grid presents a large number of challenges as new technologies and innovations becoming incorporated into and influential upon the system operation. Supposing that high penetration of intermittent distributed generations in a power grid, these generation units might stress the operation of transmission and distribution lines and might also result in voltage-var management issues. For instance, distribution systems could face a circuit congestion as a consequence of uncontrolled levels of increasing active loads. Other DER technologies such as heat pumps, electric vehicles, and batteries can assist to the power systems in the context of improving system reliability, peak time load management, and ancillary services of power systems [11].

In the meantime, apart from all profound alterations and difficulties with the transformation of grid, the primary goal of a power system still remains unchanged, which continuously serve the electric power to end-users in secure limits and with standardised quality. Hence, the system reliability needs to keep in step with the revolutionary transformation of power systems.

1.2 Status Quo of Low Carbon Technologies and ICT

Many developed countries have already announced their projections on the transformation of power sector and have started to change their energy policies according to climate change targets [12, 13]. For instance, the United Kingdom (UK) have entered into a binding agreement to cut carbon emission by 50% in 2050 compared to 1990 levels [12]. In order to achieve these targets, high-level integrations of low carbon technologies in power networks are considered as an essential step by authorities and stakeholders. In particular, photovoltaic (PV) and heat pump (HP) systems are likely to be essential driving factors in order to mitigate carbon footprint.

In perspective of renewable generation, one of the promising technologies is PV, of which the source is free, sustainable, and environmentally friendly. PVs are substantial instruments in low carbon transitions, and utilization of them is expected to reach high levels. As maintained by envisioned guidelines of governments, net generation capacity of PV technologies reached 402 GW during the year of 2017 globally [14], and the total capacity of PVs is projected to reach up to 1721 GW in 2030 [15]. In other respects, total installed capacity of PVs in the UK has exceeded 12 GW at the end of 2017, in almost 10 years [16]. With this ambitious high installation rate of PV systems, power systems are expected to face massive integration

challenges [17]. For instance, when the power grid is connected with high penetration of PV systems, there can be voltage fluctuations, rise, thermal overloading issues, etc. [17]. These issues could cause system local failures on the power systems, and therefore reduce the power system reliability. As the intermittency of PV generations, the reliability of power grid should be carefully examined for system performance continuity in high levels.

With regard to renewable heat generation, governments are offering incentives to popularize consumers renewable heat technologies such as HPs [18]. As a result, there has been renewed interest in the deployment of HPs, and their increment on power grid is likely to reach high level [18-20]. It is expected that total number of installed HPs will peak at a rate of 5.4-5.6 GWt level by 2020 in the UK [19]. Accordingly, HPs are likely to play a key role in addressing the reduction of greenhouse gases. They also give benefits to the whole system, but only if the generated electricity is decarbonised. HP technology might save heating sector from the dependency of natural gas usage. Beside the provided advantages by HP, it could also bring integration challenges into power grid and reduce the reliable operating conditions of power system, e.g. thermal overloading in the power system assets [21], higher demand peaks [22], and increasing expenses on reinforcement of the system [23]. Therefore, high installation rates of HP systems can be an important concern on the reliability of power systems.

From the point of system monitoring, the rapid digitalization of power systems throughout the integration of communications technologies (ICTs) is incorporated with advanced metering infrastructure (AMI) and other cyber-physical sensing infrastructure in order to provide support for power systems. For example, AMI have the ability to measure electricity use, connect and disconnect local power system operation, isolate outages, monitor voltage changes and communicate thermostats etc. To enable penetrating high levels of low

carbon technologies into power grid, operators should deploy high level of ICT (AMI, PMU etc.) to control these technologies remotely [188]. Due to ICT expands attack surfaces with high number of access points, high installations of low carbon technologies introduce additional risks of unusual operational conditions [188]. In the UK, just over 6 million smart meters were installed into all properties until the beginning of 2018 [24]. The installed number of AMI is expected to reach 50 million by 2020 [24].

The increased number of digitalized components in the power sector can bring new opportunities to companies and increase co-benefits when power systems take advantage of digitalized systems' monitoring and control characteristics. For example, whether there is an interrupted part in the system operation or a failure, digitalized remote control system can send information about the system operation state and state of the disturbed parts of the power system. These various benefits can improve power system operations according to design and planning approaches with internal and external factors.

On December 2015, Ukrainian distribution utility was faced with cyber-intrusions through the SCADA (Supervisory Control and Data Acquisition) management systems and the utility's computers [25]. As a consequence, 30 substations were disrupted for three hours due to remote controlling of switches by attackers [25]. Thousands of consumers experienced power cuts for several hours. Because of the complex nature of these cutting-edge technologies in power sector with their related dependent and interdependent faults, consumers and operators have been dealing with local operational breaks and even partial blackouts. As a result, these interruptions highlight the importance of power system reliability and its studies for the deployment of green and digitalized technologies.

1.3 Motivation and the Scope of the Research

The operation of power systems has always suffered from random physical failures. Due to high penetration levels of renewable energy technologies and increasing level of digitalization in power grids, these failures are expected to increase and expand failure concepts to include cyber-physical failures. As a result, this could trigger changes in power system operations and increase the possibility of high-impact low-probability events, such as cyber-attacks. Traditional power system reliability evaluations consider only physical system contingencies with constant failure and repair rates, whereas it does not evaluate the interaction of CPS with low carbon technologies. In addition, publicly available data on failure-repair rates of CPS, which is required to evaluate their interaction effects on power system reliability, is limited. CPS failure and repair rates are inconsistent due to the unpredictable characteristics of cyber-threats and erratic cyber-vulnerabilities. Systematically, these vulnerabilities can affect the ability of the system to achieve high reliability levels during the system operation. Although the CPS interruptions with cyber-intrusions are accepted as extraordinary events with low probability, reliability assessments without CPS interactions can mislead power system planners and operators and can bring high societal and financial consequences.

The scope of this research is to assess reliability performance levels considering low carbon technologies (PVs and HPs) in a smart power system environment with and without the consideration of CPS interactive operation. The availability analysis of renewable energy technologies of power systems is also carried out with the internal and external factors of cyber-physical system operations. In order to achieve the target, generic reliability models of DER are created with their critical dependent and interdependent components. Relevant case studies

are presented to demonstrate the impacts of cyber threats in the purview of power system reliability. In addition, specific issues related to cyber-attack modelling with DERs are identified and discussed in the context of power system reliability.

1.4 Aim and Objectives

The aim of this research is to investigate the reliability of a smartly operated power system with CPS operation of PV and HP systems. The main objectives of this research are as follow:

- Investigate effective reliability levels of a power system considering dependency and interdependency factors of PV and HP systems.
- Assess the acceptable penetration levels of PV systems considering dependent and interdependent components with controllability criteria of PV systems.
- Assess the HP system considering the configuration of its dependent and interdependent components for power system reliability.
- Develop an availability modelling framework of a PV system within the perspective of CPS interactive operation.
- Develop an availability analysis platform of HP systems with considering CPS interactive operation.

1.5 Contributions of the Thesis

This thesis makes several contributions. They are summarised as follow:

1. An innovative methodology is proposed to assess the reliability interaction of a physical power system with cyber network by taking into account possible threats and vulnerabilities.
2. A new availability model for PV configuration is proposed to reduce assessment process complexity of cyber-physical systems in a holistic way.
3. A new algorithm is proposed for the reliability assessment of a PV integrated power system with cyber physical interactions at PV connections with varying levels of intensity of cyber-attacks.
4. A new mathematical model for HP system configuration is proposed in order to reduce assessment process complexity of cyber-physical systems.
5. A new algorithm is proposed for the reliability assessment of HP systems with cyber physical interactions.
6. An enhanced cyber-intrusion process model is presented for cyber-physical system reliability analysis. This model also considers stochastic attack-detection time in cyber-intrusion process.
7. Sensitivity analysis of cyber-physical system repair times for PV systems is carried out.
8. Sensitivity analysis of attack-detection times in cyber-intrusion process for HP systems is performed.

1.6 Outline of the Thesis

The outline of this thesis is described in Figure 1.3.

Chapter 2 presents a relevant literature review for this research. The relevant literature is reviewed in the context of reliability issues. It consists of the concepts of reliability assessment

in engineering applications, a fundamental understanding of power system reliability and its methods, power systems reliability considering low carbon technologies, and its ICT related background. The research direction of this thesis is highlighted.

Chapter 3 highlights the importance of load and generation modelling in the context of power system adequacy. The utilized load and generation models are presented. In addition, the traditional concept framework for power system reliability assessment is proposed without considering cyber-physical system interactions in IEEE RTS79. The case studies demonstrate the intermittent pattern impacts of PV generation and consumer load demand profiles.

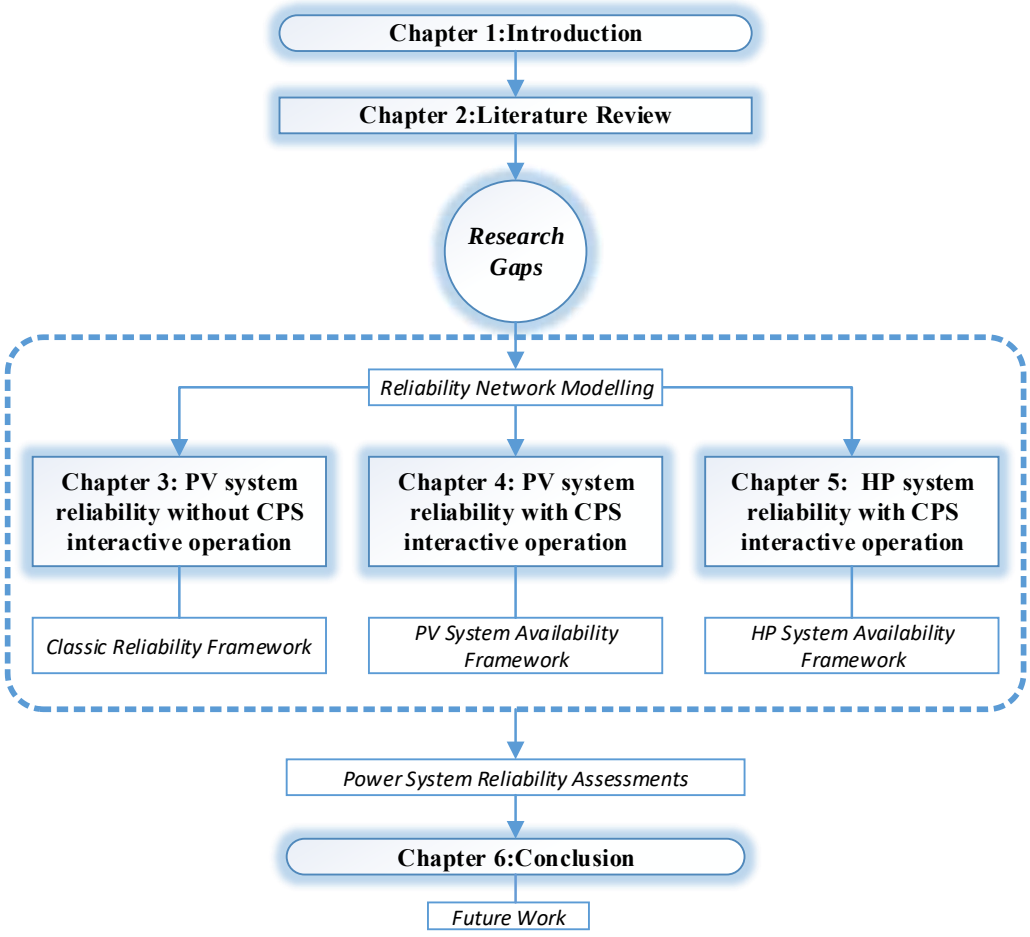


Figure 1.3 Thesis Outline

In chapter 4, the research related to cyber-physical system operation is highlighted by also explaining its research problems. The mathematical framework of cyber-physical interactive operations considering PV generation systems is proposed with a power system reliability procedure. Different case studies are presented with and without ICT extended versions of buses in order to understand CPS interactive operation of PV systems. Case studies are implemented into either RBTS or IEEE RTS79 in order to assess the integration of PV systems. The results are analysed and summarized subject to the power system reliability with CPS interactive operation of PV generation.

In chapter 5, cyber-attack pathways are discussed in relation to smart grid applications, and the limitations of previous research are discussed. The mathematical framework of cyber-attack models and the configuration of HP systems are proposed with power system availability-reliability model. The power system reliability evaluation with cyber-intrusion on HP systems is demonstrated by case studies, and their results are analysed and discussed.

Chapter 6 concludes the research findings and then presents the future work.

Chapter 2: Literature Review

2.1 Introduction

The main objective of this chapter is to provide a fundamental knowledge of power system reliability and then its status quo and interactions with PV (Photovoltaic), HPs (Heat Pumps), and cyber network operations relevant to this project. Furthermore, it highlights concepts of reliability in perspective of traditional and modern power systems.

Power systems have emerged as necessary platforms for modern society. A fundamental concern of a power system is to supply electricity to its consumers in an uninterrupted, safe and cost-effective manner [2]. The expectation of a society from a power system is to prevent the society from experiencing its unexpected failure and blackouts. Therefore, a power systems' reliability performance and its applications will always be called into question. In general, reliability, which is vital for a wide range of scientific and industrial system processes, refers to both piecewise or composite element based system availability with their successful working conditions [26].

Nowadays, power systems are evolving from conventional to smart characteristics and this transformation involves high levels of low carbon technology integration and installation of information and communication technologies (ICTs). With this revolutionary transition of the energy sector, the reliability of power systems has become an essential part of its operation and future planning. With this transition, the assessment strategies of power system reliability would also have to change in order to perform an accurate and robust evaluation of power system operations and planning.

In the sections of this chapter that follow, relevant literature will be reviewed in the context of reliability. Especially, as it contains the concepts of reliability assessment in engineering applications, a fundamental understanding of power system reliability and its methods, power systems reliability considering low carbon technologies, and its ICT related background. In the final part of this chapter, research gaps are highlighted in power system reliability related to physical and cyber-physical system operations.

2.2 Reliability Assessment of Engineering Applications

The target of this section is to give a general overview of reliability evaluation, reliability concept techniques in engineering applications, and particularly the case of power system reliability.

2.2.1 General Concept of Reliability in Engineering Systems

Engineering systems have a vital role for modern society in order to sustain and facilitate daily work processes with consistently secure operating. From basic components to complex structures of engineering systems need to be analysed for their past, current and future operation conditions to maximise their operation performance, and minimise their failures. These failures of engineering systems provoke high societal consequences such as chemical and nuclear contaminations, aircraft accidents, large-scale blackouts and many deaths [7, 26]. Hence, these severe events have raised the profile of operational conditions of engineering applications [7]. The expectation of consumers and the public from life cycle of any engineering system is to have less hazardous working circumstances, an economical and a reliable operation status at all time. In order to meet requirements, engineers and stakeholders should consider internal and

external factors of engineering systems. These factors in relation to any system's reliability are illustrated as in Figure 2.1. Overall system reliability for engineering applications is engaged with balance indicators: time duration, safety, quality, and cost [27]. These indicators are generally driven by system's material, design and technology, environmental and human factors [27]. Because of effects of these drivers and severe events, reliability has been preserved for its important position in any engineering system.

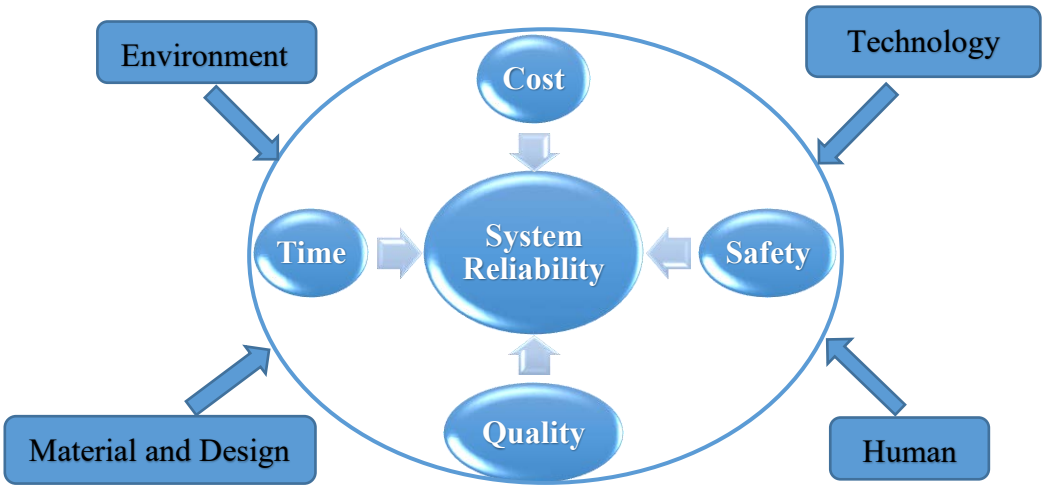


Figure 2.1 A Diagram for Engineering System Reliability Relation with Factors

2.2.2 Reliability and Availability

Due to many different environmental circumstances and variety of systems, the meaning of '*Reliability*' differs concept to concept and people to people [2, 7]. There are multiple definitions of the term '*Reliability*'. As a general dictionary term, it is paired with 'being trustworthy' or 'quality of performance indicator'. As an engineering term, '*Reliability*' $R(t)$ refers to the probability of a system or element to provide its required duties within specified circumstances with operating status for a specific time period [2, 28]. When the time of failure is identified as T, the '*Reliability*' $R(t)$ is analytically expressed by [7, 29]:

$$R(t) = P(t > T) \quad t \geq 0 \tag{2.1}$$

'*Availability*' is an operational measurement that permit a system to recover if there is a system failure. As a basis, '*Availability*' $A(t)$ defines the probability of a system or element to provide its required duties within specified circumstances with operating status for a specific time moment [2, 28]. The availability of a system is accepted as a reliability merit of a system. '*Availability*' and unavailability of a system complete each other and help to measure reliability performance of the system. Mathematically, '*Availability*' $A(t)$ is defined as [29]:

$$A(t) = \frac{Time\ to\ System\ Operating}{Time\ to\ System\ Operating\ + Time\ to\ System\ non\_operating} \tag{2.2}$$

2.2.3 Overview of Reliability Techniques in Engineering Systems

For many years, reliability has been expressed with qualitative and subjective terms by engineers [7, 26]. This approach relies experience of engineers or designers on the system operation, design and configuration characteristics. Due to subjective judgements, this is a deficient approach to have in engineering system as a reliability assessment technique when there is a need for change on performance or economic analysis on the system. In order to meet this demand of an engineering system, quantitative analysis need to be involved for a robust reliability evaluation. In general, reliability evaluation techniques in engineering systems are categorised into two groups: 1) Analytical methods and 2) Numerical methods [7, 26]. This section presents a number of mathematical and simulation methods on reliability assessments.

2.2.3.1 Fault Tree Analysis

Fault Tree analysis, an analytical technique, is one of the most broadly accepted techniques for quantification and quantitation of reliability and risk in mission-oriented engineering system [30, 31]. Fault tree analysis is identified as a top-down failure analysis tool to design and reveal possible failure pathways for system modification, operation and planning[7, 30, 31]. The Failure Tree model has a mission to determine undesired events that can provoke the system to failure state. By means of quantified overall event probability, the system reliability can be judged in perspective of engineering. This technique has also been commonly utilized in nuclear power industry, aerospace industry, chemical industry, etc. [7].

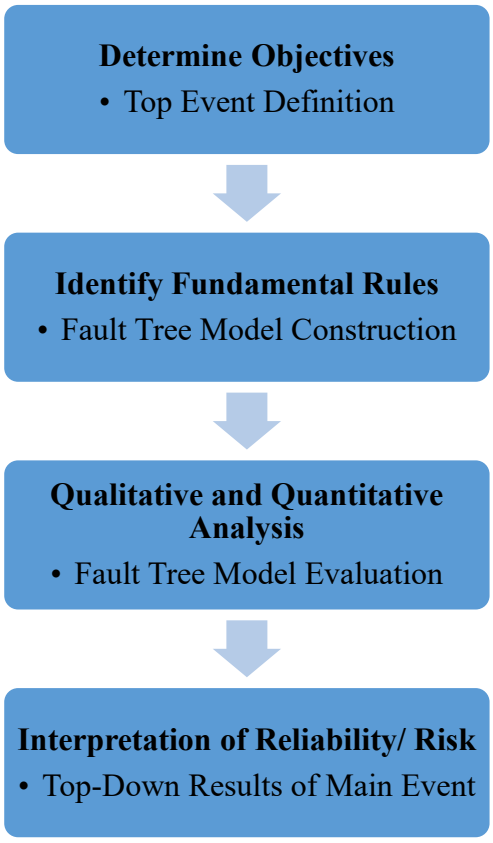


Figure 2.2 Flowchart of Fault Tree Process Steps

In order to design probable undesired events and identify a combination of failure states, Fault Tree analysis utilizes Boolean logic gates such as “OR”, “AND”, etc. For example, when there is a group of sub-events, that causes a system down, “OR” gate utilizes in the construction of the Fault Tree model. On the other hand, if the all sub-events lead to force main event down, “AND” gate is used for the model construction. The expansion criteria of the Fault Tree model construction is based on data availability and its detail [7, 26]. The Fault Tree analysis process steps [7] are described in Figure 2.2.

2.2.3.2 Event Tree Analysis

Event Tree analysis is accepted as an analytical bottom-up technique for identification and quantification of undesirable event outcomes linked with various initiating events [7, 31, 32]. The Event Tree model presents an overall picture of the system’s branches associated with its events’ success and failures [7, 31, 32]. It provides a preliminary approach to assess chronological sequence of event outcomes. Event Tree analysis is more widely utilized with security-oriented system risk analysis. It can be applied into qualitative or quantitative reliability assessments of a system. It is associated with Fault Tree analysis. The evaluation in Event Tree analysis is similar to Fault Tree analysis. Fault Tree constructing procedure [7] are demonstrated as in the following steps:

1) Define a relevant initial event that may causes undesired consequences
2) Define the restrictions and barriers that can deal with the initial event (safety functions)
3) Construct the Event Tree model
4) Determine the frequency of the event and classify the event consequences

5) Estimate the conditional probability of each tree branches

6) Quantify the consequences

7) Present and evaluate the event results

2.2.3.3 Reliability Block Diagram

There are other analytical methods utilized in reliability and risk assessments, such as minimum cut-set, tie-set, network reduction techniques [7, 26, 33]. These reliability techniques can be implemented in the block diagram of a system. In general, a system with its components

Figure 2.3 A series configuration of a system network

can be demonstrated as a network block. The system network can be modelled as a series, parallel, meshed or a combination of these configurations [26, 33]. In this part of the section, series and parallel system connections with independent elements are presented in context of reliability.

Let C_1 and C_2 represent independent elements of a system as in Figure 2.3. These two components are connected as a series system. The system reliability depends on both components' successfully working condition. Overall system reliability (R_s) can be calculated as in [26]:

$$R_s = R_{C_1} \times R_{C_2} \tag{2.3}$$

This formula can be generalised with n number of components connected as a series by following:

$$R_s = \prod_{i=1}^{n} R_{C_i} \tag{2.4}$$

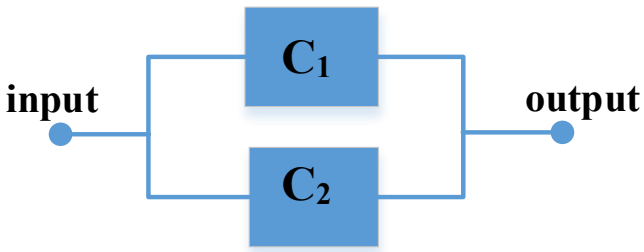


Figure 2.4 A parallel configuration of a system network

C_1 and C_2 are independent elements of a system as in the utilized independent components and are described as in Figure 2.4. In order to sustain the successful working order of the system network, either 'C_1'or 'C_2' or both of the components should be in the operating state. If the system is considered as a parallel-connected system, then overall system reliability can be expressed as in [26]:

$$R_s = R_{C_1} + R_{C_2} - R_{C_1} \times R_{C_2} \tag{2.5}$$

2.2.3.4 Markov Processes

A Markov process is defined as a probabilistic model that represents a sequence of variety events that each event probability relies on the state accomplished in the previous event [26, 33]. A Markov Chain model is a type of Markov property, can be implemented to random events, which include discrete or continuous behaviour with subject to the time and space [7, 26, 33]. The future status of an event is only dependent on the present status, not past status of

the event. Future and past status of the event are independent. Because of this, the Markov model should be categorised as memoryless [26, 33].

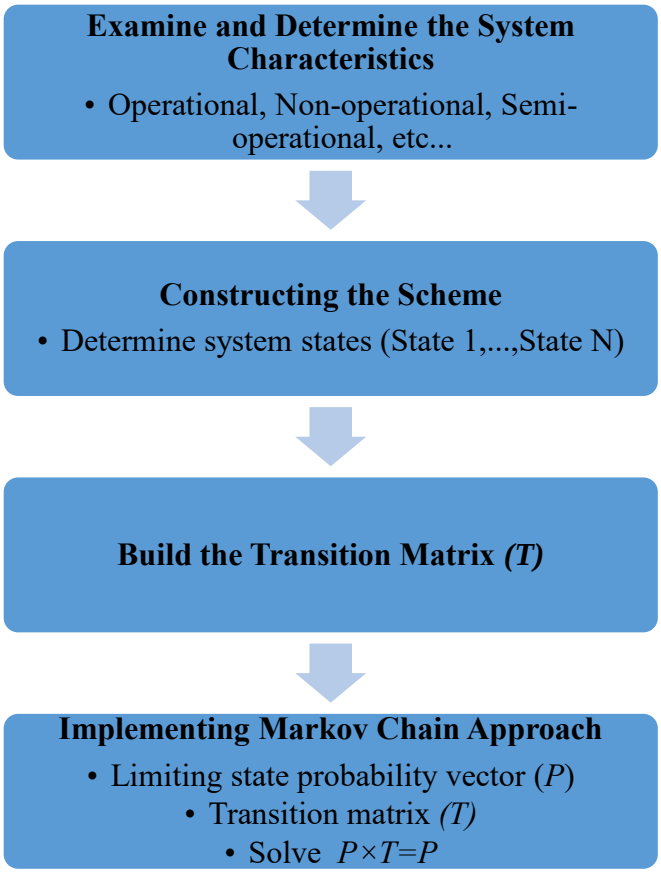


Figure 2.5 Flowchart of Markov Chain Construction Steps

Markov property can be seen in availability and reliability evaluations of the system. Markov property applications are ranging from basic elements to composite system analysis. It is mainly considered for analysing component level reliability as operating and non-operating states. This is one of the approaches of Markov modelling. In order to construct availability analysis of any engineering system with Markov Chain, its construction steps [7] can be described as in Figure 2.5.

2.2.3.5 Monte Carlo Simulation

Numerical methods for reliability evaluation in engineering are alternative approaches to analytical methods in reliability, one of which is "*Monte Carlo simulation*". This method is based on repetition of random sampling of given statistical data or probability distributions [2]. The requirement for this method is element failure-repair time data and system network configurations. The failure and recovery times of each element is represented by probability distributions of given or generated data. The system reliability indicators can be computed after applying large number of the simulation iterations into the process. By implementing this, reliability indexes of the given system can be estimated.

Monte Carlo simulation methods can be categorised into 1) Sequential and 2) Non-sequential techniques. Sequential Monte Carlo technique relies on the time dependent system or event state sequences. Due to this characteristic, a chronological system or event status can be identified [2]. This type of reliability evaluation approach is widely utilized in real life applications. Otherwise, non-sequential method considers time independent of event status or system states.

One of the advantages of Monte Carlo simulations is to have a flexibility in the reliability evaluation and, there is no virtual restriction compared to deterministic approaches. On the other hand, there is no exact result in Monte Carlo simulations. They give estimated solutions of reliability indicators. Because of this, there are also a certain number of advantages and disadvantages on reliability analysing methods, the selected reliability assessment approach cannot be guaranteed to deal with whole system reliability characteristics [26]. Therefore, engineers need to select an appropriate reliability technique according to system characteristic

merits and demerits [2, 26]. In specific cases, selected reliability approach may be a combination of the analytical method and the Monte Carlo simulation method. In this thesis, the hybrid reliability technique is also applied into relevant systems in further chapters.

2.3 Reliability Assessment in Power Systems

The electric power system, which is regarded as a highly sophisticated technological development in history invented by humankind, has a complex working order and a multitude of uses application in modern society. This phenomenal system is composed of many complex and complicated structures, systems, combined sub-systems, interactive operational components and applications, which have communication capabilities. Even though this system is associated with communication complexity and structural intricacy, the main objective of power systems is supplying, transferring and utilizing electric power to consumers while maintaining adequate security, quality and economic levels [2]. This mission also needs to be sustained with an acceptable level of continuity to avoid blackouts and brownouts. Electricity for consumers should be supplied whenever it is required by users. Power utilities have been faced with the problem of avoiding many massive blackouts and brownouts [34, 35]. Because of these catastrophic events with their high societal consequences, power system reliability has been often scrutinised and evaluated in all times.

2.3.1 Power System Reliability

As previously highlighted, reliability is one of the essential processes of any system that indicates system quality level for its current or future status according to encountered unexpected circumstances. There is a need to be explicit about exactly what is meant by

reliability for power systems. Reliability of a power system, is a performance sign for power system quality and economics, can be referred to as providing electric power in an adequate and secure degree [2, 7]. Thus, power system reliability is one the primal necessity evaluation concepts in power system planning, design and operation stage.

Traditional energy networks have a complicated nature, unidirectional energy flow and uncontrolled passive loads [9]. Due to the nature of this complex integrated system and its related failures, customers and operators have been facing electricity interruptions and disruptions [11]. These are not new experiences for stakeholders, but outage of electricity utilization is bringing a significant economic effect into the society directly or indirectly [34]. Existing energy networks have been developing in conjunction with distributed energy resources as well as communication components [11, 17, 36]. These new devices are expected to bring new challenges for customer side of the network and whole system.

Power system reliability evaluation is classified into two fundamental perspectives that are related to power systems' static, transient and dynamic status: 1) power system adequacy and 2) power system security. To integrate and operate any power system application or components in the energy networks within global reliability criteria, these two aspects of power system reliability should be taken into account [2, 7].

In terms of power system, '*adequacy'* can be defined as a capability of existing electric power system that covers consumer energy demand in a satisfactory manner considering its operational restrictions [2, 7]. Power system adequacy involves evaluating required energy supplied and transferred to customer load points by distribution and transmission networks[2, 7]. Thus, power system adequacy assesses only static circumstances of the system.

In broad terms, *'security'* can be expressed the capability of electric power system to stay in global security limits without any high consequences [2, 7]. Security is associated with power system reaction against taken place dynamic and transient interruptions in the system process. In order to evaluate power system security, one of the widely utilized approaches is to do a contingency analysis. There are several kinds of contingency analysis; N-1 and N-2 are very common approaches in power system security. N-1 contingency evaluation, considers single contingency, is utilized for planning stage of power system to avoid cascading failures during system operation [37]. Security planning and projection standard of power system is based on N-1 contingency analysis. System planners and operators also considers N-2 contingency analysis if there is a possibility of losing two components simultaneously during power system operations [37]. During the power system reliability assessment, it is essential to differentiate the perspectives of power system adequacy and security.

2.3.2 Hierarchical Levels of Power Grid

Power systems are mainly classified into electric power generation, power transmission and power distribution systems [38]. Due to increasing high structural complexity from power generation system to power distribution systems, adequacy assessment of power systems are also divided into three hierarchical levels [2] as in Figure 2.6. These segments are associated with generation, transmission and distribution system facilities.

Hierarchical level one (HL1) only considers the reliability of power generation systems. In this segment, transmission network with its energy transportation ability to meet consumer load demand is neglected in adequacy evaluations. In other respects, Hierarchical level two (HL2) takes into consideration of transmission system as well as power generation systems.

The adequacy assessment of HL2 segment has an ability to assess individual load point and overall system reliability indicators. Hierarchical level three (HL3) combines and examines all three segments adequacy ranging from generation systems to power distribution system that includes individual consumers and prosumers. The adequacy assessment of HL3 segment is the most complex and incorporates impact of interruption frequency, duration and severity.

In order to carry out an adequacy assessment on any of these segments, standard reliability indicators have been developed [39-41]. Standardised reliability indicators of HL1, HL2 and HL3 segments are described in [40], [39] and [41] respectively.

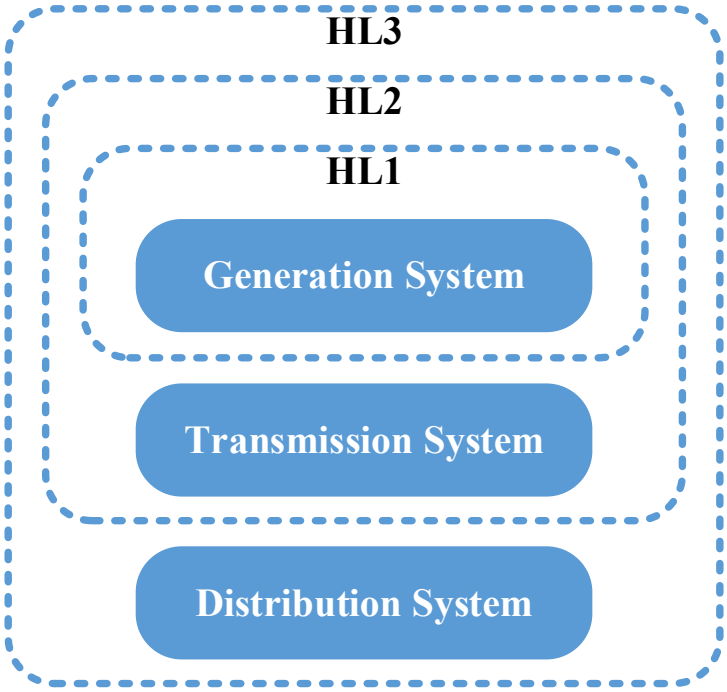


Figure 2.6 An overview of hierarchical levels for power system reliability [2]

2.3.3 Overview of Power System Reliability Studies

The evaluation of power system reliability is a necessary and vital process for transmission, distribution and generation system operations, and it has to be examined from

their deployment planning stage to the present status [42, 43]. There is a large volume of published studies describing the role of reliability indicators power system planning and operations [44-50]. Power systems needs to be evaluated with the perspective of its hierarchy [49, 50]. Power system reliability indicators have been calculated with deterministic methods [44, 48], probabilistic approaches [45, 46, 49, 50], and combination of deterministic and probabilistic aspects [47]. In general, most of the literature has focused on 1) the examination of the some system restrictions on composite power system reliability, 2) new models and system components impacts, 3) planning and optimization techniques on system reliability, 4) computing technique efficacy [51].

Reliability evaluation studies of HL1 segment first were published in the 1930s [52]. Published literature during this period was accepted as pioneering reliability studies [52]. It was suggested in [53] that generation and load demand should be evaluated in a dependent approach. The importance of loss of load [54], and frequency-duration [55, 56] approaches were demonstrated in the context of generation system reliability.

There is also a large volume of published studies describing the role of HL2 segment's reliability evaluation. The reliability research on HL2 segment is still needed and it could assist provision of information on power system planning and operations for decision makers and planners. Most of the studies have used the Monte Carlo and Markov Chain techniques, and also there have been unusual techniques which are applied into reliability evaluation such as the artificial neural network method [57] and game theory [58]. In perspective of system reliability, these implemented methods, especially the Monte Carlo simulation method, have been utilized in identification of critical components of transmission systems [59], and expansion planning of transmission network with its capacity optimization [60].

A considerable amount of literature has been published about the reliability evaluation of distribution systems. These studies are mainly focussed on system operation cost, interruption of generating systems, demand-side status (load shedding and curtailment), impact of system topology and configurations, effect of integration new components etc. Many articles evaluate reliability indicators of HL3 in the context of system operation conditions [61-63]. Each distribution system unit and its size and placement play key roles in distribution system reliability. If planners and decision makers are to ensure high operation standards to customers, they need to examine the system reliability and boost the system to optimum reliability levels [64, 65]. HL3 studies have also considered energy resource variation (dispatchable or non-dispatchable) and energy resource availability. These distributed generation circumstances are a vital part of system restoration and operation continuity of conventional generators as well as renewables [66].

Before the last three decades, the target of most of the power system reliability studies was to do an evaluation that showed the criticality of traditional power system components in composite system levels without considering renewable energy and smart grid technologies. With the integration of these innovative technologies, it has been understood that traditional reliability techniques are inappropriate due to their uncertainty and intermittency [67].

2.4 Power System Reliability Considering Low-Carbon Technologies

Electric power systems are passing from revolutionary low carbon transition that has an essential mission to minimise utilization and deployment of fossil fuel technologies and maximise renewables [68]. In the energy sector, there are various low carbon technologies

available considering either supply-side or demand-side. Such technologies photovoltaics, wind turbines, biomass, heat pumps, electric vehicles are already integrated into power systems. In order to reach ambitious targets of low carbon transition, stakeholders and power system planners would be faced with significant operation and placement challenges [17, 68, 69]. Because of intermittent features of new power resources, load demand and weather uncertainties, and random failures of power assets, power systems are having more operation disturbances, brownouts and blackouts compared to conventional operation time of power systems [70]. As a result of these transitions, there would also be an impact on power system reliability inevitably [71]. Power system operators and planners need to transform traditional reliability assessment approaches and its applications according to standard reliability levels for analysing intermittency and uncertainty of low carbon technologies.

In the next sub-sections, relevant literature of PV powered system and electric heat pumps will be presented with consideration of technology characteristics, working principles, their interactions with power systems.

2.4.1 Electric Heat Pumps

Electric Heat pumps, are globally recognised as low carbon heat generation technology for residential, industrial, and commercial usage of society, are taking heat resources from an outdoor environment such as water, ground and ambient air with auxiliary electricity and injecting heat to indoor environment [72].

Most of the electrically driven heat pumps can be utilized in a reversible approach for heating and cooling load demand of dwelling. Heat pump's specific working principles with its coefficient of performance (COP) characteristics adjust carbon emissions of heat pumps. In this

respect, COP of the electric heat pump, by means of previously determined heating ($Q_{Heating}$) and cooling ($Q_{Cooling}$) demand of dwelling, low (outdoor, T_L) and high (indoor, T_H) temperatures (Kelvin), and input energy demand (W_{input}), can be expressed as following equations [73]:

$$COP = \frac{Q_{Heating}}{W_{input}} = \frac{Q_{Cooling}}{W_{input}} \tag{2.6}$$

$$COP_{ideal} = \frac{T_L}{(T_H - T_L)} + 1.0 \tag{2.7}$$

This promising electrically driven-heat generation technology is mainly divided into three categories according to type of heat source: Air-Source Heat Pump (ASHP), Ground-Source Heat Pump (GSHP), and Water-Source Heat Pump (WSHP). They have been integrated into power systems in many developed and developing countries and their deployment trend will continue to reach significant levels into the power grid due to global carbon emission targets [72, 74]. In case of the United Kingdom, the interest of HP's integration has been re-established and its increment level on energy sector is expected to hit extremely high levels [19, 20]. Especially, air-source heat pumps which will have a significant positive impact on carbon emissions for the UK's 2050 targets [75].

From a technical advantage point of view, heat generation transformation is expected to bring increased flexibility to the system operation on supply-side fluctuations and consumer flexibility on demand-side management [76, 77]. Within the smart grid vision, researchers have carried out heat pump studies in the centre of supply-demand flexibility that is related to demand-side management, demand response and distributed energy resources [72]. HPs are bringing greater level of flexibility and peak demand shaving opportunity to the existing energy networks as a component of demand-side management, which are beneficial for power grid's

reliability and safety [78, 79]. It has been observed that another advantage is in [78] that HPs with possible DSM strategy could reduce electricity bills significantly and help to reduce carbon emissions per dwelling. Except these advantages, these technologies also have a number of serious technical and economic drawbacks to the energy networks and society.

From a technical disadvantage point of view, there is a great deal of literature highlighting challenges experienced by operating HP's [20, 23, 72, 78, 79]. According to [20, 78], it is pointed out that technical issues of HPs that GSHP need a large space in the ground for installation and ASHPs have a number of problems such as noise and inadequate productivity. Moreover, due to cooling load demand is in low consumption level on summer in UK, deployment of these technologies can be affected negatively in consideration of investment. As in [23], increase on load demand at peak time, significant voltage drop, and transformer thermal overloading have been observed and the high penetration level of HPs is applied that can lead to not only hazardous influences on reliability of individual devices on the related energy network. Although most of the literature of heat pump research are associated with smart grid load-generation control management, system optimization-impact analysis and electric heat pump load modelling [77, 80-82], any of these studies do not directly cover reliability issues of heat pumps their related impacts on power systems.

With the consideration of power system reliability, recently published reference [83] represents a stochastic study to investigate optimum placement of air-source heat pumps in power grid and its related reliability issues. The benefit of this study [83] is to demonstrate and analyse uncertainty characteristics of distributed generation with heat pumps in a holistic approach. On the other hand, the study is not composed of detailed component reliability of heat pumps and various heat pump technology consideration [83]. In addition, heat pumps are

only implemented into radial distribution systems, no consideration of ring or meshed system topologies [83].

There is also the Markov chain approach on availability system modelling applied into heat pumps' and other heat generation systems' reliability studies [84-87], but this approach has been utilized in a limited number of literature papers. References [85-87] purpose availability and reliability analysis of different heat generation technologies as well as heat pumps in the context of mechanical system features. Mechanical reliability indicators of ground-source heat pump have been introduced by using Markov transition matrix [87]. Heating system reliability studies [85, 86] are more advance compared to [87]. These two researches [85, 86] are considered as reliability analysis of combined cooling, heating and power systems with the top-down approach. Both of the studies have evaluated the system reliability without considering power system reliability. System elements' configuration is demonstrated in both studies for system availability assessment with Markov chain [85, 86]. The difference between [85] and [86], mechanical availability and reliability evaluation are utilized for maintenance prioritization analysis of system components in [85].

A recently published study [84] examines overall system reliability of heat network with renewable generation in the context of power system reliability. The study evaluates combined cooling, heating and power system in distribution system levels. The study objective is to increase renewable energy generation capacity of power distribution network with utilizing optimum number of heat pump technology [84]. However, there is no consideration of the impact on communication elements of heat pumps on operational system reliability [84]. Together all these studies provide important insights of heat pumps for power systems as well as heat pump characteristics in perspective of power system reliability.

2.4.2 Photovoltaic (PV) Powered Generation Systems

Basically, solar PV can be defined as electricity generation from solar light and is done by direct conversion [88]. PV generation systems have many pros and cons for society. Their advantages are being reliable systems, having a low cost operation and maintenance, clean and free energy resource, having a high level of operational availability during clear weather, eco-friendly, noiseless and decreasing greenhouse gas emission levels for society [88]. Otherwise, auxiliary system availability limitation of PV (evacuated tube collectors for solar thermal PVs) in some markets, high capital cost, large area for instalment and geographical conditions are disadvantages of PV technologies for society [88].

Although this technology has some drawbacks, PVs are accepted as fundamental elements in low carbon transitions, and usage of them are expected to reach high levels [89]. High penetration of PV systems into power network can bring two-way power flow experience, voltage increment, and fluctuations in the power network [17, 90]. These characteristics give a clue to stakeholders that reliability analysis of future energy networks is expecting to be differentiated with existing ones. Because of this transform, new aspects on reliability assessment may play a vital role for integration of PV systems into power grid. According to its capacity level on power grid, PVs can be mainly classified into three categories. These are utility–scale (1-10 MW), medium-scale (10-1000 kW) and small-scale (up to 10 kW) PV systems [17].

The existing literature on PV system reliability is extensive and focuses on many different aspects of PV. Therefore, the literature review of PV systems can be divided into two viewpoints that are fundamental and futuristic aspects of PV systems. The fundamental part of

the literature consist of the impact of PV system configurations, critical elements of PV systems, reliability assessment methods for PV systems and its intermittency impacts. The futuristic aspects of PV systems are composed of cyber-physical components that includes their effect on power system reliability, voltage management scheme of PV systems and the effect of extreme weather conditions.

Due to high intermittency and uncertainty characteristics of PV systems with their internal and external effects, power systems are already facing high risk of disturbances during their operation and planning stage [91-93]. These intermittency characteristics, includes environment humidity and temperature, high-voltage bias and solder bond integrity, are affecting disturbance and interruption rates of PV systems in power grid according to lifetime of PV subsystems and components such as power electronic components significantly [94, 95].

If there is a necessity of consistent electric power with PV systems for critical loads in such telecommunication and medical systems sectors, battery becomes a vital component for PV systems, especially for stand-alone PV systems [95]. Batteries could affect PV system operational reliability during extreme temperatures, but improved life cycle of batteries and their low cost of maintenances could increase overall PV system reliability and minimise PV system operation costs [95].

There has also been great attention on PV system inverters with respect to operational system reliability and they have been accepted as most vulnerable components of PV systems [96-98]. In addition, PV system modules (solar cells), capacitors, and inverter topologies have critical positions during the reliability analysis of PV power systems. These studies [99, 100] are focused on individual component reliability evaluation; nevertheless, composite system

reliability assessment of PV system is limitation in this studies [99, 100]. Some commercially available PV technologies are subject to string topologies with individual independently operation and this approach can be beneficial during the PV system operation due to individual disturbance and interruptions. If there is a fault on a PV string, other PV strings can still continue for PV system operation and generate electricity [101].

Moreover, the configuration of inverters and their internal electronic parts have a huge impact on PV system reliability and generation losses according to [102, 103]. Introducing new smart inverter concepts in direction of autonomous control can decrease energy losses and rise operational reliability of PV systems, but also the system vulnerability can be maximised by their software operations[104]. Solutions for all these problems have been introduced in the direction of voltage management and implementing new equipment into the power grid. However, mitigating the problems with these solutions are probably going to increase PV powered systems' capital and operation costs, which are undesirable for investors and operators [100, 105]. It is clearly shown in previous studies [92, 93, 95, 96, 99-101, 103-105] how performance dependencies of PV systems can reveal reliability issues, nonetheless, these technologies should be deemed by its status from basic component to composite level including transmission and distribution networks during power system reliability assessments.

For composite reliability analysis for PV systems, there have been various methods and techniques introduced. In respect to low carbon technology performance factors, the Monte Carlo and analytical methods have had a significant contribution on assessment of operation reliability of PV systems [101]. Markov chain availability analysis is implemented into a reliability assessment in order to estimate performance metrics with energy yield of PV system including impact of inverter topology [105]. It has a limitation that needs to include and

highlight PV-weather intermittency effects on overall power system reliability [105]. The reliability of PV powered systems with cloudy impacts under weather conditions is evaluated in [106, 107]. Agricultural, residential, commercial and industrial area loads are analysed in direction of reliability performance of PV system within detailed cloudy effects by Markov Chain state transition model [107]. Reference [107] describes that cloudy effects brings huge impacts on PV system operation and reliability when the integration of PV systems into power grid is in high levels. Nevertheless, these two studies are only considered weather conditions and neglected cyber-physical operation of PV system for power system reliability [106, 107].

During the peak time of PV system operations, power system can suffer from voltage fluctuation and high voltage issues due to intermittency and reverse power flow. Because of these problematic statuses, power electronics of PV systems are accepted as the most affected part that is less reliable compared to other parts [94, 95]. Before the effect on inverters, on load tap changer and capacitor banks can be integrated into the power grid in order to mitigate voltage issues with active voltage management. Advantages of voltage control management mechanism for smart grids have been introduced in [108, 109]. Nevertheless, it is indicated that this control mechanism brings extra capital cost for PV system investments by implementing communication infrastructures [108, 109]. According to [109], voltage control schema with PV system can increase power system reliability, in addition, by evolving network characteristics with active voltage control management could also alter PV generation output levels.

With increasing communication infrastructure in power systems, cyber-vulnerability is increased and it is noticed its importance on power system reliability [101]. In general, power system in classic reliability studies is seen as a pure physical system. Though, cyber-physical operation of power system needs to be covered in power system reliability analysis [101]. Many

parts of power systems including PV systems have cyber interactions with system components such as DC-AC or DC-DC converters' and voltage control algorithms, maximum power point trackers, smart inverters etc. [110]. Due to cyber vulnerability characteristics of PV systems, power system reliability as well as power outputs of PV systems can be influenced harmfully. Thus, PV's cyber-physical parts should also be considered during the reliability analysis of PV powered systems.

2.5 Power System Reliability Considering Information and Communication Technologies

With having smarter and automated power grids, the importance of Information and Communications Technologies (ICT) has increased for power system operation and control [110]. With assistance of ICTs on power grid, network operators can keep system operations in a more reliable, secure and steady conditions. For instance, if there is a faulted part during the power system operation, smart automation-control system can open switch and send information about faulty part of the system. Due to these two-way communication capabilities on remote sites in smart grids, ICT devices can encourage attackers to access power system network and lead to interruptions on power system operations. Moreover, attackers provoke brownouts and blackouts by connecting communication network that can result in high societal consequences [111].

Considering the communication network of power systems, there are many subsystems and devices deployed in order to improve power system operations and control. These technologies can be Supervisory Control and Data Acquisition (SCADA), substation automation-control systems, Phasor Measurement Unit (PMU) for transmission level networks,

and Advanced Metering Infrastructure (AMI), Distributed Energy Resources (DER) management system, distribution automation-control systems for distribution level networks [112]. These technologies are mainly integrated for increasing power system performance, observability and interoperability [112]. Besides advantages, it has been observed that they can bring also vulnerabilities on power system operation by opening gates for intruders [35]. According to records [113], forty six cyber-intrusions or cyber incident related failures have occurred and they affected power system utilities and stakeholders in 2015. These harmful events on smart infrastructures of power grids is expected to be increase, and as result of this, decrease operational reliability of power systems. Cyber vulnerabilities can be classified into three domains: application software threats, communication network threats and field device threats [114]. In general, increasing complexity, options (ZigBee, Wi-Fi) and interconnections in ICT components [115], connecting power system ancillary services with external communication links and extensively pervasive internal two-way communication links can bring cyber vulnerabilities for power systems significantly [114]. To maintain reliability of power system within the optimum operation levels, these new technologies and related vulnerabilities should be considered in planning and operation stages of power grids and examined in power system reliability studies.

There have been numerous efforts in the power system reliability assessments that are mainly based on physical system reliability, not including cyber-physical segments of power systems. Power system reliability studies considering physical systems have reviewed in previous sections. This section focusses on cyber-physical system interactions of power system reliability that includes impact analysis of ICTs on power system related to cyber-attack and detection system modelling, setting up virtual cyber-environment on power grids.

In this context, the literature is reviewed under umbrella of power systems reliability-impact studies on cyber-physical systems and it is divided into security study analysis [116-125], adequacy study analysis [126-138] and other impact studies [139-141] as in Figure 2.7. A number of studies have focussed on contingency-oriented reliability assessment [119, 122-125]. In reference [123], intruder is targeted phasor measurement unit (PMU) and the result of cyber intrusion is to have n-1 contingencies in different lines.

In addition, the defensive solution against intruder has been proposed with optimal allocation of PMU and finding PMU criticality levels for the power systems that can prioritize power system operation budget [123]. Generators [124], lines [124] and substations [122, 124, 125] have been considered with multiple failure cases for overall power system operational reliability. In these studies [119, 122, 124, 125], it is suggested that security-oriented reliability analysis on cyber enabled power systems should consider conventional contingency approaches (n-1 and n-2), but also cascading contingencies for composite operational reliability. Following studies performed substation protection analysis [116, 118, 125], cascading failure impact analysis [117, 122, 125], resiliency analysis [121], voltage regulation assessment [120], general failure analysis related to cyber-enabled systems [119].

For these security related assessments, reviewed literature utilized different type of attacks in order to demonstrate cyber-physical system impacts on power system reliability. These are categorised into three types: false data injection attacks [116, 117, 123], coordinated attacks [122, 125] and generalised attacks [118, 121, 122, 124] that represent cyber-attacks without having any categorisations. Most of these studies evaluated power system reliability in perspective of security-orientation and they did not include adequacy analysis or had very limited assessment, except [124]. According to attack-defence model in [124], robustness of

power system is increased against N-1 contingencies with possible cyber-attacks by proposed optimization technique and loss of load is decreased.

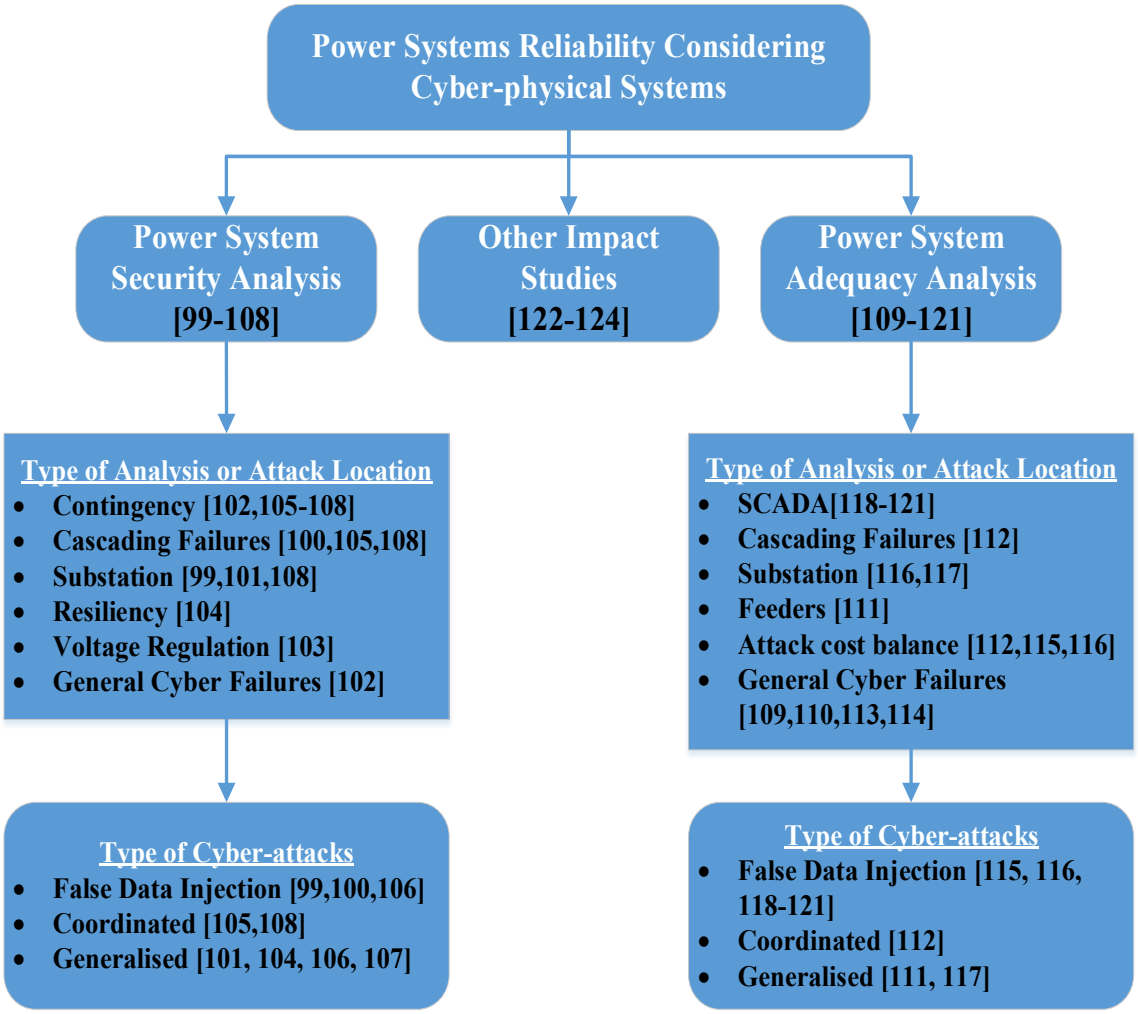


Figure 2.7- A literature overview of power system reliability considering cyber-physical systems

The literature on power system adequacy related to cyber physical system operations has highlighted several aspects and pointed out direct and indirect impacts on power system reliability [126, 127]. The cyber-physical system interaction with power systems and its related general cyber link failures have examined in [126, 127, 130, 131]. Power system direct [127]

and indirect [126] cyber interdependency effects, which include cyber-attacks on power grid applications, cyber-physical system's unreliability, cyber-malfunctioning and cyber-destruction on power system monitoring-protection systems, have considered in power system adequacy analysis. It has been demonstrated that direct and indirect impacts of cyber-physical system interaction with power systems can significantly reduce power system reliability [126, 127]. According to these findings, failure and repair rates of power system applications should be updated for power system reliability assessments. Moreover, references [130, 131] have implemented non-sequential and sequential Monte Carlo simulations for cyber-physical system reliability interaction with power systems. There are only considerations that consists of cyber-dynamic routing, delay, and communication errors and cyber traffic [130, 131]. Such studies [126, 127, 130, 131], however, have not included cyber-attack models and assumed failure-repair rates of some cyber-physical components. In addition, they did not demonstrate cyber-impacts on low carbon technologies and related effects on power system reliability.

A number of studies have examined and highlighted cyber-attacks' impacts on different part of power system applications and components. The impacts of cyber-attacks have evaluated on SCADA [135-138], substations [133, 134], power system feeders [128] and transmission line [129]. In addition, these studies have implemented different type of attacks that are false data injection attacks [132, 133, 135-138], coordinated attacks [129] and generalised attacks [128, 134] for analysing power system adequacy. By means of game theory, attack–defence mechanism have modelled in the most of the literature [135-138]. In general, attack models have considered successful intrusion pathways with time duration of cyber intruders in the system for statistical calculations [135-138]. These mathematical calculations are important to identify time duration of attack process to force system to be in the position of

system outages. Due to unavailability data of cyber-physical system's failure and repair rates, these calculations can be utilized for quantifying statistical frequency of cyber disruptions and interruptions in order to implement into reliability calculations of power systems. It has been already clarified failure and repair rates of traditional power system's components and applications. However, this information is still not clear for cyber-physical system's interactions with power systems and it has been assessed very limited in current power system reliability studies. The main reason can be data unavailability of cyber-physical system interruptions due to lack of experiencing cyber-attacks and being new technologies or being not shared by stakeholders because of national security. This problem keeps up to date for power system reliability.

Cost–budget balance of cyber-security on attack-defence modelling have attracted some researchers in order to reduce operation costs of cyber security of power systems. The main target of these studies is to model optimum defence resources to reduce or limit expenses of power system operation as well as cyber-impacts by analysing of cyber-physical power system reliability [129, 132, 133].

Except these studies [116-138], there are other impact studies has been carried out in the context of cyber-physical system interactive operations [139-141]. The power system state estimation has been evaluated during sparse attacks [141] and false data injection attacks [139]. Reference [141] have examined sparse cyber-attacks in perspective of voltage control with AC power flow. In addition, reference [139] have performed an optimization technique reduce the cost of launching a cyber-attack in power system with lack of power network information. However, it has explored that cyber-intruders can also identify critical cyber-links and cyber-vulnerabilities with incomplete grid information [139]. Therefore, identification of cyber-links

and related cyber-vulnerabilities have been very essential for attackers how to going forward to force the power system outages and minimize power system reliability and operations [140].

2.6 Summary

This chapter presents fundamental concepts of reliability engineering and reviews relevant literature in the context of power systems reliability and its interactions with PV, HPs, and cyber network operations relevant to this research project. Section 2.2 introduces definition of reliability and related concepts for engineering point of view and relevant reliability assessment methods for engineering applications. Section 2.3 presents power system reliability concepts in perspective of traditional approach and reviews necessary literature. Section 2.4 introduces low carbon technologies (PVs and HPs) in the context of power system reliability and explains how these cutting-edge technologies can bring challenges into power grid with pointing out relevant literature. Section 2.5 reviews the relevant power system reliability literature for power system applications considering cyber-physical system interactive operations. It also highlights research gaps on power system reliability considering cyber-physical systems.

In the next chapter, effects of load demand and PV generation modelling on power system reliability will be introduced and assessed without considering cyber-physical system operations.

Chapter 3: Power System Reliability Analysis without Cyber-Physical System Integration

3.1 Introduction

The main aim of this chapter is to analyse power system reliability without considering cyber-physical system integration. The chapter describes how intermittent characteristics of load demand and power generation can affect power system reliability by exemplifying with case studies.

Transformation of traditional power systems into smart power systems has been driven by the deployment of low carbon technologies including photovoltaics (PVs). The uncertain nature of PV generation technology with its high installation level into power grids has been problematic for distribution and transmission system operators. Not only high-level deployment of PV powered technologies but also, load demand of consumers with its probabilistic characteristics has increased the uncertainty pattern of generation-load demand balance for power system operators and planners. With this transformation and complex interaction of intermittent power generation and load demand, there are also effects of two-way communication systems on the evaluation of power system reliability. Before demonstrating the impact of cyber-physical systems on power system reliability, this chapter will present conventional generation adequacy assessment considering PV powered generation with influence of consumer load demand.

Some sections of this chapter are prepared from the reference [1] of which the first author is the author of this thesis. This publication's case studies and reliability assessment procedure have been produced from the research in this chapter. In [1], the first author introduced the innovative concepts and ideas of PV generation profile linearization and developed the framework of power system reliability evaluation, related simulations and case studies. The second author mainly contributed on the methodology of load and PV generation profile linearization. The third author designed PV generation model.

In the following sections of this chapter, the importance of load and generation modelling is presented aligning to a power system adequacy assessment. Then, the load and generation models applied to the case studies in this chapter are presented. It is also extended with the traditional conceptual framework for power system reliability assessment without considering cyber-physical system interactions. In the final part of this chapter, case study is presented to demonstrate the intermittent impacts of PV generation and consumer load demand profiles on reliability of a power system.

3.2 Load and Generation Profile Modelling

3.2.1 Load Modelling

Load modelling has a substantial effect on power system evaluation studies. With low carbon transition, load modelling has received a critical attention from different areas in power systems including distributed generation integration, demand-side management and in particular from power system planning, operation and control. The uncertainty of the load demand is one of the most common concerns for power system operators and planners. Stochastic characteristics of load demand and its physical behaviour are directly and indirectly

linked with power system reliability studies. The diversity of load elements, variation on load consumption time and weather are increasing challenges on load demand approximation and forecasting in order to utilize load profiles in any power system study assessments in this new era of emerging power grids [142]. There are many approaches for designing load demand profiles, but load modelling can be classified into specific component-based (hypothetical approach with theory-based) and measurement-based load modelling [142]. Notably measurement-based load models are more suitable compared to component-based ones due to its feature that compromises real time consumption data measurements with instantaneous load demand behaviour from meters [142]. Resulting from this characteristic, any power system reliability assessments can be done for the increase accuracy and robustness.

Not only stochastic patterns of load profiles but also the total number data points of the temporal resolution of load demand curves are essential for power system reliability studies. Load curve synthesising with fewer steps could potentially deliver smaller computational times for the reliability assessment process, allowing the power system operation and control mechanisms to act fast. However, load curves with less resolution can result reduced the accuracy of sensitive load points and therefore a solid power system reliability indices may not be delivered for the effective utilization. Because of these reasons, the number of steps needed in load demand curves and load profiles' stochastic pattern should be carefully considered for power system reliability analysis.

3.2.1.1 Original and Linearised Load profiles

Due to the complexity of high volume load data, one of the objectives of the linearisation concept applied on load profiles is to reduce non-linearity and complexity of original load

profiles in order to be used in any power system analysis without losing accuracy and robustness [143, 144]. The load demand data in this chapter is from the 'ISSDA CER' smart metering dataset [145]. This load data represents almost 6000 Irish residential and business consumers' load consumption records during the period 2009 to 2010 and original dataset of load demand was measured with 30 minutes resolution [143]. Figure 3.1 demonstrates average load demand profile of consumers' data measurements used in this chapter [143].

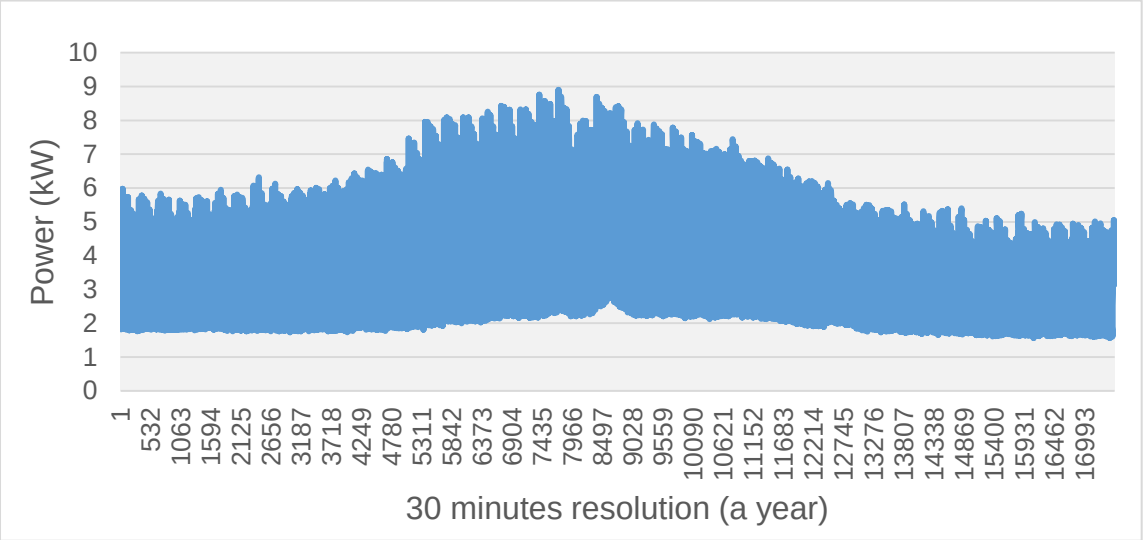


Figure 3.1 A Line diagram of Average Aggregated Load Profile of Consumers' Data Records [1]

To diminish the amount of data usage from smart meters and the intricacy of the utilized data, consumers' load demand data was implemented into the extended k-means clustering algorithm for the linearization process [1]. Thirty-eight load demand data clusters were generated and each profile was composed of 17520 data measurement records [1]. The effect of linearization process of load profiles on power system reliability is examined with case studies in following sections of this chapter. The linearisation process is aimed to reduce the complexity of utilized data with optimizing the energy capture between original (raw) and

linearized load demand profiles [1, 143]. An example of these load profiles has been demonstrated in Figure 3.2. The red dotted line and black solid line represent a section of linearized load and original demand profiles, respectively in Figure 3.2 [1].

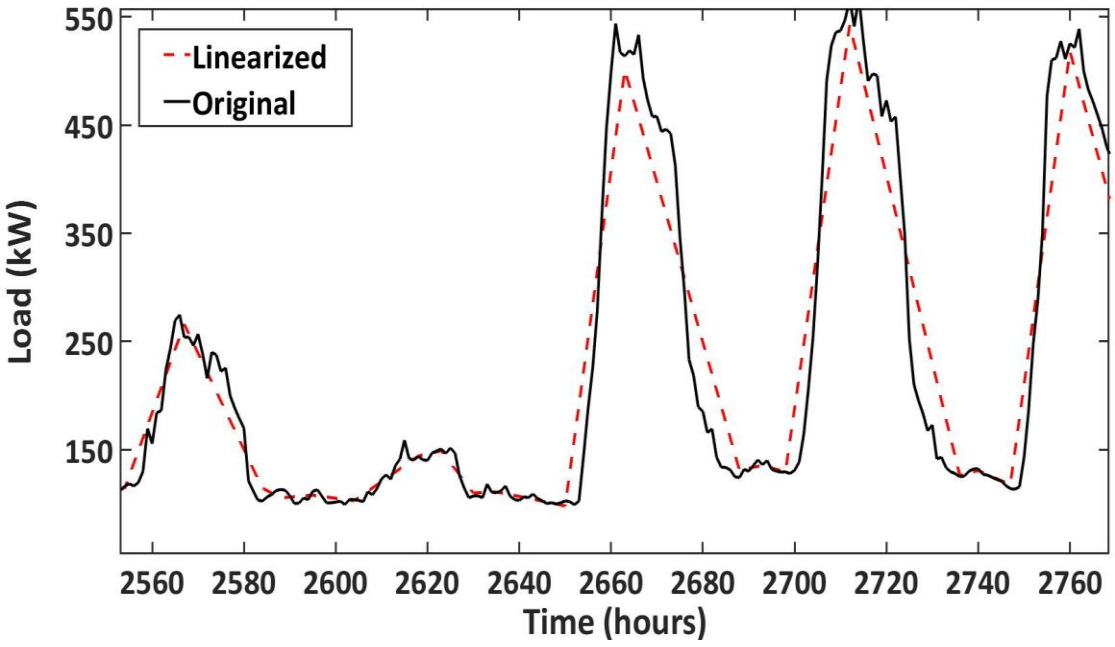


Figure 3.2 A part of linearized (red dotted line) and raw (black solid line) load profiles [1]

3.2.2 PV Generation Modelling

As similar to the load modelling, generation modelling has an important effect on power system planning, operation and control studies. Due to global warming and climate change effects, renewable power generation profile modelling, particularly on solar PVs generation, has received a considerable attention from system and project planners. This increase in popularity from power utilities is expected to increase because of high deployment projection of solar PV capacity all around world. Since solar PV has an intermittent nature and heavily

relies on geographical and weather conditions, its integration at high capacity level into power system causes more difficulties. Power utilities have already been faced with many challenges related to PV generation such as in power system stability, security, reliability and so on. The modelling of PV generation is subject to its components, design and size characteristics. In order to do a robust analysis of PV generation model, power utilities and stakeholders should take into account all the features of solar PVs in its model design process [146].

The utilized PV generation profile model in this chapter has considered PV system operating temperature, solar irradiance and shading with climate conditions for a specific region [147]. The geographical location for PV generation was selected as Belfast [1].

3.2.2.1 Original and Linearized PV generation profiles

In this chapter, the below PV generation profile is utilized which also incorporates the influences of air temperature and solar insolation [1, 147]. Before the linearization process of PV generation profiles, hourly PV generation profiles were transformed into half hourly PV generation profiles by interpolation. Before the linearization process of PV generation profiles, hourly PV generation profiles were transformed into half hourly PV generation profiles by interpolation. A half hourly PV generation profile for a year is demonstrated in Figure 3.3. With the same methodology implemented into load profile simulation, the linearization process was also applied into original PV generation profiles in order to diminish the complexity of them. PV generation profiles has been taken from reference [1]. As in Figure 3.4, an executed sample of the PV generation profile is demonstrated with its linearised and original versions [1, 143].

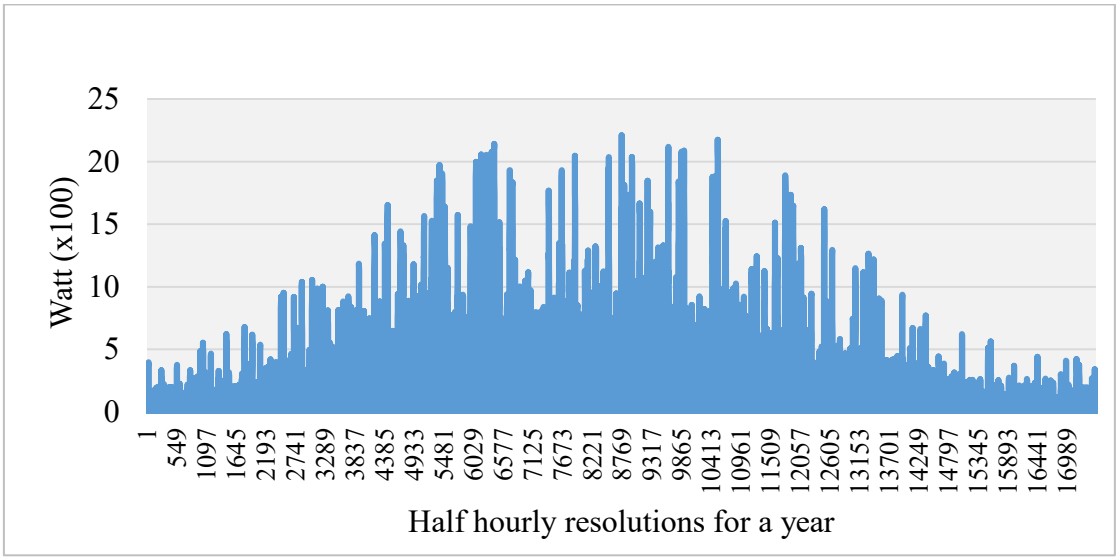


Figure 3.3 An example PV Generation Profile for Belfast City (annual) [1]

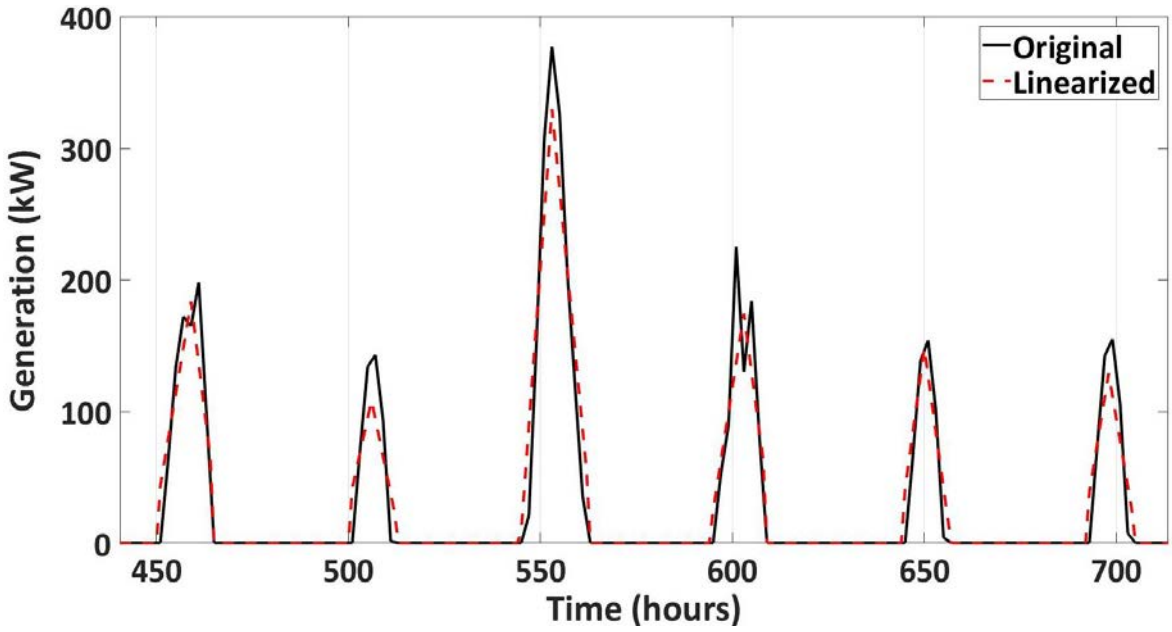


Figure 3.4 A part of linearised (red dotted) and raw (black solid) PV generation profiles [1]

3.3 Methodology for Power System Reliability Assessment without Considering Cyber-physical System Integration

Reliability evaluation of power systems is dependent on analysing all credible states of a system's elements considering their basic and complex configurations. Traditional power system reliability evaluation considers a failure model, load model, generation model, the design of the system state and statistical analysis in order to generate reliability indices of power systems. The failure-repair models can demonstrate behaviour of the system elements during fails or repairs with a specific time duration for each event. The failure model also includes how often these failure-repair events might occur in a specific time period. As previously highlighted, load models can be composed of load demand of consumers or forecasted load demand scenarios. In addition, generation models are necessary to supply the system's load demand which is generated by load models. These failure, load and generation models can help to design the system states under specific conditions. After defining the system states, a statistical calculation can be made to calculate the reliability index with a probabilistic approach. A probabilistic model of each component of a power system is subject to failure rate and repair time calculations. These calculations depend on the system elements' availability and unavailability status [2].

In order to achieve the aim of the power systems, which is to supply the required power within a secure, economic and continuous way, the composite power system reliability analysis is required to evaluate all credible system conditions within the global and local limits of power systems. However, fulfilling the criteria of the power system reliability analysis can holistically be challenging for power utilities and power system planners due to the computational cost and

time of the analysis and the forecasting accuracy of available generation and load demands [1]. With respect to these challenges, the process of power system reliability needs to be carefully considered from all proponents with possible scenarios for power system planning studies.

3.3.1 The Procedure of Power System Reliability Assessment

The procedure steps of power system reliability evaluation for this chapter is demonstrated in Figure 3.5 [1] and power system reliability index calculation agenda is expressed as following steps:

1. Define and extract power system load and generation profiles from [1] and apply to the system.
2. Initialize the load demand and PV generation profile characteristics.
3. Determine reliability data for each power system component (transformers, power lines, busbars, etc.).
4. Select randomly the system state based on non-sequential Monte Carlo simulation.
5. Perform the power flow considering power balance with global voltage limits.
6. Converge the computation, assess the system state with the system overloading and satisfy power flow. If not, go to step (4).
7. Update statistics for the load curtailments of each sampled system state.
8. Finally, use a globally known reliability indicator for power systems, Expected Energy Not Supplied (EENS), is estimated and reliability index is reported.

The network topology of IEEE RTS79 [148] was utilized for this study. The network system topology is composed of 24 substations and 32 traditional generating units. The network's branch, power line, transformer, generator unit and reliability data were gathered

from [148]. The IEEE RTS79 reliability test system is slightly adjusted according to each case study and these changes are presented in the result of each case study.

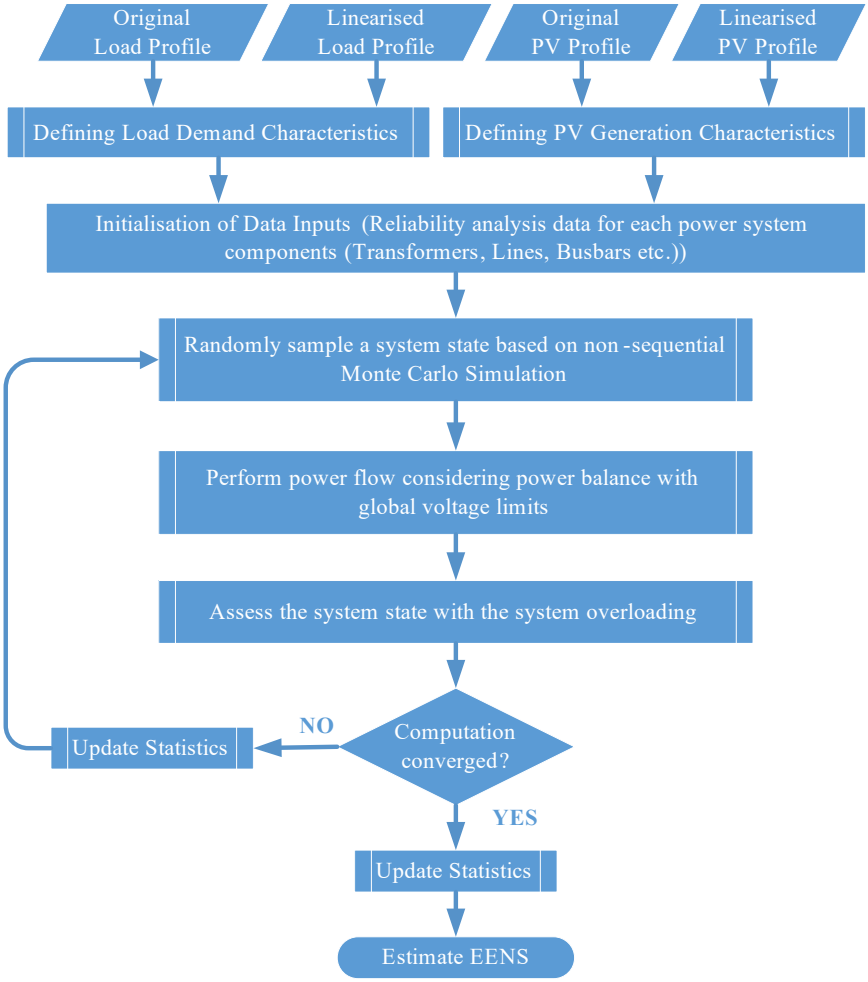


Figure 3.5 The Flowchart Diagram of Power System Reliability Evaluation Procedure [1]

3.4 Case Studies and Analysis

In order to demonstrate the effects of load demand curves and PV generation curves on power system reliability analysis, different case studies are examined with relevant scenarios in this chapter. These case studies do not only evaluate power curves of supply and demand,

but also evaluate their intermittent characteristics within the context of power system reliability evaluation. In this chapter, load flow analysis is carried out on DigSILENT platform using AC Newton-Raphson technique, and utilised load-generation profiles are modelled on MATLAB and then interfaced.

Case study 1 assess the impact of different types of load demand with increasing nominal load demand of the power system exclusively. The case study 2 investigates intermittency impacts of PV power generation on power system reliability. Centralised and distributed PV power generation are applied on the IEEE RTS79 reliability test system. In case study 3, impacts of PV generating units' installation capacity on the reliability performance is evaluated with different deployment methods.

3.4.1 Case Study 1: Impact of Load Demand on Power System Reliability

The aim of the case study 1 is to assess impacts of consumers' load demand data on the power grid. The study 1 analyses the intermittency of load demand characteristics through the calculation of reliability indices of a power system. The linearised load demand and original load demand were applied on to 13 load buses of IEEE RTS79. These 13 load points were chosen randomly that selected in order to connect load demand of consumers. In order to perform a robust analysis, the original loads of the proposed power network were removed from 13 load buses. Instead of base case load demands of them, 38 load demand clusters were implemented in each load bus. After the base case was simulated, the magnitude of the load was incremental in steps of the base load level in each scenario until reaching the maximum load scaling level of the power system. Comparison of the influence of linearised load demand data and original load demand data is presented in Figure 3.6 [1].

As can be seen from Figure 3.6, the reliability indices show moderate growth in both linearised load demand and original load demand cases. The growth of EENS is started from the 1st load scaling factor until 7th load scaling factor. With increase steps on x axis of Figure 3.6, the profile of linearised load demand has slightly associated with greater EENS values

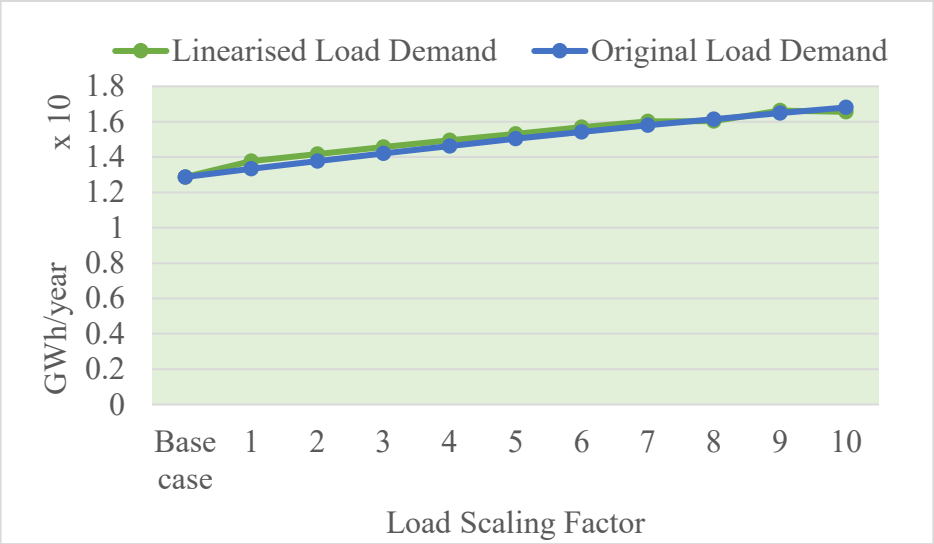


Figure 3.6 A Line chart of EENS considering with the scaling factor of different load demands [1]

compared to original load demand profiles due to design of load profiles. Afterwards, the behaviour of EENS fluctuates until the maximum load capacity level and its value is reached almost 17 GWh/year in both cases. These fluctuations can be associated with the design error of linearised load profiles. Thus, the highest error between load demand curves is computed as 1.33% [1].

As a result, two outcomes can be drawn from the results. First, the selection of load demand curves can play a key role in the robustness of reliability analysis. Second, a small intermittency on demand profiles of 6000 consumers can result in a considerable impact on the

EENS in parallel with the reliable operating status of power systems. This could mislead system operators on demand-generation balance scheduling and might increase the electricity cost due to the unavailability of cost-effective generators [1].

3.4.2 Case Study 2: Effects of PV Power Generation on Power System Reliability

One of the objectives of the case study 2 is to investigate how intermittent PV generation affects power system reliability. In order to evaluate uncertainty impacts of PV power generation on the power system reliability analysis, linearised PV profile curves and original PV generation profile curves were implemented while considering two generation deployment methods (centralised and distributed generation) [1].

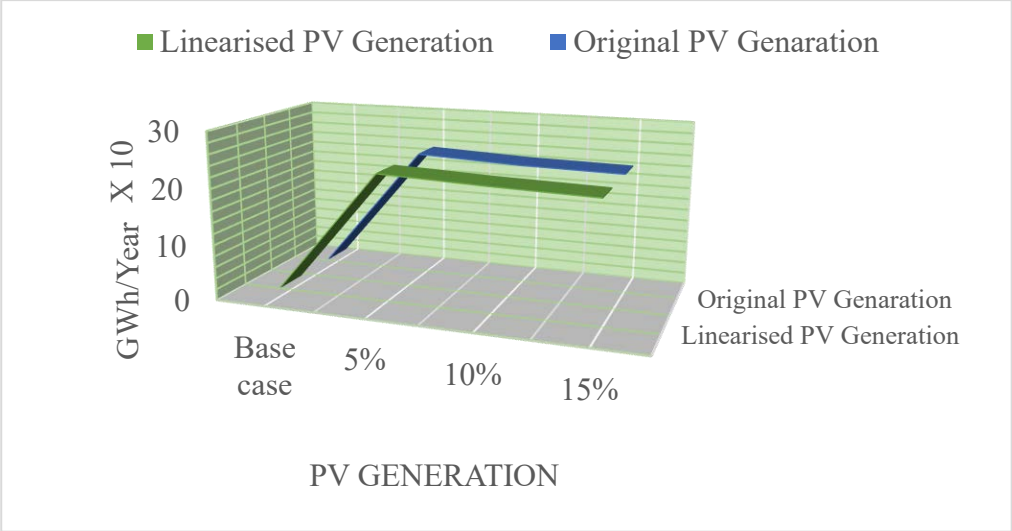


Figure 3.7 A line chart of EENS for Centralised implementation of PV generating unit [1]

Substation 7, and substation 4, 5, 6, 7, 8 are chosen for the centralised and the distributed PV integration scenario nodes, respectively. The total active power load capacity of the IEEE RTS79 is as 2850 MW. As a result, the nominal installed capacity of PV power generation is set approximately as 5 % of the total load capacity, which is 142 MW [1].

To analyse the correlation between original PV generation and linearised PV generation, same generation profiles were used in both scenarios. The installed capacity of the PV generating unit is increased with 5% of the total load demand and this increment is expected to continue as far as the power system is within the voltage limits. Figure 3.7 presents EENS merits of the power network with the centralised implementation of PV generating unit. Figure 3.7 reveals that there has been a sharp increase on EENS from the base case until 5% of installed capacity PV generation. The sharp increase on EENS is unexpected and EENS should not be escalated if there is an increment on power generation. It is due to the location of PV generator in the system. This result reveals that substation 7 has a critical importance for PV generator connections [1].

When the installed capacity of PV generation is increased from 5% till 15%, EENS seems to be levelled off. In reality, EENS diminish steadily but, EENS varies with 0.001% - 0.003% until reaching 15% of PV generating unit capacity. This reaction of EENS may be because there is no either new growth in load demand or need of generation that shows the generation capacity is adequate for the test system. It is also apparent from Figure 3.7 that centralised PV generation capacity is reached up to around 15 % generation capacity limit in both linearized and original PV generation profiles. Power system is expected to have a collapse in operation as a consequence of reaching centralised PV generation limits. Installed PV generation capacity for linearised PV generation reaches around 13.25 %. On the other hand, original PV generation capacity is limited with 11.9 % of base case capacity [1]. These PV generation limits appear because the test system reaches operational capacity limits. The realisation of different PV generation capacity limits is as a result of the disparity on the profile volatility, and the creation error between linearised and original generation profiles.

Similarly, Figure 3.8 shows that there has been a steep rise on EENS value from the base case PV generation till 5 % capacity level of PV generation due to the criticality of PV generator location. Although PV generation capacity increases up to 25% of base case levels,

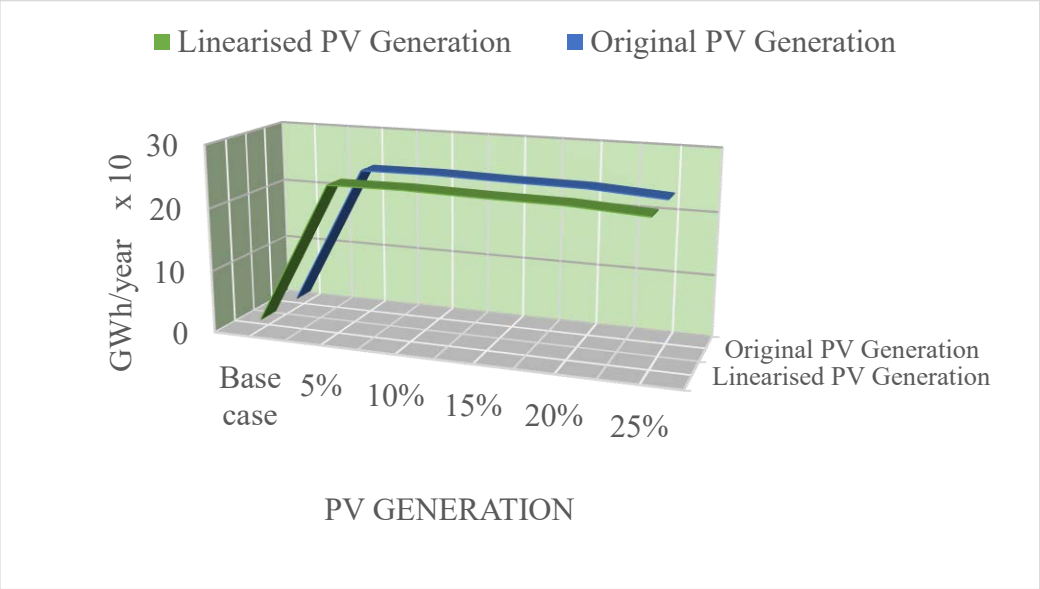


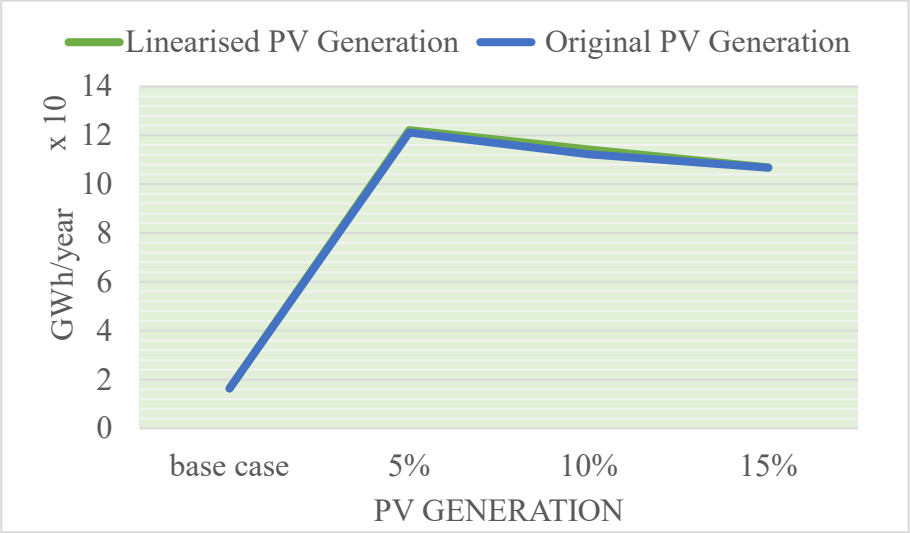
Figure 3.8 A line chart of EENS for distributed implementation of PV generating unit [1]

EENS mainly seems to be remained constant according to Figure 3.8. In fact, EENS declines very slowly at the first until up to 20% of base case levels of PV generation and EENS changes with portion of 0.0012% -0.002 %. Following that, the decrease on EENS between 20% and 25% of base case levels of PV generation can be seen more clearly and it is 0.1%. One reason why EENS has this reaction that the electricity generation is sufficient enough for local part of test system. It is declined owing to the topology of test system. Location of PV generating unit has been an important factor for EENS changes in this study [1].

3.4.3 Case Study 3: Impacts of Load Demand versus PV Installation Capacity on Power System Reliability

The objective of the case study 3 is to investigate what the PV generation capacity limits are when the load demand capacity is in its maximum and minimum levels.

a.



b.

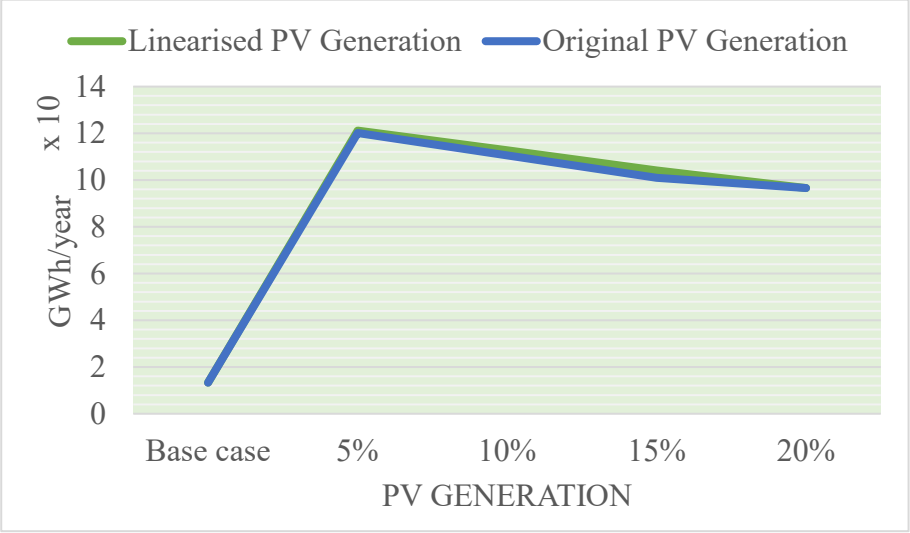


Figure 3.9 Line charts of EENS for Centralised PV generation considering Load capacity a. Maximum Load Capacity, b. Minimum Load Capacity [1]

As similar to the case study 1, the capacity of load also increases in the substations for case study 3. PV systems are integrated as centralised and decentralised. The results of case study 3 for centralised integration scenario are shown in Figure 3.9.What is interesting in this scenario (in Figure 3.9) for the integration of centralised PV generation systems is that the general pattern of EENS has increased sharply resulting from the system topology (the criticality of bus 7). EENS has gradually declined stemming from new PV generators till reaching the capacity limits of their installation in the test system. In addition, both cases of PV generation profiles have behaved in a similar pattern, except PV integration capacity level ranges which ranged between 10 % and 15 %, resulting from the design of PV generation profiles. According to Figure 3.9-a, there has been a slight difference in between both PV generation profiles due to the volatility between generation profiles [1].

With implementing maximum load scaling factor in Figure 3.9-a, the capacity limit of PV generating unit integration into the power grid is given 14.75 % and 13.15 % of the base case for linearised and original PV generation profiles, respectively (Table 3.1). As in Figure 3.9-b, the system installation capacity limits for linearized and original PV generation concepts are also 19.75 % and 17.5 % of base case capacity accordingly (Table 3.1). These variations mainly owing to the design error between PV generation profiles [1].

As a consequence, minimum load scaling factor is more favourable for implementing PV generators compared to maximum load scaling factor, and the location of load in the test system could be another influencing factor for the occurrence of higher penetration of PV generation with minimum load scaling factor.

Table 3.1 Comparison of linearised PV and original PV profiles on the system reliability [1]

Minimum Load Capacity				Maximum Load Capacity		
Centralised Integration	EENS (MWh/year)	PV Capacity Limit (%)	Disparity Rate (%)	EENS (MWh/year)	PV Capacity Limit (%)	Disparity Rate (%)
Linearised PV Profile	96570.22	19.75	2.25	106832.619	14.75	1.6
Original PV Profile	96608.266	17.5		106725.494	13.15	

Furthermore, the results of distributed PV generation under maximum loading conditions are presented in Figure 3.10. Implemented PV generation capacity in each bus is 5 % of nominal total load of the power grid for this scenario. The value of the reliability indicator (EENS) remained steady until the connection of the PV generator in bus 7. It can be clearly seen in Figure 3.10 that EENS is significantly escalated when the PV generator is connected to bus 7. This reaction of EENS can justify the criticality of the substation 7 and validates the reason of changes due to the topology of power system. EENS also varies between linearised and original PV generation profiles.

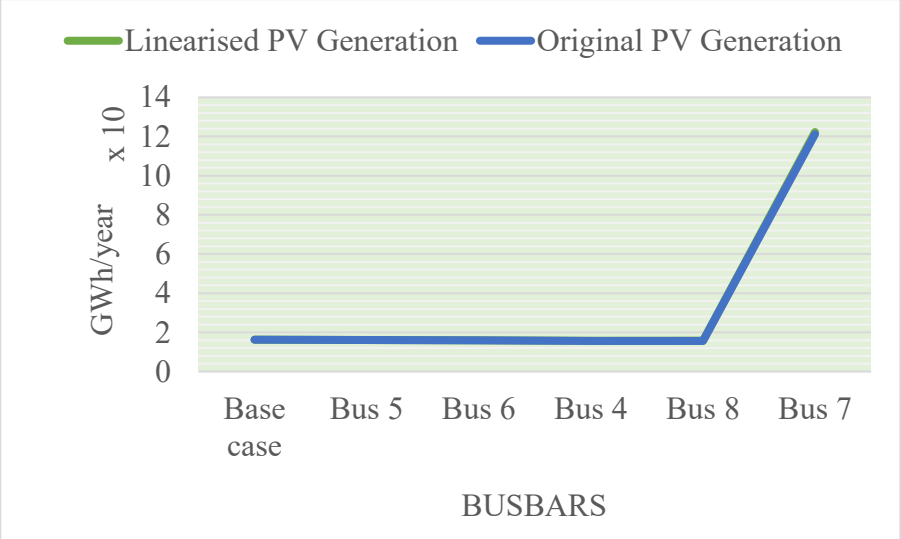


Figure 3.10 Distributed PV generation under Maximum Loading Condition [1]

Although the variation of EENS is limited between the linearised and original PV generation profiles, linearised profiles can be advantageous when less volatility and complexity are necessity for the analysis [1].

3.4.4 Discussion

This chapter presented the general effects of load demand profiles and PV power generation curves on power system reliability assessment without considering cyber-physical system integration. Most of the current researches on power system reliability are linked to the reliability of the system with data complexity, accuracy, efficiency and the computing time the analysis. When the load demand and generation profile curves have created with small number of data points, the calculation accuracy of reliability index can be reduced compared to actual load demand and generation models but, this approach can reduce the processing time of the assessment that can be effective to fast responses. On the other hand, the calculation accuracy of reliability index can be increased if the profiling is designed with large data points, though it can expand the level of data complexity and the processing time of the assessment. Thus, load demand and generation profile curves have a critical role to evaluate power system reliability.

Case study 1 and 2 confirm that incorporating consumers' and prosumers' generalised pattern characteristics can be effective for power system reliability analysis due to the calculation accuracy. It can diminish the work load of computers with less data usage on power system analysis. Therefore, these might affect the processing time of power system analysis positively, when there is a high-level of work load on analysis. Not only the volatility features, but also the system topology and the location of PV generating units have a significant effect on their installed generation capacity limits in power grid. Results show that it does not

necessarily mean maximum load capacity can cause higher penetration levels of PV generating unit. The proposed scenarios also highlight that composite power system reliability analysis is sensitive to changes even if they are small changes in load demand and PV generation curves.

Case study 3 demonstrates the impact of PV generation with different load conditions and presents power system generation capacity limits under different integration methods. Minimum load scaling factor is more promising for implementing PV generators compared to maximum load scaling factor. Furthermore, the loading conditions of power lines connected with bus 7 affects PV generation capacity limits. Critical buses have a key role in increasing PV penetration levels. This indicates also the importance of PV generating unit locations in power system reliability analysis.

3.5 Summary

This chapter presents the procedure of power system reliability analysis and is exemplifing with case studies that show the impact of PV generation and load demand curves on power system reliability. Case studies point out that the details of demand and generation curves play a vital role on power system reliability assessment. They could affect the processing time of the analysis as well as the accuracy of the analysis.

However, these case studies do not consider the analysis of cyber-physical system integration and its impacts on power system reliability, which are going to be evaluated in the next chapter of this thesis.

Chapter 4: Power System Reliability Analysis with Cyber-Physical Interactive Operations of PV Systems

4.1 Introduction

Information and communication technologies (ICT's) are revolutionising the way that power grid systems work, moving from conventional power applications toward intelligent and carbon-free technologies. There is no doubt that ICTs' interactivity can affect the performance of power systems. Since the interactions of traditional power systems with ICTs have been limited, classic power system reliability studies have not considered the effects and performance of ICTs, and these should be taken in the evaluations.

The main objective of this chapter is to evaluate power system reliability with cyber-physical interactive operations of PV generating units. Moreover, this chapter was designed to investigate the effects of the integration of cyber-physical systems in power grids. In order to do so, an analysis framework for the availability and unavailability of the ICTs' components is proposed. Relevant case studies are presented by performing the integrated environment of the cyber-physical system in the IEEE RTS79 and Roy Billinton Test System (RBTS).

Some sections of this chapter are prepared from the reference [3]. This publication's case studies and reliability evaluation framework have been produced from the research in this chapter. In [3], the first author mainly contributed to the innovative procedure of the power

system reliability evaluation, the framework of the cyber-physical system interactive operations, related simulations and case studies.

This chapter is structured with the following sections. Relevant research work related to cyber-physical system operations is given with the research problem in subsection 4.1.1. In section 4.2, the mathematical framework of cyber-physical interactive operations considering PV generation systems is proposed with the power system reliability procedure. In section 4.3, the cyber-physical system interactive operation of PV systems is exemplified using case studies and their results are analysed. Following this, section 4.4 is a summary of the research work that has been presented in this chapter.

4.1.1 Status Quo of the Research Problem

Power system reliability analysis is the heart of the understanding of power system planning and operational performances. One of the dominant generation technologies of the energy sector, low-carbon technologies such as solar PV, is reshaping power grids. The deployment plan of PV technologies into power networks needs a detailed reliability evaluation to sustain a secure and reliable power delivery. It is mentioned in Chapter 2 that the existing literature on PV powered system reliability is extensive and focuses particularly on component-based reliability; however, there is limited involvement of the impacts of the cyber-physical systems with PV generating units.

According to the National Institute of Standards and Technology (NIST), cyber-physical systems (CPS) can be defined as intelligent systems that consist of structured interactive operational networks of physical and computing elements [149].With the two-way communication characteristics of cyber-physical systems, power systems are becoming smarter

and more flexible. However, cyber-physical systems can also bring additional vulnerabilities resulting from increasing level of digital complexity with attack surfaces in power systems.

There is a relatively small body of literature that is concerned with cyber threats on PV power generation systems [150-152] and there is no direct consideration of the evaluation of power system reliability with cyber-physical system operation of PV systems. Moreover, there have not been any real cases reported where cyber-attacks have affected PV generating units. However, these studies [150-152] have demonstrated that cyber-attacks are expected to impact on the reliability performance of the PV generation systems in the power grid.

In [152], it is presented that some components of PV power plants are more likely to be exposed to cyber malfunctions and threats. The map of cyber-physical system risk management for PV power generating unit is presented according to PV system components and stakeholders. Reference [152] also analyses vulnerabilities and attack vectors related to PV power generation. It highlights that the specific subsystems of PV plant are vulnerable to cyber-attacks within the information security triad (integrity, confidentiality and availability)[152]. However, this study remains unfulfilled because of limited analysis on quantification of system vulnerabilities, and lack of numerical explanations of threat effects.

On the other hand, Liu et al. have quantified the PV system's performance, overall system's risk levels and monetary risks when there are cyber-physical incidents in a real micro-grid test case. The effects of cyber-attacks on the operation and controls of PV systems are also introduced with their operational management characteristics and under related communication protocols. Although it incorporates cyber-operational failures of the micro grid, the study does not directly exemplifying the effects of cyber-attacks on the PV systems [151].

As the importance of communication protocols is noted in [151], there is a universal standard, IEC 61850, which defines core communication protocols for electric power system automation. This standardises the communication road map of low-carbon technologies, their related components and protocols during power system operations.[153]

According to [150], IEC 61850 is greatly anticipated to dominate communication services of distributed energy resources, especially PV generating units. In order to analyse the potential capability of cyber-attacks on PV inverters, this research study was performed with a test bed utilizing real PV components and communication tools. It is clearly shown that cyber-attacks can intrude and diminish the performance and output of PV generation. In addition, it is interesting that a cyber-attack was able to shut down the PV system operation without the knowledge of SCADA operations. It highlights the importance of IEC 61850 for PV generation systems [150].

As can be clearly seen in previously published literature [150-152], there is a limited consideration on power system reliability assessments of PV systems under cyber-physical operations. The main question of this chapter is how would all stakeholders of DERs be affected by cyber-malfunction and cyber-intruders in context of power system reliability?

4.2 The Mathematical Framework of Cyber-Physical Interactive Operations Considering PV Generating Units

One of the important aspects of power system adequacy analysis for any system is to understand the relationship between targeted system and its network configuration. This section

presents the reliability concept methodology of cyber-physical interactive operation of PV generation systems considering its network model.

4.2.1 Reliability Analysis Procedure of PV Systems

Power systems are composed of a great deal of sub-units and systems that contain power generation components and power delivery elements connected with serial, parallel or meshed network arrangements. Similarly, PV generation units also include these network

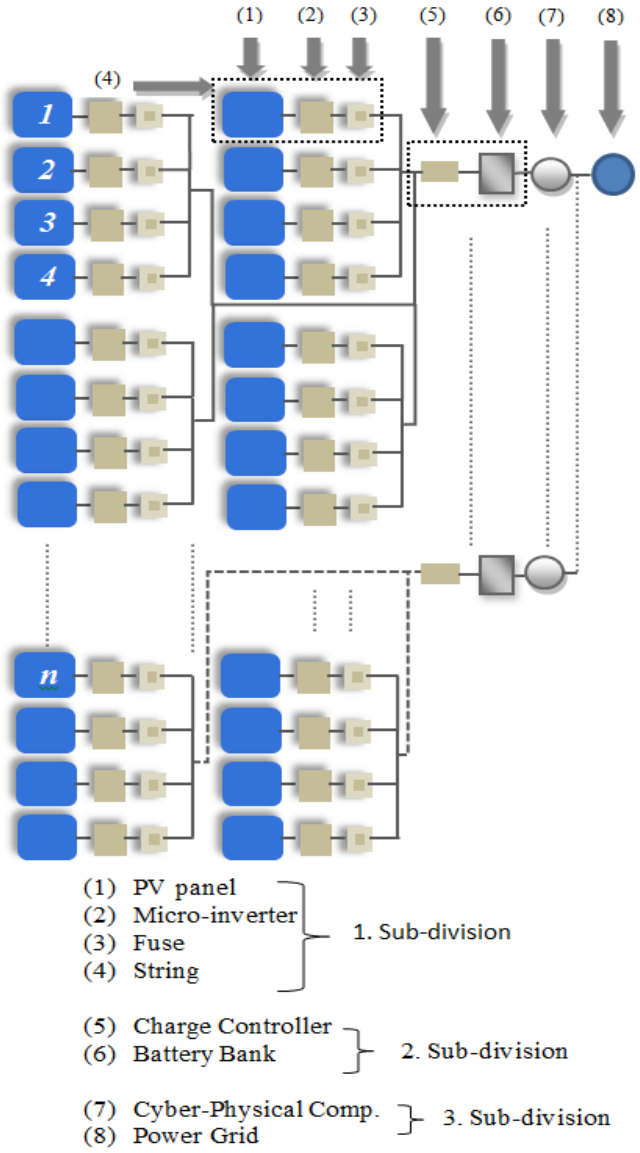


Figure 4.1. A block diagram of PV generating units with cyber-physical systems [3]

configurations according to its deployment location and technological constraints. In order to perform a solid reliability analysis of PV generation units in power grid, the network configurations of PV systems with its components as a serial or parallel has pivotal functions. Thus, the network configuration of PV generation units is presented as in Figure 4.1 [3].

As a generic method, a two-state Markov chain model is implemented in failure process for this study. The operation states of the PV system components are defined as operating (Up) and non-operating (Down). The operation process can be clearly seen in Figure 4.2.

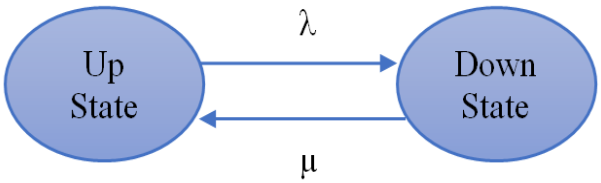


Figure 4.2 A single block diagram of Markov chain operation[3]

The PV system network configuration is arranged with three sub-divisions as in Figure 4.1. The 1st sub-division consists of a PV panel, a micro-inverter, and a fuse as a serial configured unit. Also, this division represents a PV string. There are n-independent numbers of parallel strings that are linked with n-independent of 2nd sub-divisions. The 2nd sub-division is composed of a charge controller with a battery bank as a serial. Serially connected these two sub-divisions are also connected to 3rd sub-division in a series order. It comprises of cyber-physical system components [3].

$$\frac{U}{A} = \frac{P_f}{P_r} = \frac{\lambda_{System}}{\mu_{System}} \Longrightarrow \lambda_{System} = \mu_{System} \times P_f \times P_r^{-1} \quad (4.1)$$

In order to compute composite failure and repair rates of sub-divisions of PV generating unit, the balance equation (4.1) is produced from [26], and availability (A) and unavailability (U) indices of the system are expressed with $(\lambda_{System}, \mu_{System})$ and (P_f, P_r) that represent failure-repair rates of the system and the failure-repair state probabilities of the system respectively [3].

$$P_r^{MI} = \prod_t^n \left(\frac{\mu_{Panel}^t}{\lambda_{Panel}^t + \mu_{Panel}^t}\right) \times \left(\frac{\mu_{MI}}{\lambda_{MI}+\mu_{MI}}\right) \times \left(\frac{\mu_F}{\lambda_F+\mu_F}\right) \qquad t: 1,2,3, \dots, n \tag{4.2}$$

$$P_f^{MI} = 1 - \prod_t^n \left(\frac{\mu_{Panel}^t}{\lambda_{Panel}^t + \mu_{Panel}^t}\right) \times \left(\frac{\mu_{MI}}{\lambda_{MI}+\mu_{MI}}\right) \times \left(\frac{\mu_F}{\lambda_F+\mu_F}\right) \quad t: 1,2,3, \dots, n \tag{4.3}$$

$$\lambda_{String_t}^{MI} = \sum_t^n \lambda_{Panel}^t + (\lambda_{MI} + \lambda_F) \qquad t: 1,2,3, \dots, n \tag{4.4}$$

$$\mu_{String_t}^{MI} = P_r^{MI} \times \lambda_{String_t}^{MI} \times \left(P_f^{MI}\right)^{-1} \tag{4.5}$$

For computing the composite failure and repair rates of 1st string as serially configured, 4.2 - 4.5 equations are utilized. Equations 4.2 and 4.3 calculate the failure-repair state probabilities of the PV string (P_f^{MI}, P_r^{MI}) with the failure-repair rates of PV panel $(\lambda_{Panel}^t, \mu_{Panel}^t)$ micro-inverter (λ_{MI}, μ_{MI}) and fuse (λ_F, μ_F). Given failure-repair rates of components and the state probabilities, the failure and repair rates of 1st string $(\lambda_{String_t}^{MI}, \mu_{String_t}^{MI})$ are calculated with equations 4.4 - 4.5 [3].

$$P_{r_{String}}^{MI} = 1 - \prod_t^n \left(\frac{\lambda_{String_t}^{MI}}{\lambda_{String_t}^{MI} + \mu_{String_t}^{MI}}\right) \qquad t: 1,2,3, \dots, n \tag{4.6}$$

$$P_{f_{String}}^{MI} = \prod_t^n \left(\frac{\lambda_{String_t}^{MI}}{\lambda_{String_t}^{MI} + \mu_{String_t}^{MI}}\right) \qquad t: 1,2,3, \dots, n \tag{4.7}$$

$$\mu_{String}^{MI} = \sum_{t}^{n} \mu_{String}^{MI} \qquad t: 1,2,3,\dots,n \tag{4.8}$$

$$\lambda_{String}^{MI} = \mu_{String}^{MI} \times P_{f_{String}}^{MI} \times \left(P_{r_{String}}^{MI}\right)^{-1} \tag{4.9}$$

Before calculation of composite failure and repair rate of 2nd sub-division, n-independent parallel strings are included into calculation of composite failure and repair rate of 1st sub-division by equations 4.6 - 4.9. ($P_{r_{String}}^{MI}, P_{f_{String}}^{MI}$) and ($\lambda_{String}^{MI}, \mu_{String}^{MI}$) which represent the failure-repair state probabilities of n-independent PV strings and the failure-repair rates of 1st sub-division, respectively [3].

$$P_{r_{Storage}}^{MI} = \prod_{t}^{n} \left(\frac{\mu_{CC_t}}{\lambda_{CC_t} + \mu_{CC_t}} + \frac{\mu_{BB_t}}{\lambda_{BB_t} + \mu_{BB_t}}\right) \tag{4.10}$$

$$P_{f_{Storage}}^{MI} = 1 - \prod_{t}^{n} \left(\frac{\mu_{CC_t}}{\lambda_{CC_t} + \mu_{CC_t}} + \frac{\mu_{BB_t}}{\lambda_{BB_t} + \mu_{BB_t}}\right) \tag{4.11}$$

$$\mu_{Storage}^{MI} = \sum_{t}^{n} \mu_{Storage}^{t} \qquad t: 1,2,3,\dots,n \tag{4.12}$$

$$\lambda_{Storage}^{MI} = \mu_{Storage}^{MI} \times P_{f_{Storage}}^{MI} \times \left(P_{r_{Storage}}^{MI}\right)^{-1} \tag{4.13}$$

$$\lambda_{Cyber}, \qquad \mu_{Cyber} \tag{4.14}$$

As previously described, 2nd sub-division of PV generating units consists of storages that include battery banks and charge controllers. ($\lambda_{BB_t}, \mu_{BB_t}$) and ($\lambda_{CC_t}, \mu_{CC_t}$) denote the failure-repair rates of a battery bank and a charge controller, respectively. Equations 4.10 and 4.11 compute the failure-repair state probabilities of the storage units. The failure and repair rates of 2nd sub-division ($\lambda_{Storage}^{MI}, \mu_{Storage}^{MI}$) are calculated using equations 4.12 - 4.13 [3].

The 3rd sub-division includes the cyber physical component of a PV generating unit and its failure and repair rates (λ_{Cyber} , μ_{Cyber}) are used in composite reliability for a PV generating unit. By utilizing composite failure-repair rates of PV generating system's sub-divisions and Markov chain state transition for the PV generating unit is developed as in Figure 4.3.

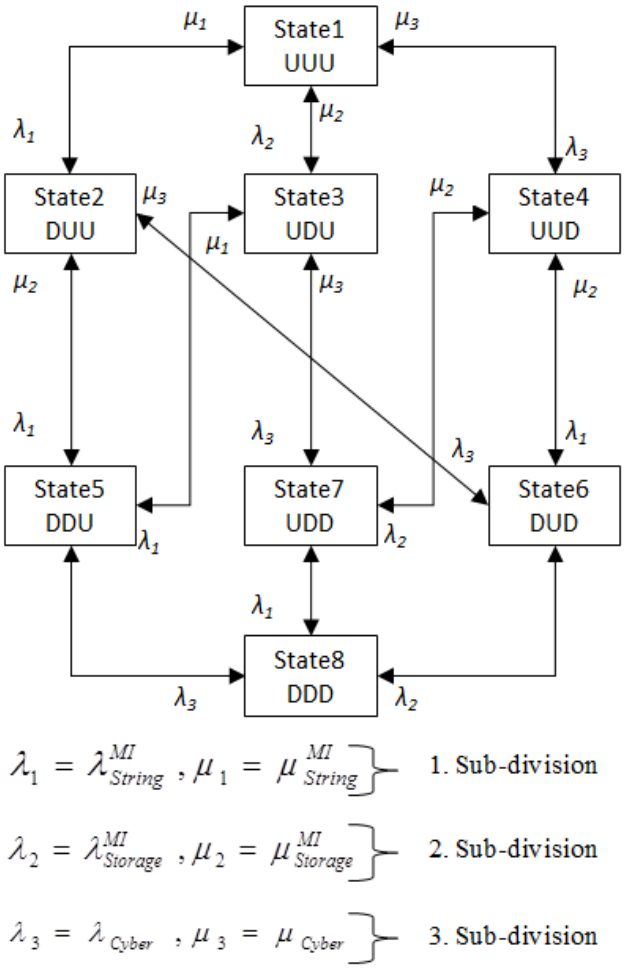


Figure 4.3 Block diagram of Markov chain state transition of PV generating unit[3]

4.2.2 Reliability Analysis Procedure of Cyber-Physical Systems

As previously highlighted, published research on the reliability of a PV system with Cyber-Physical Systems (CPS) is limited. Failure-repair rates of many physical components

have been assessed and they are publicly available for any system's reliability evaluation. Because CPS is comprised of not only physical layers but also virtual layers, the interaction of CPS's virtual layers with its physical part can affect the reliability of the system operations. Due to data availability of failure-repair rates of CPS components and their calculation challenges, the evaluation of the composite power system reliability becomes a more challenging task. In addition, it needs to be indicated that the estimation of failure-repair rates of CPS and the statistical detection procedure of cyber-attacks are vital to assess CPS's interaction with PV systems because of CPS's stochastic nature. Thus, the working principle of CPSs' components is considered with a two-state unit approach as operating and non-operating states in order to increase its applicability into reliability-risk analysis concepts [154] [3].

Previous studies suggests that not all cyber-intrusions with different intensity can lead to a failure in a power network, thereby cyber incidents are accepted as an uncommon event [155]. In order to estimate failures of a cyber-physical system in a pool of a fixed number of events, the Poisson random number generator is utilized due to its rare event characteristics [155]. Utilization of Poisson distribution in a rare event is justified by Palm - Khintchine theorem and it states that events with small intensity level follow the pattern of a Poisson process [155]. Thus, this chapter considers cyber incidents and related threats as rare events [3].

General assumptions are made for the availability simulation of CPS. These are as following: 1-The traditional power system is not compromised of any defensive mechanism for cyber-intrusions and there is no partially-operating rule for CPS's cyber layer; 2-The permeability criteria of the cyber layer in the power grid is constant and memoryless; 3-The iteration number of availability simulation and the number of randomly generated cyber-attacks are chosen as 10000 for a year; 4-The intensity of cyber-intrusion is regarded as the arrival rate

of cyber-intrusion to the cyber layer of the CPS; 5-The number of successful intrusions can be calculated only if comparison of attack intensity and the cyber layer of CPS's permeability criteria can be made [3]. In order to calculate the availability indicator of CPS, a framework is created as in Figure 4.4 by the help of the studies in [156, 157]. The main objective of the availability framework of CPS is to estimate availability-unavailability rates of CPS. Proposed generic electric sector failure scenarios related to cyber threats by National Electric Sector Cybersecurity Organization Resource (NESCOR) are analysed with reference [156]. According to information security, cyber threats are categorised into three main classes in order to calculate their impacts on a power grid [156].

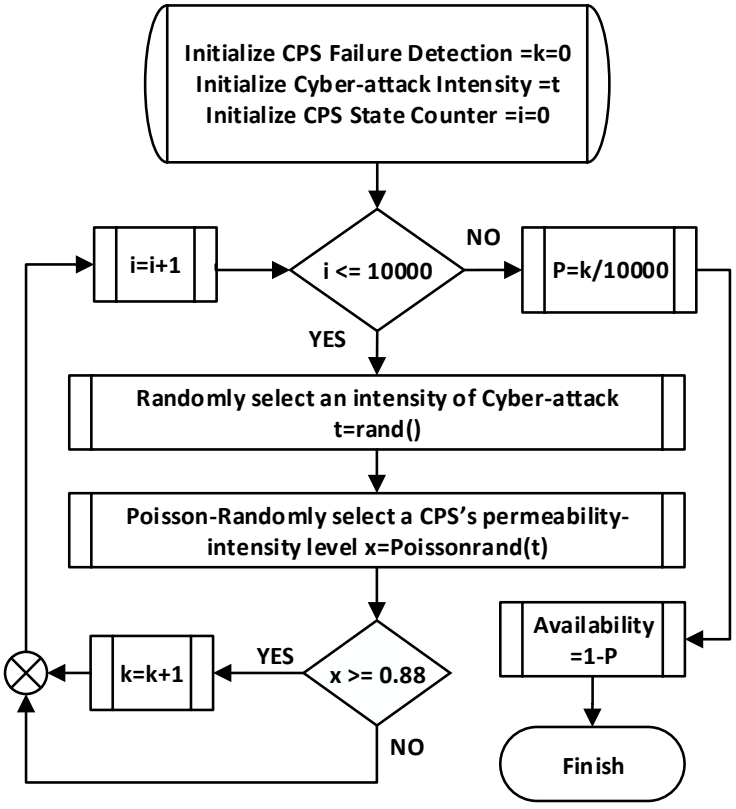


Figure 4.4 Procedure of Availability analysis of Cyber-physical system[3]

Confidentiality can be referred that the state of cyber-intrusion to access data and take confidential information or data without any permission or authorization of operators. As a result of the cyber-intrusion, the power grid has still not experienced any destruction or damage [3].

Integrity can be defined as cyber-intruder changes to the information and modifications to the private data in a power grid. However, there are no interruptions to service or disruptions in power grid operations [3].

Availability can be described as a system or infrastructure which is able to sustain its standard operations without any damage and destruction. Power network outages may be generated by the lack of availability of the system [3].

Due to the lack of availability of the system can cause system outages in context of a power grid, the availability analysis for CPS is the main focus of this framework. Unavailability of the system is described as power system outages at a high level [156]. In this manner, large scale power outages are generated as result of the effects of a high intensity level cyber intrusion [156]. So as to compute the availability ratio of CPS, the permeability-intensity criteria of the cyber layer of the CPS needs to be obtained, which may assist to identify the severity level of a cyber-intrusion that may result in the system outage. It is also assumed that cyber-intrusions with different severity levels, which are classified with different attack configuration groups (confidentiality, integrity and availability), can affect the operation status of the system. Cyber-attack is successfully intruded into the system only if the intensity level of cyber-intrusion meet the limit criteria of the permeability-intensity of the cyber layer of the system. Hence, if the intruder passes the criteria, CPS is going to be in the state of unavailability that is linked with

system contingency. For this mathematical framework of the CPS availability analysis, the limit criteria of the permeability-intensity of the cyber layer of the system is obtained as 0.88 [156]. This framework with the limit criteria estimates the contingency number of CPS considering the strength of cyber-intrusions and their asynchronous characteristics [3].

After the calculation framework for the availability of CPS as in Figure 4.4, the calculation procedure of the failure-repair rate of CPS is expressed as the following stages [3]:

I. Set initial counter states of the failure detection of the CPS and the intensity ratio of the cyber-intrusion.
II. Specify the total number of cyber-intrusions in the simulation.
III. Determine an intensity ratio of the cyber-intrusion with a random selection.
IV. According to the intensity ratio of the cyber-intrusion, select a Poisson random number for arrival level of cyber-intrusion.
V. Examine the permeability-intensity criteria of the cyber-intrusion on the cyber layer of the CPS. If the arrival level of cyber-intrusion is higher than the criteria, increase the contingency number of the CPS.
VI. Follow the availability process stages of CPS until the fulfilling the number of cyber-intrusions in the simulation.
VII. Calculate the availability rate of the CPS.
VIII. In order to perform the sensitivity analysis on the repair rate of CPS, select a CPS repair rate strategy (low, medium, and high mean recovery time).
IX. According selected repair-time strategy of CPS, time to repair (*TTR*) of CPS is calculated as in the equation below 4.15.

$$\frac{1}{\mu_{Cyber}} = Time\ to\ Repair\ (TTR) \tag{4.15}$$

Where μ_{Cyber} and TTR represent the repair rate of the CPS for a year and the time to repair of the CPS, respectively.

X. Finally, the failure rate of the CPS (λ_{Cyber}) is estimated by the following formula (4.16) and it is re-designed from [158]. The availability of the CPS is described as A, which is generated by the availability framework.

$$\lambda_{Cyber} = \frac{8760 - 8760 \times A}{TTR} \tag{4.16}$$

4.2.3 The Procedure of Composite Power System Reliability Evaluation

One of the objectives of power system reliability studies is to investigate the capacity limits of the power system to fulfil the demand of consumers within a certain amount of time. The standard procedure of composite power system reliability evaluation incorporating with availability framework of the CPS is presented as follows:

i. Model and determine the critical elements of PV powered systems, its generation output and load demand of each busbar.
ii. Find out and determine failure and repair rates of power system components as well as the components of the PV generating unit.
iii. By means of the repair time strategy for the CPS and the calculation of CPS's availability, all failure-repair rates of subdivisions of PV generating unit can be calculated. Calculated values of the failure-repair rates are implemented into the presented Markov chain transition model for computing the state probabilities of PV generating unit.

iv. Generate a random sample of the state of the PV generating unit with CPS.

v. Initialize power equilibrium in the test system and scrutinize standard voltage boundaries during the power flow analysis.

vi. Perform power flow analysis with 10000 iterations and compute the Expected Demand Not Supplied (*EDNS*) according to equation (4.17) [107, 159].

$$EDNS = \sum_{i \in S_i} L_i \times p_i \tag{4.17}$$

The unit of *EDNS* is subject to GW, where S_i represents system state *i;* L_i describes load curtailment in system state *i*; p_i denotes the system state probability.

vii. In the final step, Expected Energy Not Supplied (*EENS*) can be calculated by following the formula (4.18), which is given in GWh/year.

$$EENS = \sum_{i \in S_i} L_i \times p_i \times 8760 = EDNS \times 8760 \tag{4.18}$$

Figure 4.5 describes the procedure of the reliability assessment framework of PV generating units with CPS. The procedure is divided into two parts. The first part of the procedure determines the failure-repair rates of CPS and the state probabilities of the proposed Markov model, which are calculated by MATLAB. Calculated data from the simulation of the first part is fed into an eight-state Markovian model in order to determine the state probabilities of a composite PV generating unit subroutine in DIgSILENT (StoGen) for the second part of the procedure [159]. StoGen is a component of a multi-state stochastic power generation model incorporating with each PV powered generator (ElmGenstat). In order to estimate EDNS and EENS with related scenarios, Monte Carlo Simulation is performed through an optimal power

flow routine with the data of 8-state PV system probabilities and availabilities calculated from the first part of the simulation [3].

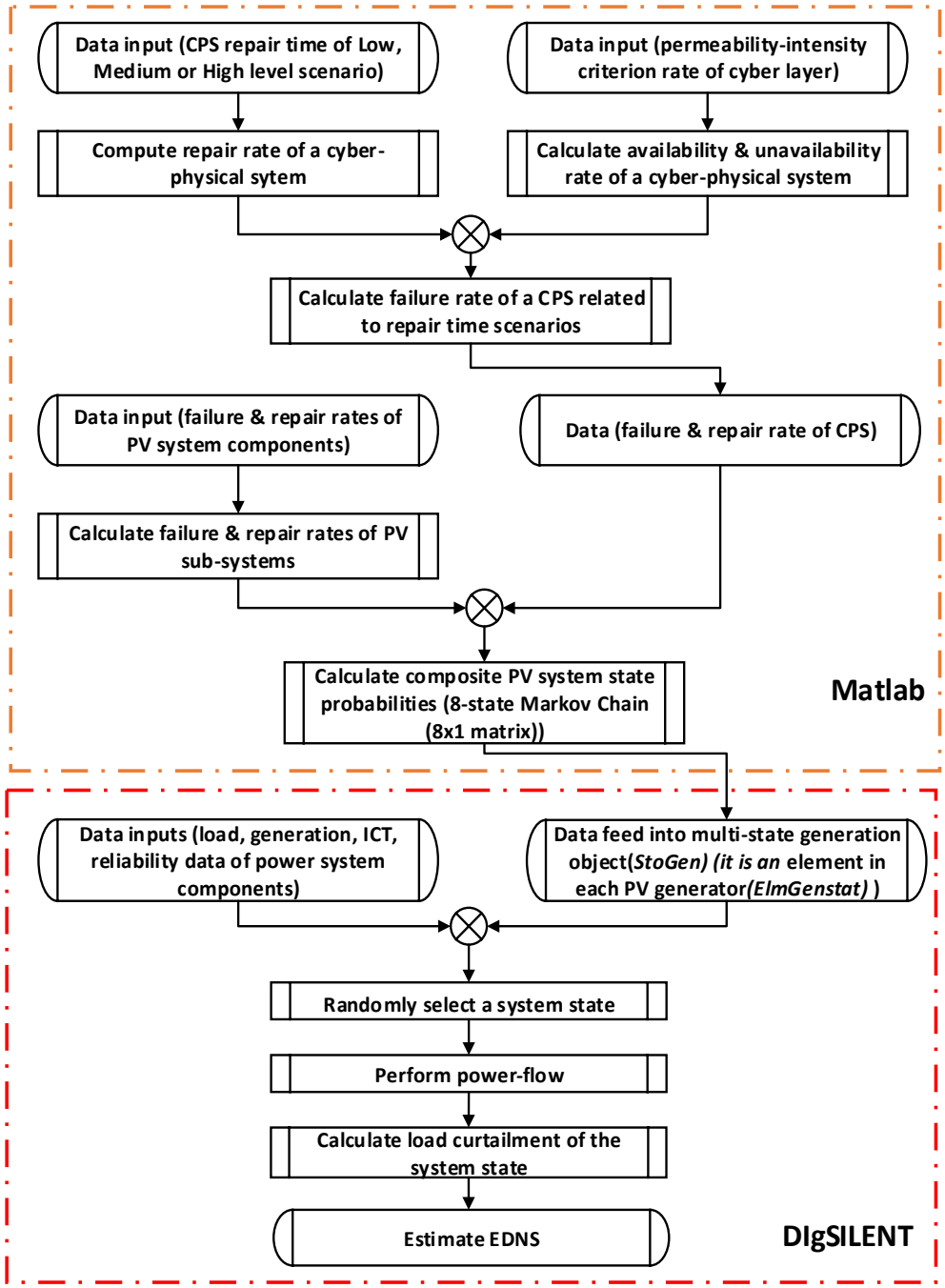


Figure 4.5 The procedure of the reliability assessment framework of PV generating units with CPS [3]

4.3 Case Studies and Results Analysis

4.3.1 The Topology of Reliability Test Systems and Utilized Data for Case Studies

This section of the chapter introduces utilized test systems with their modifications and implemented reliability data of power system components for case studies. In addition, extended version of buses are used for reliability test systems and this is demonstrated with its components.

4.3.1.1 Information and Communication Technology Extension for Busbar Protection

The CPS operations of power networks have been involved as a secondary part of power systems in power system assessments. Previously proposed reliability test systems in the literature did not integrate the components of cyber-physical systems. Thus far, there are limitations on available standard test systems to assess the operation effects of cyber-physical systems on power grids. On the other hand, a recently published study [160] proposes a protection mechanism to apply IEC 61850 standard for the protection of substations. Incorporating with this mechanism, the reliability test systems (RBTS and IEEE RTS79) are extended with ICT components for proposed case studies in this chapter. The architecture of the protection system in substations is modelled as in [15]. The detailed architecture of the protection system of a substation is presented in Figure 4.6-a) with exemplifying the Bus 3 in the IEEE RTS79. The topology conventional version and extended version of IEEE RTS79 are also demonstrated in Figure 4.6-b) [3].

Because of the complexity and variety of CPS components, it is difficult to extend all substations with ICT components in the reliability test systems. Thus, bus 3, 4, 8, 9, 10 and 13

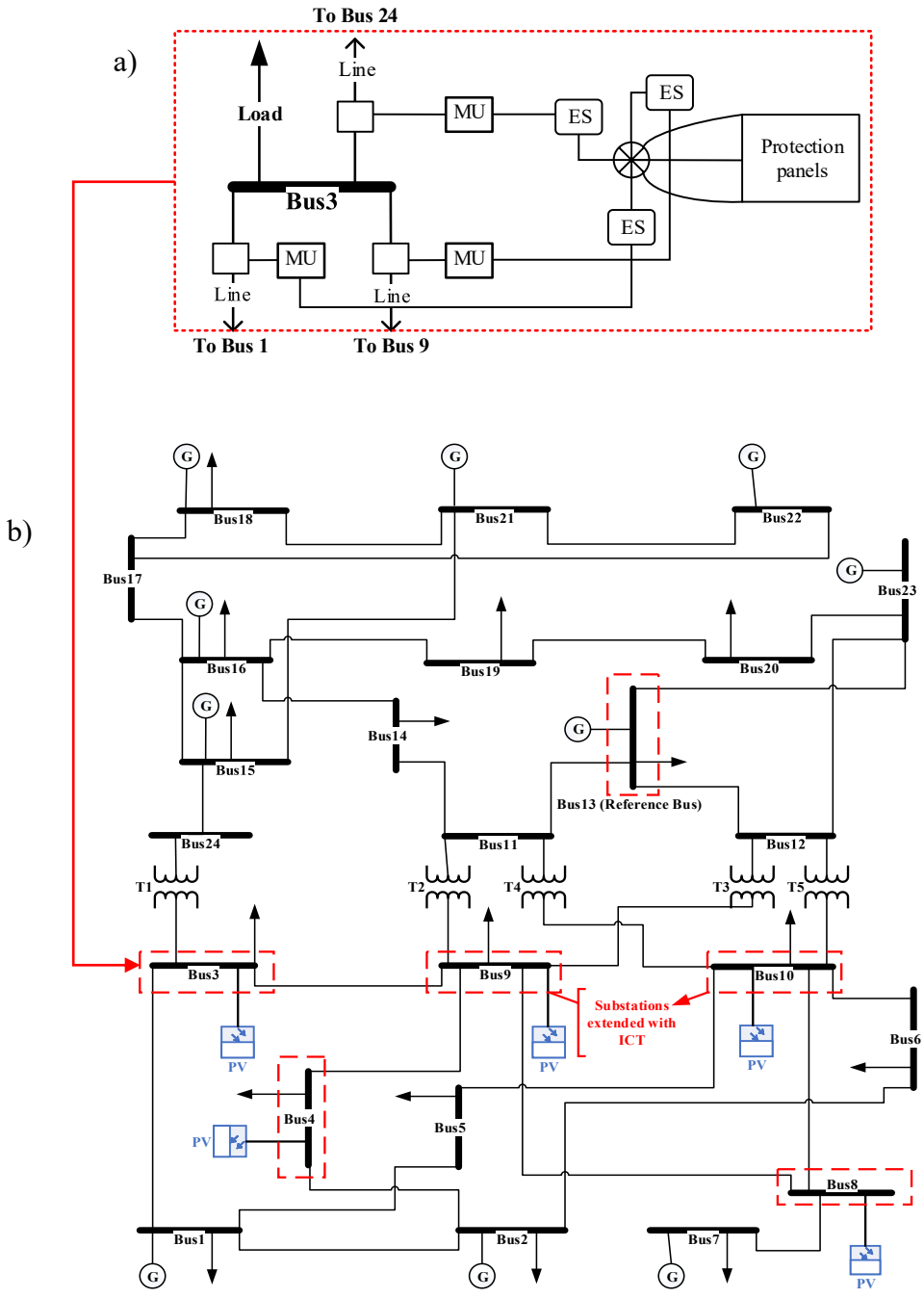


Figure 4.6 a) An example of the detailed architecture of the substation with ICT extension, b) Diagram of the extended version of IEEE RTS79 with PV systems and ICT [3]

of IEEE RTS79 are only modified with an interdependent CPS that are comprised of a merging unit (MU), ethernet switch (ES) and line protection panel as in Figure 4.6. All these elements of an ICT system in the specified terminals are connected to each other serially. This configuration of the ICT protection system is implemented only in the extended version of IEEE RTS79 for relevant case studies. The conventional IEEE RTS79 is composed of 24 buses and 32 traditional generators with the system peak load demand of 2850 MW. Its' related topology with parameters are obtained from [148] [3].

PV generating units are implemented into both conventional and extended versions of IEEE RTS79 with either centralised or decentralised connections. Centralised PV generating units are only applied into busbar 9 for specified case studies of IEEE RTS79 by cause of its critical characteristics. In other respects, decentralised PV generating units are implemented into busbar 3, 4, 8, 9 and 10 for relevant case studies. The nominal capacity of a PV generating unit at a consumer level is accepted as 4 kW and the total number of consumers in IEEE RTS79 is assumed as 949,994. Remain reliability parameters for case studies are obtained from [161, 162] [3].

4.3.1.2 The RBTS extended with Information and Communication Technology Configurations and Utilized Reliability Data for Case Studies

In order to examine the effect of CPS in distribution systems, the Roy Billinton Test System (RBTS) is utilized in the analysis of power system reliability. The RBTS is comprised of 9 transmission lines, 6 main terminals and 230 kV, 138 kV, 33 kV, 11 kV and 400 V buses are classified as voltage levels in the test system. The nominal peak load demand and peak power generation are 185 MW and 240 MW respectively. As similar to IEEE RTS79, the

topology of ICT extended version of the RBTS and conventional version of the RBTS are extended to apply to PV generating units with centralised and decentralised integration modes for specified case studies. Terminal 3 of the RBTS is used for a centralised PV generation integration mode. On the other hand, terminal 3, 4, 5 and 6 are used for a decentralised integration mode of PV generating units. PV generating units are integrated into 11 kV voltage levels. The nominal capacity of PV generating unit at a consumer level is accepted as 4 kW and total number of consumers in the RBTS is assumed as 18,308. Remaining reliability parameter

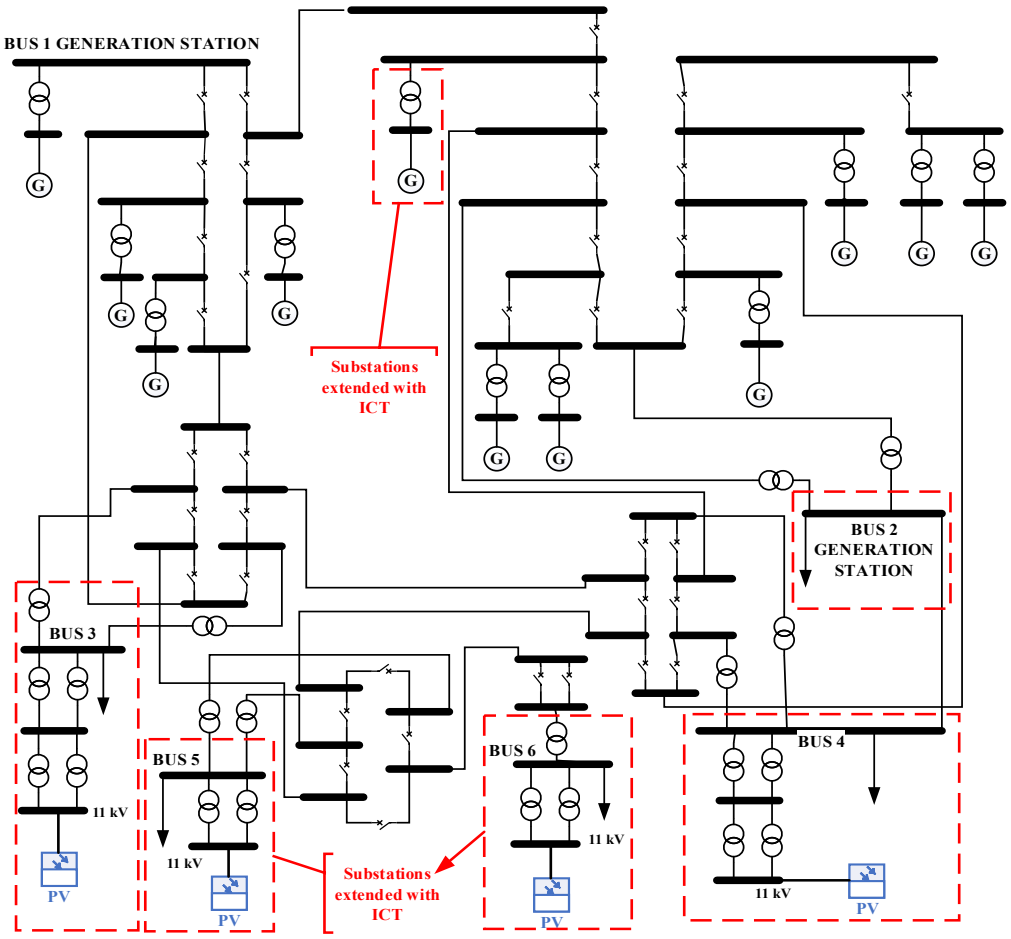


Figure 4.7 Single line diagram of the extended version of RBTS with PV systems and ICT [3]

data for case studies are obtained from [2, 161, 162]. ICT extended version of terminals of the RBTS are designed to be similar to those used in the ICT extended version of terminals of the

IEEE RTS79. Figure 4.7 describes schematic diagram of the RBTS with PV systems and ICT extended version [3].

In order to demonstrate the impact of CPS on power system reliability, the failure rate and repair times of CPS needs to be calculated or obtained. Although there is no available data for repair times of CPS which can be used for reliability analysis, the failure rates of CPS cannot be calculated without the assumption of the repair times of CPS. With respect to [163], 23% of the UK companies recovered from cyber-intrusions within less than a day. 13 % of business firms affected by cyber-attacks returned to normal working conditions in less than a week. Almost 3 % of companies influenced by cyber-attacks repaired their system in either from a week to a month or beyond [163]. As a reference point, survey [163] shows that recovery time ranges from hours to months. For this chapter, the repair times of CPS are estimated as 15, 30 and 60 hours. These repair times are identified by low to high level harmful levels of cyber-intrusions on a power grid. Relevant repair times with computed failure rates and the reliability data of PV generating units with ICT components are given in the following Table 4.1 [3].

Table 4.1 Reliability data for PV system, ICT components and CPS repair time strategies[3]

PV System and ICT Components	Failure rate	Repair time
PV panel	1.14×10^{-6}	0.0209 (48h)
Micro-inverter	0.05	0.05 (20h)
Charge-controller	0.125	0.1 (10h)
Battery bank	0.00702	0.0825 (12.11h)
Fuse	0.00137	0.05 (20h)
Merging unit	0.02	8h
Ethernet switch	0.01	8h
Protection panel	0.02	8h
Repair Strategy	Failure rate	Repair time
High Repair Time	0.019	0.016 (60h)
Medium Repair Time	0.0097	0.033 (30h)
Low Repair Time	0.0048	0.066 (15h)

4.3.2 Case Study 1: Large-scale of PV Generating Unit Integration on Transmission System

The objective of case study 1 is to describe the effects of recovery time strategies of the CPS on the reliability of the power systems when the penetration level of PV generating units is increased.

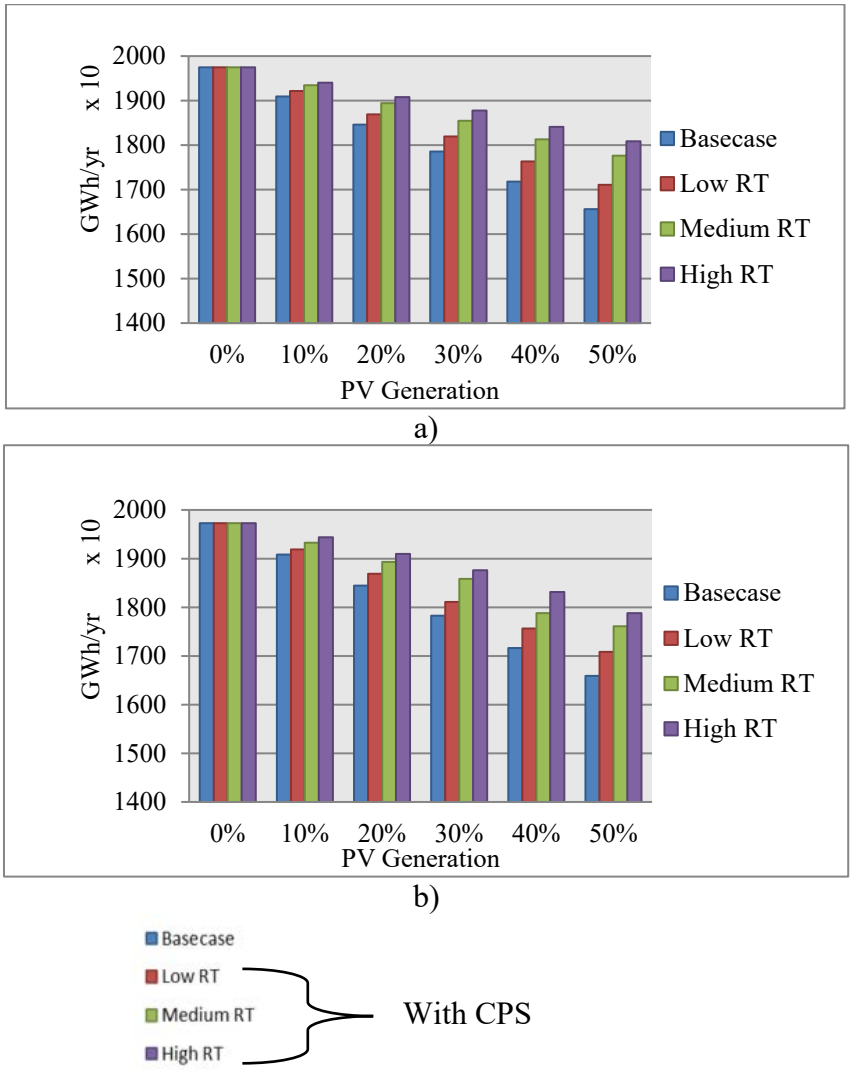
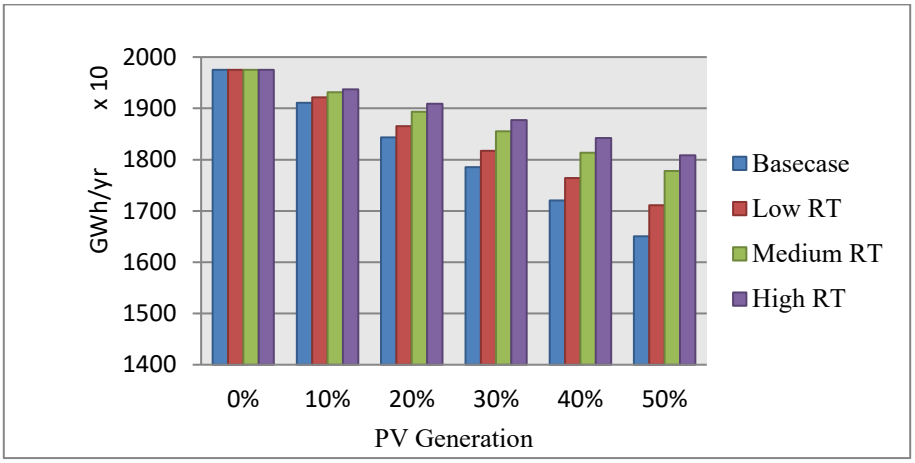


Figure 4.8 Graphs of EENS changes in IEEE RTS79 with centralised PV generating units- a) EENS for centralised PV generating units' integration in IEEE RTS79, b) EENS for centralised PV generating units' integration in IEEE RTS79 with ICT extensions [3]

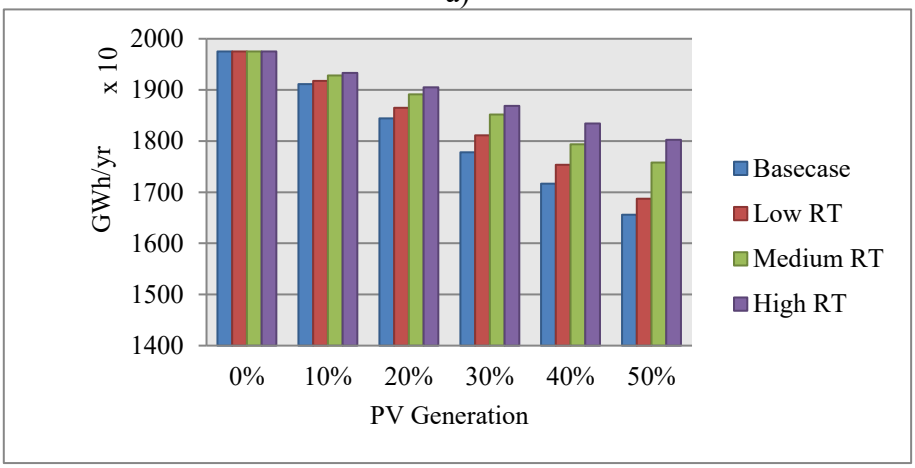
In order to assess the reliability of power systems, the traditional and ICT extended versions of

IEEE RTS79 are utilized with centralised PV generating unit modification. Figure 4.8 describes EENS changes in IEEE RTS79 with centralised PV generating unit integration considering Figure 4.8-a) IEEE RTS79 without ICT extensions and Figure 4.8-b) IEEE RTS79 with ICT extensions. Similarly, Figure 4.9 demonstrates EENS changes in IEEE RTS79 with decentralised PV generating unit integration considering Figure 4.9-a) IEEE RTS79 without ICT extensions and Figure 4.9-b) IEEE RTS79 with ICT extensions. The installed capacity level of PV generating units ranges from 0% (base case) to 50% of the base case level for both centralised and decentralised cases [3].

Both Figure 4.8 and Figure 4.9 represents an increase in PV powered generation that diminishes the EENS of the power network due to the large-scale penetration level of the PV generation. As described with all the case studies of PV generating units in both Figure 4.8 and Figure 4.9, the EENS index of each case study is adversely affected by the integration of the CPS. When there is an increment on the capacity level of the PV generating unit with CPS, the index of EENS escalates all of a sudden. Despite this there is a significant growth in between CPS's repair times, the EENS index of the PV generating unit with CPS has higher value compared to the base case of the PV generating unit in all repair scenarios. It can be clearly seen from both Figure 4.8 and Figure 4.9 that the EENS index has linearly declined in all scenarios if the capacity level of PV generation is linearly raised. In particular, there is a steep increase on EENS in comparison of the PV generating unit case scenarios of 40% with 50% capacity levels and the case scenarios of 10%, 20%, and 30% capacity levels. The cause of the variation on the rise of EENS is owing to the diversification in the failure-repair rates of PV generating units. Also, it is as a result of a systematic variation of the PV generating unit's availability in a power grid. There is no significant disparity in between the rest of the cases.



a)



b)

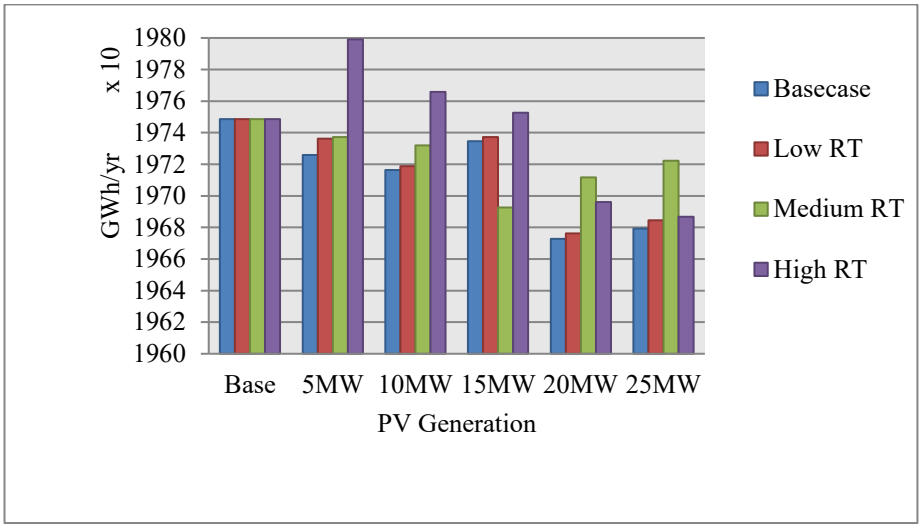
Figure 4.9 Graphs of EENS changes in IEEE RTS79 with decentralised PV generating units- a) EENS for decentralised PV generating units' integration in IEEE RTS79, b) EENS for decentralised PV generating units' integration in IEEE RTS79 with ICT extensions [3]

Nevertheless, if the PV generating unit passes 30% capacity level, the EENS is limited by the repair time of the CPS with its lowest point. From the point of view of economics, it may be more advantageous to choose a low repair time strategy in order to diminish the effect of labour cost during the recovery. For this reason the EENS index in case study 1, the centralised PV generating unit is a slightly more secure option to invest in compared to a decentralised PV generating unit even if there is a proposed CPS due to the intact operation of CPS compared with decentralised operation. Within the case scenarios of ICT extended versions of IEEE

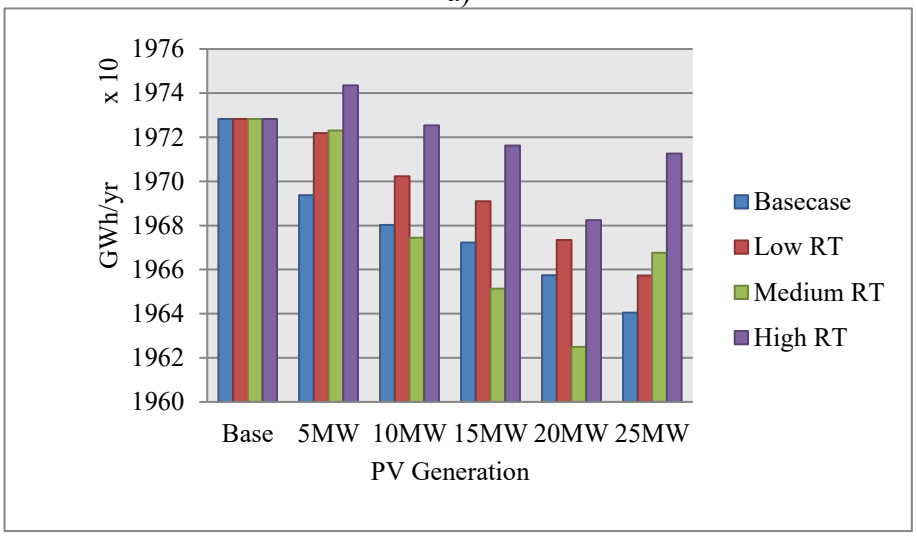
RTS79 in both Figure 4.8-b) and Figure 4.9-b), there are steep falls in the EENS index when the integration of a PV generating unit is as either centralised or decentralised cases. Comparison of EENS changes in between 'with and without' ICT extension of transmission systems, varies between 0.1% and 1.4% on the EENS index when considering both decentralised and centralised cases because of the protection features of ICT elements. It can be observed that the effect of ICT elements in power system reliability within the medium and high repair time of CPS case scenarios if the installed capacity level of PV generating unit is 40% and 50% of the base case [3].

4.3.3 Case Study 2: Comparison of PV and synchronous generator for IEEE RTS79

The purpose of case study 2 is to compare the integration of conventional generation against PV generation systems for understanding the reaction of power grid and sensitivity of different CPS repair time scenarios. Case study 2 adopts a procedure that increases the capacity level of PV generating unit with a 5 MW; decreases the capacity level of conventional generation of slack bus (bus 13) of IEEE RTS79 with a 5 MW at the same time. This strategy is implemented into centralised and decentralised generating units taking into consideration 'with and without' ICT extension of substations, and it is continued until it reaches 25 MW PV generation capacity, to observe the effects on EENS. It can be clearly seen from Figure 4.10-a) and Figure 4.11-a) that a rise in PV generation decreases EENS index when considering the strategies of the base case, Low and Medium repair time. What stands out in the Figure 4.10-a) is that the system reliability is improved with Low and Medium repair time strategies compared to the base case scenario of centralised PV generation when there is an increase on the generation capacity [3].



a)



b)

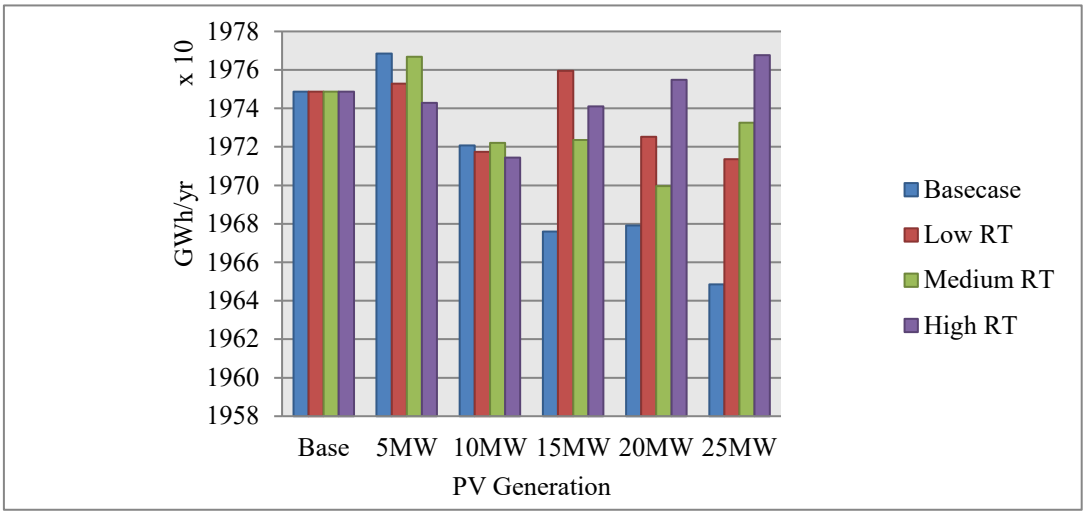
Figure 4.10 EENS changes in centralised PV generation with different topology features [3], a) Centralised PV generating units' integration in IEEE RTS79, b) Centralised PV generating units' integration in IEEE RTS79 with ICT extensions [3]

In addition, the sudden variation of EENS is more prominent with an increment in the penetration of decentralised PV generating unit as shown in Figure 4.11-a). There is a unique variation in this scenario even if PV generation reaches 5 MW in the scenario of the high repair time. Although the mean time failure rate of a PV generating unit is higher than the conventional generating unit, the EENS is steadily reduced by the integration of the PV generating unit at

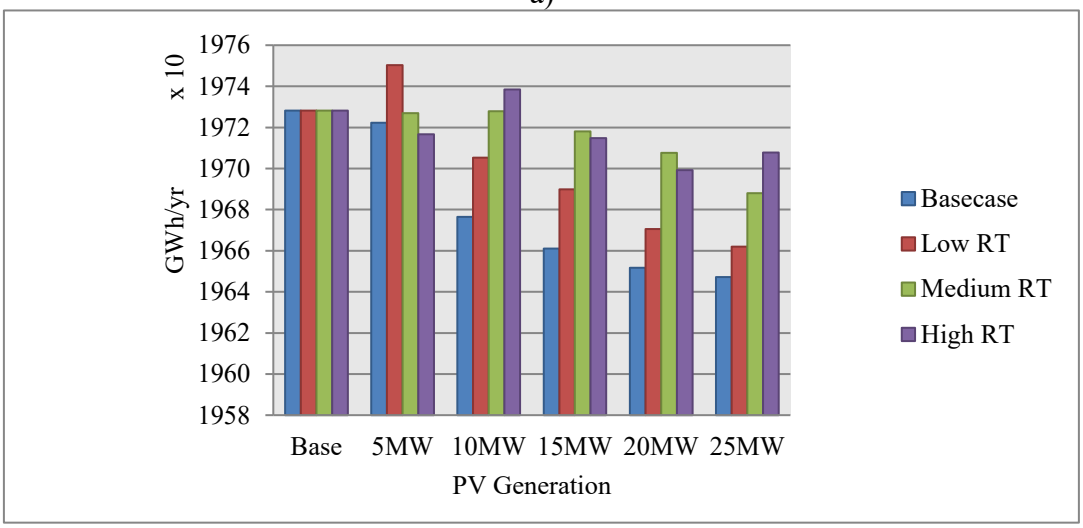
bus 13. However, it is not always true that PV generating units are more reliable than conventional generating units. In this case, there can be three reasons that cause an apparent decrease on the EENS, which are the topology of the test system, the integration location of the PV generating unit and the intermittent nature of the PV generating unit. Moreover, the sudden variation on EENS with different repair time strategies of PV generating units may be stemming from either the availability of and the intermittency effect of the PV generating units or the location of the PV generating unit in the power grid [3].

Figure 4.10-b) and Figure 4.11-b) show that the ICT extended version of substations have positive effects on the system reliability compared to their traditional version. It can considerably diminish EENS when considering the medium and high-level recovery-time scenarios of CPS for PV systems. ICT protection of the substations improves the system reliability resulting from a reduction of EENS between 0.1% and 0.5% compared with the traditional version of IEEE RTS79; excluding 25MW centralised PV generating unit with a high recovery time strategy as in Figure 4.10. When the capacity of the PV generating unit reaches up to 25 MW, the EENS is decreased with the medium and high-level recovery-time scenarios of CPS. In the angle of CPS scenarios, the threshold point of the PV generating unit capacity for the test system might vary between 20 and 25 MW in both Figure 4.10 and Figure 4.11 [3].

In order to investigate the root cause of a discovered sudden changes as shown in case study 2, two additional case studies were performed which focused on the power system topology effects on EENS in parallel with the contingency analysis of power systems.



a)



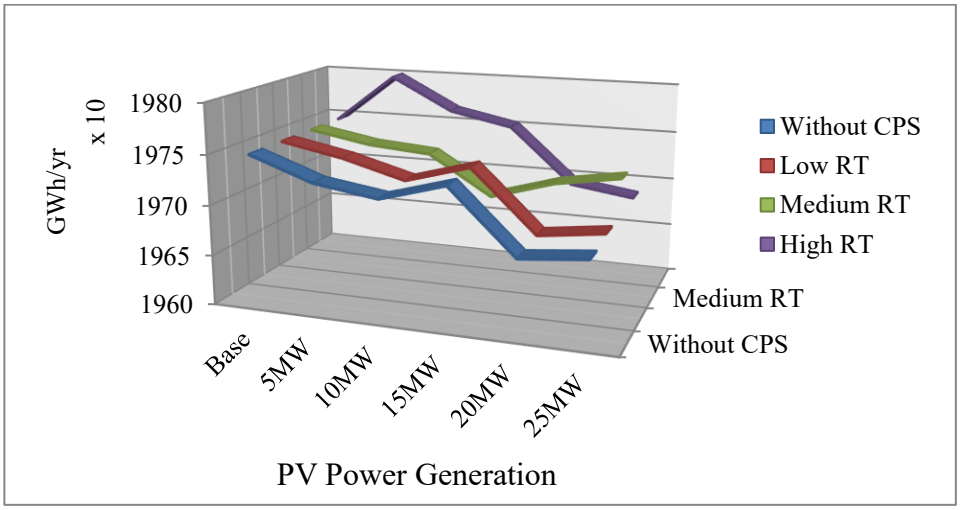
b)

Figure 4.11 EENS changes in decentralised PV generation with different topology features- a) Decentralised PV generating units' integration in IEEE RTS79 b) Decentralised PV generating units' integration in IEEE RTS79 with ICT extensions [3]

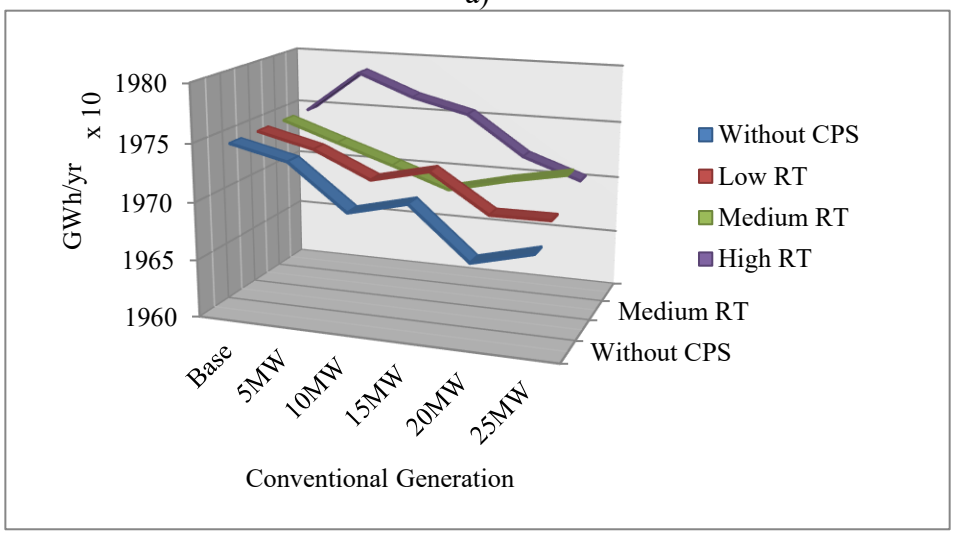
4.3.4 Case Study 3: Impact of power network topology on system reliability in IEEE RTS79

Case study 3 aims to explore the root causes of unforeseen EENS changes to PV generating units as previously observed in case study 1 and 2. The first step of the procedure for case study 3 starts by removing the PV generating units from bus 9, then integrating a

synchronous generating unit with same capacity into the bus 9. The second step is similar to the procedure of case study 2 that an increase on generation at bus 9 will decrease an equal amount of generation capacity from the generator of bus 13 (slack bus).



a)



b)

Figure 4.12 Comparison of EENS variation considering different generating units in Bus 9- a) PV Power Generation, b) Conventional Generation [3]

If the outcome from this procedure is similar to the case of PV generating units, then the outcome indicates that the sudden changes of EENS are because of the topology of the power grid. On the other hand, if the outcome from this procedure is different, the sudden changes on

EENS are because of the intermittent nature of the PV generating units. Synchronous generating unit capacity changes from 0 MW to 25 MW as executed in the case study 2. Figure 4.12 demonstrates that the results of the EENS index with synchronous generating units are almost the same as compared to PV generating units taking into account all the different repair-time strategies of CPS. However, small changes between both case scenarios can be linked with the intermittent feature of the PV generating unit's output. Thus, the sudden variations of the EENS index as highlighted in case study 2 are affected by the location of PV generating units.The EENS index varies between 0.008% and 1.2% compared to the base case scenario due to intermittent characteristics of PV generating units. It can be seen from comparison of PV and synchronous generating units with 20MW generating capacity considering high repair time strategy of CPS that at its highest, changes within the EENS index reach 1.2 %. Also, a 20 MW PV generating unit capacity has a minimal intermittent effect on the EENS index when compared to the base case with 0.008%. Therefore, when considering the intermittent conditions of the PV generating unit, a 20 MW PV generating unit capacity with medium repair-time strategy is the most feasible scenario for this terminal [3].

4.3.5 Case Study 4: Contingency Analysis

The contingency analysis of a power system is a part of comprehensive reliability evaluation of power systems. In order to examine the security analysis, it is important to carry out contingency analysis for high to low probable failures. The purpose of case study 4 is to perform the contingency analysis on IEEE RTS79 considering PV generating units with other components and to investigate what is the security margin limit of the test system during the integration of PV generation in both centralised and decentralised case scenarios. Single (N-1) and multiple (N-2) contingencies are examined in the test system for investigating the security

performance considering the system voltage and loading limits. After implementing stochastic contingencies, terminal 6, transformer 3, 4 and 5 are investigated being as critical elements of the IEEE RTS79 when integrating PV generating units. Due to the highest level of voltage violation in the power network, terminal 6 is chosen for security testimony during both centralised and decentralised PV generating unit integrations.

Table 4.2 Contingency Analysis of the IEEE RTS79 for Critical Components [3]

Vulnerable Component	**Centralised Integration** Terminal 6	**Decentralised Integration** Terminal 6	**Vulnerable Component**	**Centralised Integration** Transformer 3	**Decentralised Integration** Transformer 3
PV (MW) Generation	Maximum voltages (p.u)	Maximum voltages (p.u)	**PV (MW) Generation**	Maximum loading (%)	Maximum loading (%)
5	1.012	1.012	5	98.0	97.5
10	1.021	1.047	10	96.5	96.1
14	1.043	1.049	15	95.0	94.8
15	1.045	1.053	20	93.6	94.6
20	1.048	1.057	25	92.1	93.7
24	1.049	1.058	***	***	***
25	1.050	1.058	***	***	***
Vulnerable Component	**Centralised Integration** Transformer 5	**Decentralised Integration** Transformer 5	**Vulnerable Component**	**Centralised Integration** Transformer 4	**Decentralised Integration** Transformer 4
PV (MW) Generation	Maximum loading (%)	Maximum loading (%)	**PV (MW) Generation**	Maximum loading (%)	Maximum loading (%)
5	95.4	95.6	5	87.9	87.5
10	94.5	94.7	10	87.8	87.0
15	93.6	93.7	15	87.6	86.6
20	92.7	92.7	20	87.5	85.4
25	91.8	91.7	25	87.4	84.7

Table 4.2 represents contingency analysis for the critical components of the network. According to the analysis, centralised and decentralised PV integration reach to the system voltage violation limits with 24 MW and 14 MW capacity levels, respectively. When the capacity of PV generating units is to reach a limit, there is a high risk of cascade collapse due to load violation. One should be mindful of the fact that, additionaly, transformer 3, 4 and 5

must be considered during the power system operation and planning phases for this test system, in particular transformer 3. Even if the PV generating unit capacity is increased up to 25 MW for both integration scenarious, transformer 3 wouldstill overload and it needs to be carefully assessed by operators [3].

4.3.6 Case Study 5: Large-scale PV Generating Unit Integration on a Distribution System

Case study 5 demonstrates the effects of a PV generating unit capacity with the integration of CPS. The case also evaluates distribution system reliability considering different repair time strategies of CPS when increasing PV generation capacity levels. The procedure is applied same as in the case study 1. As might be expected that RBTS should behave differently than IEEE RTS79 because of their differing complexity levels and the differing structural details between them. The reliability assessment is performed with centralised and decentralised PV integration considering with the ICT extended version of the RBTS and original version of the RBTS. The capacity level of the PV generating unit is lifted from 0% to 20 % of the base case of load demand capacity gradually. Figure 4.13 demonstrates that there are reductions on EENS index of the RBTS in all case scenarios compared with base case scenarios while the capacity of the PV generating units is increased. This implies that the integration of PV generating units with CPS brings a backlash effect on the power system reliability [3].

With an increment in PV generating unit capacity with CPS, EENS changes abruptly. There are different behaving of EENS index in the case study 5 compared to the case study 1. The difference on between EENS reaction of the RBTS and IEEE RTS79 is that the system

reliability is not constantly decreasing when considering with CPS repair-time strategy scenarios. A possible explanation for this behaviour might be that the RBTS is comparatively smaller and more complex than IEEE RTS79. In addition, the variation of EENS in small test systems may be smoothly observed compared to large test system.

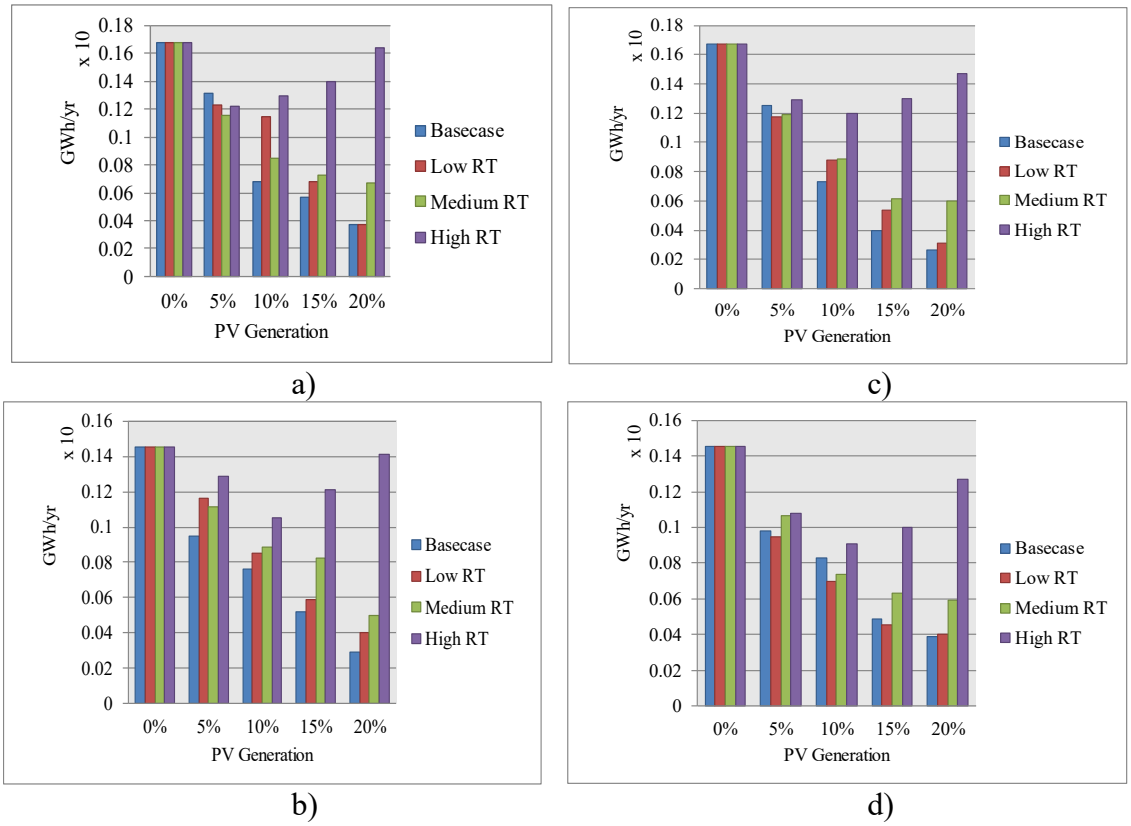


Figure 4.13 Graphs of EENS changes in RBTS with PV generating unit integrations- a) Centralised PV generating units' integration in RBTS, b) Centralised PV generating units' integration in RBTS with ICT extensions, c) Decentralised PV generating units' integration in RBTS, d)Decentralised PV generating units' integration in RBTS with ICT extensions [3]

As seen from both Figure 4.13-a) and Figure 4.13-c), there are adverse impacts on EENS variations considering an increase on PV generation capacity level in both low and medium repair time of CPS scenarios. Nevertheless, EENS escalates in tandem with PV generation capacity level in the scenario of the high repair time strategy of CPS. Even if the increment of

PV generating unit capacity level reaches to 20 MW, EENS index of the RBTS with high repair time strategy nearly reaches to base case levels. Figure 4.13-b) and Figure 4.13-d) present the EENS variations of ICT extended version of the RBTS considering centralised and decentralised PV generating unit integrations. There are similarities between Figure 4.13-b) and Figure 4.13-d) that even if there are integration effects of CPS, the system reliability is positively impacted by the ICT extension of the RBTS. As a result, the EENS of the ICT extension of RBTS is enhanced with between 13% and 25% of base case levels. This is a prove of the importance of ICT protection extension in substations [3].

4.3.7 Case Study 6: Comparison of PV and synchronous generator for RBTS

The case study 6 set out to compare the integration of conventional generation against PV generating units for understanding the reaction of distribution test system and, additionally to examine the impact of different CPS repair time scenarios. As similar to case study 2, the procedure of case study 6 is to increase PV generating unit capacity level, and decrease the capacity level of synchronous generation from the slack bus (bus 1) of the RBTS at the same time. Centralised and decentralised PV generating units with CPS are also considered under ICT protection extension schemes for substations. The capacity limit of PV generation ranges between 0 MW and 40 MW with increasing 10 MW intervals in this case study. Terminal 3, and terminal 3, 4, 5 and 6 are utilized for centralised integration and decentralised integration case scenarios, respectively. The topology of utilized test system is shown in Figure 4.7. The results are described in Figure 4.14 that the EENS of all the scenarios with CPS is less than the EENS of the base cases when PV generating capacity level increases. It is expected outcome when PV generation is escalated. As seen in Figure 4.14, EENS of the RBTS pursues a different trend compared to in case of transmission system for case study 2. In all case scenarios of CPS

repair time, it can be observed in Figure 4.14-a) and Figure 4.14-b) that there are declining trends in the EENS compared to base case scenarios when the capacity level of the PV generating units is in step-increase [3].

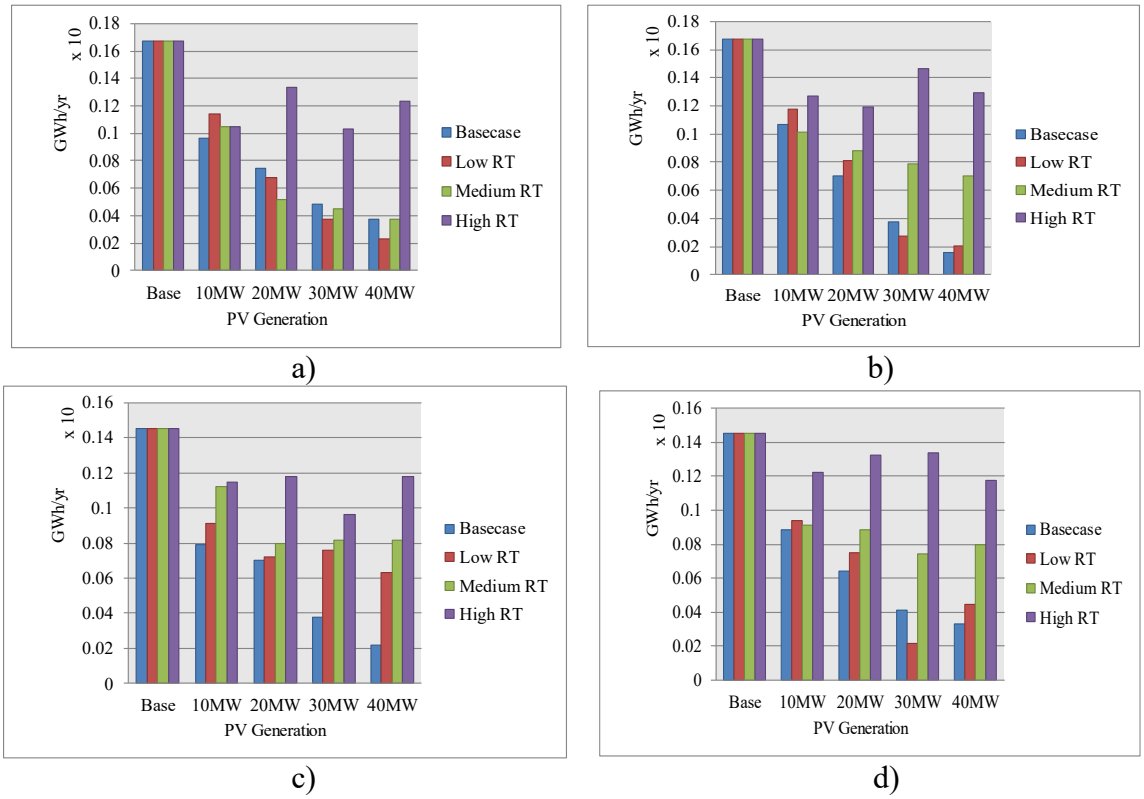


Figure 4.14 EENS changes in RBTS considering conventional and PV powered generation- a) Centralised PV generating units' integration in RBTS, b) Decentralised PV generating units' integration in RBTS, c) Centralised PV generating units' integration in RBTS with ICT extensions, d) Decentralised PV generating units' integration in RBTS with ICT extensions [3]

Though, EENS with high repair time of CPS scenarios do not always follow declining trend. There are fluctuating trends in the EENS with high repair time of CPS scenarios in both centralised and decentralised integration of PV generating units (Figure 4.14-a) and Figure 4.14-b)). With similar manner in case study 2, this trend of EENS is because of the PV generating unit location and loading conditions of the test system. Unexpected pattern of the EENS of the RBTS is as result of the location of PV system integration as similarly seen in the

case study 2. This is the root cause of the fluctuating behaviour of EENS in the case of centralised and decentralised PV generating unit integration with CPS high repair time. Even though with this unique behaviour of the EENS with high repair time scenarios, EENS is associated with smaller values compared to base case scenarios. As seen from the comparative analysis of centralised and decentralised PV generating units in Figure 4.14, centralised PV generating unit integration in the RBTS outperforms compared to decentralised PV generating unit integration considering power system reliability improvement [3].

In general, high penetration levels of PV generating units increase power system reliability unless if the generation of slack bus does not vary. It is possible that PV system with high repair time strategy of CPS can diminish overall system reliability in both test systems. ICT protection scheme of selected substations can mitigate negative effects on EENS. ICT protection scheme varies EENS between 0.1% and 1.4% compared conventional transmission system in both distributed and centralised cases. In addition, it might be more effective to select low repair time strategy for CPS to mitigate effect of labour cost during repair-time of PV generating units. Although the integration of distributed PV generation systems is more beneficial than centralised PV generation systems, the propagation of cyber-intrusions can be constrained by centralised PV connection nodes with substation protection elements. On the other hand, ICT protection scheme with RBTS diminishes EENS between 13% and 25% level compared to conventional RBTS. The complete approach reduces the complexity of the assessment process and shows the applicability of availability framework of CPS of PV generating in other traditional operating practices [3].

4.4 Summary

This chapter introduces an innovative probabilistic framework for power system reliability assessment in order to analyse the integration of PV powered systems with CPS component interactions. A portion of the proposed model calculates the availability-unavailability of the CPS's interactions at PV generating unit nodes using homogeneous Markov Chain transitions. The entire concept diminishes the complexity of the evaluation procedure and ensures an innovative pathway to analyse system reliability in a holistic way.

Presented case studies have shown that integration effects of PV generating units on power grid and varying cyber-threats were inconsistent with varying the capacity levels of PV generating units. Locations of PV generating units and their topology interactions are much more forceful on the effects in comparison to the intermittent characteristics of PV generating units. The propagation of cyber-intrusions can be restricted with centralised PV generating unit integration though the integration of decentralised PV generating units are more beneficial as oppose to the integration of centralised PV generating units. Therefore, the large-scale integration of PV generating units can be limited more when the operation of power systems comprises of ICT environment with CPS operations compared to the conventional operational practices [3].

Chapter 5: Power System Reliability Analysis with Cyber-Physical Interactive Operation of Heat Pump Systems

5.1 Introduction

The energy sector is undergoing a period of transformation from a conventional power systems towards intelligent and carbon-free technologies. The importance of information and communication technologies (ICTs) has inevitably been escalated in the power grid as a result of increasing penetration level of distributed generation and their capability of bidirectional communication. ICTs have become a critical part of a power grid infrastructure due to their essential features for the power system's economic, reliable and secure operation. ICTs' two-way communication interactivity with distributed energy resources, such as with heat pumps integrated in a power system, may potentially increase the cyber-physical vulnerabilities of a power system. As a consequence, this can affect the reliability of power systems

The aim of this chapter is to propose the model of heat pumps and then to assess the power system reliability with cyber-physical interactive operation. A composite system availability assessment framework with piecewise consideration of heat pump systems' elements is proposed for reduce complexity of the reliability assessment. In addition, a new algorithm incorporating cyber intrusion process with heat pumps and cyber-physical interactive operation of a power system is proposed for the assessment of the reliability of the entire system.

This chapter is structured with the following sections. Relevant research work related to cyber-attack modelling is explored considering smart grid applications, and the limitations of previous research work are discussed in subsection 5.1.1. In section 5.2, the mathematical framework of cyber-attack model and power system reliability model with heat pump (HP) systems are presented. In section 5.3, the power system reliability evaluation with cyber-intrusion on HP systems is exemplified by case studies and then their results are analysed and discussed. Following this, section 5.4 is a summary of the research work that has been presented in this chapter.

5.1.1 Status Quo of the research problem

Increasing installations of cyber-physical based systems such as Advanced Metering Infrastructures (AMI), bring wide-ranging advantages, but also open doors for cyber-attack agents to access end-users' energy data, understand system weaknesses and the criticality of consumer for the system operation. By accessing end-users' information, data alteration or manipulation, intruders can force the system into abnormal states and even cause power outages. Because of their harmful and unexpected nature, prevention of cyber-attacks has been recognized as a critical issue in the power sector. While there is little disclosed data at present, there have been two well documented cases of power-related cyber-attacks which are as follows: At the end of 2015, the Ukraine's power distribution system was exposed to a sophisticated cyber-attack [35]. The pre-attack period was started months before the attack-day and, hackers observed and determined the intrusion pathways in the power grid [35]. As a result, data of key assets was manipulated and almost 225,000 customers experienced a black-out for several hours [35]. Cyber-attack incidents on distributed energy resources (DER), as well as electric vehicles have also been reported. According to [164], an electric car was hacked

through a mobile application of cyber-vulnerability. Hackers gained the control of the vehicle's air-conditioner in approximately 10 seconds and drained its battery during the cyber-incident [164]. Unfortunately, there is a limited information on the reconnaissance and sojourn time duration of cyber-attacks. As can be noticed from these two cyber incidents reported in [35, 164], cyber threats have different time scales, unpredictable acts, different reconnaissance and waiting (sojourn) times for different technologies and platforms. These complex features increase complexities in cyber-attack intrusion modelling for a power system significantly.

Cyber-intrusion process modelling has received considerable critical attention. In [165], a study which was conducted to quantify security failures due to cyber vulnerabilities considering conventional computer system layers. It was found that although the security failure quantification in the study was well designed, the time scale identification of cyber layer's detection-attack agents present in the study was limited [165]. A recent study [166], utilized a semi-Markov process [167] in a similar way as in [165] to investigate the probability of a successful cyber-attack process. The difference between cyber-intrusion methodology applied in [166] and the methodology implemented in [165] is that different reconnaissance and waiting time scale ranges were created in the former. When the detection-agent time interval was modified with different limits, the cyber-attack waiting (sojourn) time in each layer and pre-attack (reconnaissance) time changed significantly. Thus, changes on calculation of cyber-attack waiting and pre-attack times has an effect on cyber-attack impact analysis. In addition to [165, 166], the same methodology of cyber-intrusion process was used in [168]. Reference [168] differs from [166] only in the cyber-attack types and pathways. The studies [166, 168] did not take into account the futuristic characteristic of system smart components, smart capability of layers in the procedure and sophisticated attacks.

5.2 The Mathematical Framework of Cyber-physical Interactive Operations Considering Heat Pump Systems

5.2.1 State Transition Model for Smart Grid

As reported by National Electric Sector Cybersecurity Organization Resource (NESCOR) in [169], power systems need a different manner to preserve critical infrastructures for present and future developments. Hence, power system studies also require distinctive approaches in order to assess futuristic features of smart grid elements. As stated in Figure 5.1,

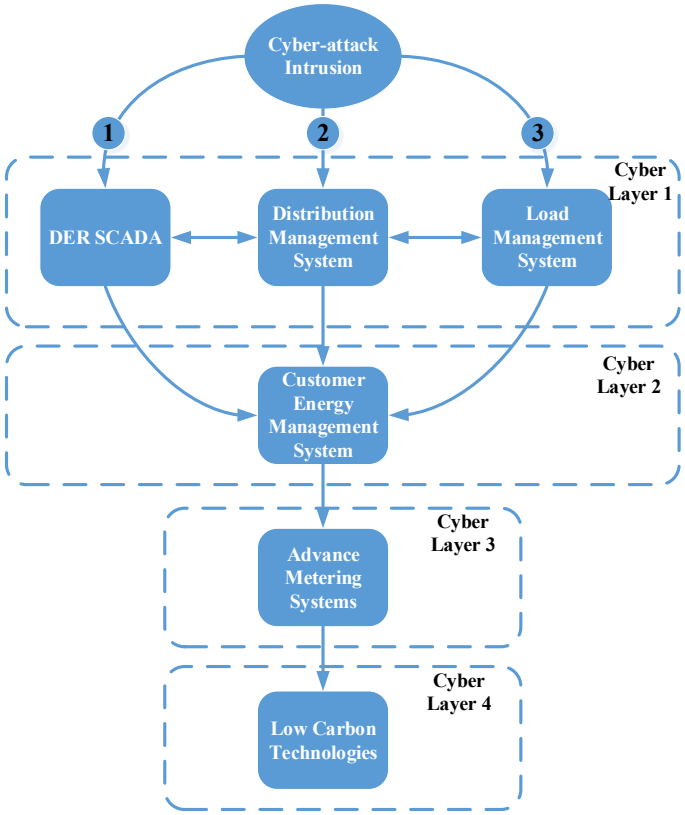


Figure 5.1 Generic attack tree graph for smart grid environment

the study considers three different typical process ways to reach successful cyber intrusion for smart grid. This chapter selected only intrusion path 1 (Figure 5.1) through the DER SCADA

(Supervisory Control and Data Acquisition of Distributed Energy Resources) to show the cyber-attack process in a power grid. All three intrusion pathways have equal probabilities to compromise a cyber-attack. To demonstrate intrusion path calculations, the final canonical form of transition matrix of K is used as follows:

$$K = \begin{bmatrix} T & C \\ 0 & I \end{bmatrix} \tag{5.1}$$

$$T = \begin{bmatrix} 1-P_1 & P_1 & 0 & 0 & 0 & 0 \\ 1-P_2 & 0 & P_2 & 0 & 0 & 0 \\ 1-P_3 & 0 & 0 & P_3 & 0 & 0 \\ 1-P_4 & 0 & 0 & 0 & P_4 & 0 \\ 1-P_5 & 0 & 0 & 0 & 0 & P_5 \\ 1-P_6 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{5.2}$$

where T (5.2) represents state transition probabilities that [167] demonstrates state transitions of semi-Markov model for smart grid, and sub-matrix C refers to transition probabilities between the layers. According to these probabilities, there are six distinctive phases P_1–P_6 that are defined as secure and failed system states respectively. In this cyber-intrusion process, the cyber-attack tries to get an advantageous status to pass to the next phase. Thus, P_1, P_2, P_3, P_4, and P_5 demonstrate the probability of each phase for cyber-intrusion to pass to the next state

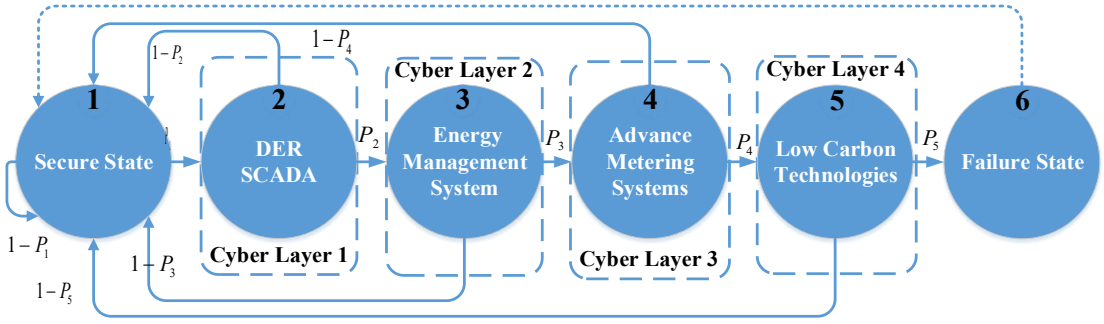


Figure 5.2 Semi-Markov model for cyber-attack states

(Figure 5.2). The cyber-intrusion process is successful only if the attack reaches absorption state P_6 of the system.

5.2.2 Calculation Procedure for Cyber Intrusion Process Times

5.2.2.1 Definitions and Assumptions for Intrusion Process

The mission of an attack-agent is to gain a privilege status in a particular period against the detection agent. A smart-attack-agent needs to help to the attack-agent for simplifying cyber-intrusion preparations in a certain amount of time. In addition, the detection agent must spend some time to detect the cyber-intrusion to isolate the attack and limit to successful-attack intrusion in each cyber-layer. By means of playing this cyber game in between agents, $MTTC_{Cyber}$ (Mean Time to Compromise for Cyber-attack) can be computed. It is defined as a statistical time variant that is to obtain the required mean time value to go from the normal status to the abnormal status of the system. Moreover, $MTTD_{Cyber}$ (Mean Time to Detection for Cyber-attack) refers to another statistical time value that is cyber-forensic with physical restoration time and this is necessary for the statistical probability evaluation of a successful cyber-attack intrusion ($P_{Cyber\text{-}attack}$). These two statistical values of threats can vary with attack type, frequency, strength and severity of layers etc. Their statistical relation is presented as follows:

$$P_{Cyber-attack} = \frac{MTTD_{Cyber}}{MTTD_{Cyber} + MTTC_{Cyber}} \tag{5.3}$$

Statistical calculation of $P_{Cyber\text{-}attack}$ in (5.3) can be utilized in power system reliability and resiliency assessments. The investigation aim is to present the smart attack agent role in a process of intrusion and to assess the impact on the statistical value of $MTTC_{Cyber}$. Additionally, the study has some assumptions related to cyber-intrusion process. They are as follows:

- The investigation considered the mission of a cyber-attack is to force the system to the abnormal states. The system has a detection agent in each cyber layer that adversely effects the detection of threats and preserves the system at normal conditions.

- Available detection systems in the cyber-security sector have been designed with available cyber-attack data, which are assumed as normal attacks, in a dataset [170]. Intelligent attacks or smart-attacks are accepted as unknown and unseen attacks.

- The investigation assumed component characteristics of a power system would change with smart features that would include subordinate smart firewalls and smart detection assets. As a result, the investigation includes the detection agents for cyber-attack detection. Each cyber layer has a smart detection system and different ability against threats in order to minimize their impacts on the system. Thus, the detection time is considered in a random manner.

- The attacker agent needs to spend some time to gain trust of the cyber layer in order to get an authorization for passing next stage of smart grid. Additionally, it is assumed that the target of the attacker is to cause harm to a smart meter or control panel of HPs for energy theft from end users.

- The intruder is presumed to inject bad data into the system for manipulation of energy reading measurements and the detector is supposed to have a capability of anomaly behavior detection because of generic $MTTD_{Cyber}$ estimation for present study.

5.2.2.2 Calculation of $MTTC_{Cyber}$

This sub-section aims to introduce statistical calculations of cyber-attack waiting (sojourn) times in each cyber layer and total intrusion process time. A fundamental instrument is to develop cyber intrusion occurrence and its waiting time in each cyber-physical layer. Hence, it is vital to point out the calculation of the required time for each attack phase as well as the full attack process. In order to quantify security levels of cyber-physical components on the smart grid, the $MTTC_{Cyber}$, refers to requisite time to go from secure to failure status of the system that is implemented for power system reliability evaluations. As previously mentioned, normal attack $f(X_i^n)$, smart-attack $f(X_i^n)$, and detection agents$f(Y_i)$ are introduced.

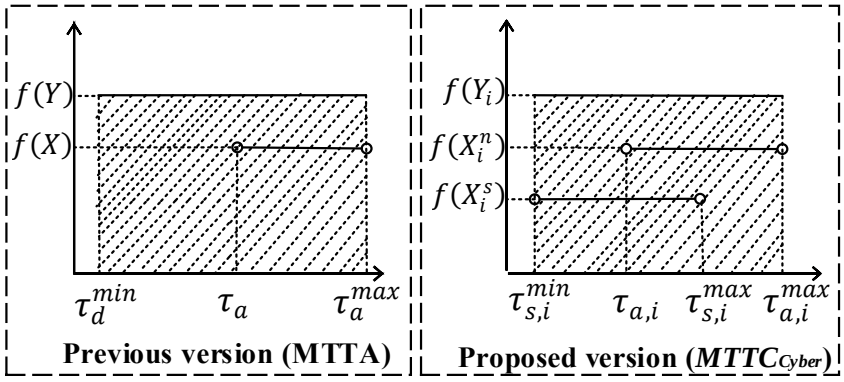


Figure 5.3 Comparison of calculation procedures of MTTA and $MTTC_{Cyber}$

The difference between this chapter approach and previous studies in [165, 166] on $MTTC_{Cyber}$ calculation is to consider the implementation of a smart-attack agent in each layer. Figure 5.3 shows the difference between previous studies approaches on calculation of MTTA (Mean time to Attack) [165, 166] and the proposed approach on $MTTC_{Cyber}$ in this chapter. As

given in equations (5.5 and 5.6), $[\tau_{a,i}, \tau_{a,i}^{max}]$ and $[\tau_{s,i}^{min}, \tau_{s,i}^{max}]$ are utilized for lower-upper boundary limits of normal attack agent and smart attack agent in each phase respectively.

This study models attack and defense times while incorporating uniform distributions. To begin the calculation process, let X_i^n and X_i^s denote normal attack and smart-attack time needed during *i*-th phase of cyber intrusion for attack and smart-attack agent. Therefore, the total attack time equals to normal attack time plus smart-attack time of each phase. In this study, corresponding attack intervals are selected in from uniformly distributed random numbers. Time range and density functions can be expressed by (5.4), (5.5) and (5.6):

$$0 < \tau_{s,i}^{min} < \tau_{a,i} < \tau_{s,i}^{max} < \tau_{a,i}^{max} < +\propto \tag{5.4}$$

$$f(X_i^n) = \begin{cases} \dfrac{1}{\tau_{a,i}^{max} - \tau_{a,i}}, & \tau_{a,i} < X_i^n < \tau_{a,i}^{max} \\ 0, & otherwise \end{cases} \tag{5.5}$$

$$f(X_i^s) = \begin{cases} \dfrac{1}{\tau_{s,i}^{max} - \tau_{s,i}^{min}}, & \tau_{s,i}^{min} < X_i^s < \tau_{s,i}^{max} \\ 0, & otherwise \end{cases} \tag{5.6}$$

As described in (5.5) and (5.6), $[\tau_{a,i}, \tau_{a,i}^{max}]$ and $[\tau_{s,i}^{min}, \tau_{s,i}^{max}]$ are utilized for lower-upper boundary limits of X_i^n and X_i^s in each phase respectively.

Whereas X_i^n and X_i^s refer to the total operations of attack times, Y_i refers to the detection time of the cyber intrusion during *i*-th phase for detection agent. To select appropriate time intervals for Y_i, uniform distribution function is applied in the present study. The Y_i detection time interval is chosen as $[\tau_{s,i}^{min}, \tau_{a,i}^{max}]$ for each cyber layer. In each phase of the system, relation on determination of successful attack intrusion and detection probability are presented by:

$$P(Y_i < [X_i^n + X_i^s]) + P(Y_i > [X_i^n + X_i^s]) = 1 \tag{5.7}$$

As stated in (5.7), the probability of successful detection, where $P(Y_i < [X_i^n + X_i^s])$, is computed by using conditional probability theorem as:

$$P(Y_i < [X_i^n + X_i^s]) = \int P(Y_i < [X_i^n + X_i^s] | [X_i^n + X_i^s] = \tau)\, f_{[X_i^n + X_i^s]}(\tau)\, d\tau =$$

$$\Rightarrow \left\{ \begin{array}{c} \dfrac{3(\tau_s^{min})^2 - 2(\tau_s^{min} - \tau_a) - 2\tau_s^{max} + (\tau_a)^2 - (\tau_s^{max})^2 + (\tau_a^{max})^2}{2\left(\tau_s^{min} - \tau_s^{max}\right)\left(\tau_s^{min} - \tau_a^{max}\right)} + \\ \dfrac{\left(2\tau_s^{min} - \tau_a - \tau_s^{max}\right)(\tau_a - \tau_s^{max})\left((\tau_a)^2 - (\tau_s^{max})^2 + 2\tau_s^{min}(\tau_s^{max} - \tau_a)\right)}{4\left(\tau_s^{min} - \tau_s^{max}\right)\left(\tau_s^{min} - \tau_a^{max}\right)^2(\tau_a^{max} - \tau_a)} + \\ \dfrac{\tau_s^{min}}{\tau_s^{min} - \tau_a^{max}} \end{array} \right\} \quad (5.8)$$

While the probability of successful detection at each phase of the system is as in (5.8), waiting (sojourn) time W_i at each phase of the system is referred to $Z_i = min\{Y_i, [X_i^n + X_i^s]\}$. By the help of [165], waiting time (W_i) at each phase is calculated for the transient state.

$$W_i = \int_{\tau_{s,i}^{min}}^{\tau_{a,i}^{max}} (1 - P(Z_i \le \tau))\, d\tau = \int_{\tau_{s,i}^{min}}^{\tau_{a,i}^{max}} P(min\{Y_i, [X_i^n + X_i^s]\} \ge \tau))\, d\tau =$$

$$\Rightarrow \frac{1}{18} \left\{ \begin{array}{c} \dfrac{(\tau_a - \tau_s^{max})^5(2\tau_a + \tau_s^{max} - 3\tau_a^{max})}{\left(\tau_s^{min} - \tau_s^{max}\right)^3(\tau_a - \tau_a^{max})} + \dfrac{6(\tau_s^{max} - \tau_a^{max})^3}{\left(\tau_s^{min} - \tau_a^{max}\right)(\tau_a^{max} - \tau_a)} \\ - \dfrac{3\left(\tau_s^{min} - \tau_a\right)\left(2(\tau_a)^2 + 2\left(\tau_s^{min}\right)^2\right)}{\left(\tau_s^{min} - \tau_s^{max}\right)\left(\tau_s^{min} - \tau_a^{max}\right)} \\ - \dfrac{3\left(\tau_s^{min} - \tau_a\right)\left(6\tau_a^{max}\tau_s^{max} - 3\tau_a(\tau_s^{max} + \tau_a^{max})\right)}{\left(\tau_s^{min} - \tau_s^{max}\right)\left(\tau_s^{min} - \tau_a^{max}\right)} \\ - \dfrac{3\left(\tau_s^{min} - \tau_a\right)\left(\tau_s^{min}\left(2\tau_a - 3(\tau_s^{max} + \tau_a^{max})\right)\right)}{\left(\tau_s^{min} - \tau_s^{max}\right)\left(\tau_s^{min} - \tau_a^{max}\right)} \end{array} \right\} \quad (5.9)$$

The $MTTC_{Cyber}$ is calculated according to the procedure obtained by[165, 171]. It is as follows:

$$MTTC_{Cyber} = \sum_{i=transition} N_i W_i \quad (5.10)$$

where N_i is expected statistical number of times in i transient state phase that the system reaches failure state finally. It is considered as in [171] and is written (5.11):

$$N_i = q_i \sum_j N_j T_{ji} \tag{5.11}$$

where q_i denotes the probability of the process starts from state i. It is assumed that the initial status is the secure state.

As explained previously, calculation process of $MTTC_{Cyber}$ needs to be carefully examined due to disparities (time intervals, severity of layers etc.) between each cyber/system layer characteristics. Taking into consideration these disparities, security of each cyber layer could be quantified more accurately with this process. It is assumed that each layer behaves differently against cyber intrusion during the process due to future characteristics of smart grids. Each layer could have a different impact on statistical calculations of $MTTC_{Cyber}$. For this reason, calculation process of cyber intrusion probability ($P_{Cyber\text{-}attack}$) is carefully examined with effect of $MTTD_{Cyber}$.

As far as $MTTC_{Cyber}$ is concerned, $MTTD_{Cyber}$ plays an essential role when evaluating $P_{Cyber\text{-}attack}$ as well as cyber-physical system reliability. It is important to highlight that the system will remain in the failure status for a certain amount of time until the detection agent catches the attacker. In this study, detection time denotes detection time plus recovery time of the system. Therefore, it is necessary that detection time ($MTTD_{Cyber}$) identification for $P_{Cyber\text{-}attack}$ calculations is essential. This unique value could change according to attack type, frequency, strength and severity of layers etc. As previous studies stated [166, 168, 172], there is no available real data for detection time. These studies [166, 168, 172] utilize a constant number for $MTTD_{Cyber}$, which should be different statistical value in each system. For this

reason, this mean detection time needs to be determined according to statistical analysis of detection agent's capabilities. Within this target, this study has tried to understand fundamental behaviour of detection processes and underlying distribution of detection time. There is a large volume of published studies describing the role of intrusion detection related to computer science. Mainly, intrusion detection studies are classified into two types: misuse and anomaly detection[173, 174]. As the aim of the attacker is energy theft from consumers with false data injection, the study only considered as anomaly detection of the detection time. In the anomaly-based detection mechanism, the intruder can only be detected if it acts in a different way compared to legitimate behaviour of the system. Thus far, several studies have indicated that intrusion detection process could obey heavy-tail distribution characteristics [175-177]. Heavy-tail distributions are probability density functions that their tails are not limited exponentially. The results show that detection time follows heavy-tail distribution nature, especially in [176]. Sampling path of a heavy-tailed featured system declines slowly, and its efficacy falls over time. Therefore, heavy tail distributions have been utilized for sampling of many extreme event such as floods, tsunamis etc. Because cyber-attacks are considered as rare and extreme events and they are less extreme over time due to not being anymore as unseen threats [176, 178], marginal distribution of intrusion detection times may follow heavy tail pattern. On the other hand, some previous studies confirmed the effectiveness of Gaussian distribution on intrusion detection process [179, 180]. As in [179], system error is assumed to follow normal distribution. Reference [180] has confirmed that manipulated data may pursue Gaussian distribution if adversary has information on detection technique. As a result of many variables and uncertainties in relation of adversary and detection, statistical value of $MTTD_{Cyber}$ is considered as a random number. By the help of MATLAB, these random numbers are determined from a

pool that has a specific range and distribution technique. $MTTD_{Cyber}$ is carefully chosen from following pool with pre-defined distribution:

$$4h = \alpha_1 \leq MTTD_{Cyber} \leq \alpha_2 = 1000h$$

$$MTTD_{Cyber} = \left| \alpha_2 + (\alpha_1 - \alpha_2) \times \left\{ (select\ a\ random\ number) \begin{matrix} randp \\ randn \\ gprnd \\ stblrnd \end{matrix} \right\} \right| \quad (5.12)$$

$\alpha_1$and α_2 are considered as lower and upper boundaries of detection time, respectively. For this study, heavy tail (General Pareto, Stable, Pareto distributions) and Gaussian distributions are utilized for selection of $MTTD_{Cyber}$ in each case. One might disagree with upper boundary limit of $MTTD_{Cyber}$ due to inexperience of power sector on cyber-intrusions, but restoration of the system could take more than a month [163]. Having discussed how to calculate $MTTC_{Cyber}$ *and* $MTTD_{Cyber}$, the following section of this chapter addresses component-based reliability model for heating system.

5.2.3 Component-based Reliability Modelling for Heating System

Heat pumps are becoming a fundamental property of a smart grid and low carbon transitions. As a result of an increase in the installment rate of heat pump and its deployment projection in power grids [181], effect of heat pumps on power system reliability needs to be addressed carefully. The study utilizes a common implementation model of heating system in a power grid to compute composite system availability with piecewise element consideration [182]. By doing so, Markov transition models are developed for the heating system and heating system model is divided into three subsections as in Figure 5.4. It consists of control panel (λ_C, μ_C), heat pump and auxiliary heater with switch (λ_H, μ_H), and storage (λ_{Str}, μ_{Str}) as a

series system respectively. This system is modelled with 8-state Markov transition matrix (M_8) if there is a successful cyber-intrusion.

$$M_4=\begin{bmatrix} -\lambda_H-\lambda_{Str} & \lambda_H & \lambda_{Str} & 0 \\ \mu_H & -\mu_H-\lambda_{Str} & 0 & \lambda_{Str} \\ \mu_S & 0 & -\mu_{Str}-\lambda_H & \lambda_H \\ 0 & \mu_{Str} & \mu_H & -\mu_H-\mu_{Str} \end{bmatrix} \tag{5.13}$$

$$M_8=\begin{bmatrix} -\lambda_C-\lambda_H-\lambda_{Str} & \lambda_C & \lambda_H & \lambda_{Str} & 0 & 0 & 0 & 0 \\ \mu_C & -\mu_C-\lambda_H-\lambda_{Str} & 0 & 0 & \lambda_H & 0 & \lambda_{Str} & 0 \\ \mu_H & 0 & -\lambda_C-\mu_H-\lambda_{Str} & 0 & \lambda_C & \lambda_{Str} & 0 & 0 \\ \mu_{Str} & 0 & 0 & -\lambda_C-\lambda_H-\mu_{Str} & 0 & \lambda_H & \lambda_C & 0 \\ 0 & \mu_H & \mu_C & 0 & -\mu_C-\mu_H-\lambda_{Str} & 0 & 0 & \lambda_{Str} \\ 0 & 0 & \mu_{Str} & \mu_H & 0 & -\mu_H-\mu_{Str}-\lambda_C & 0 & \lambda_C \\ 0 & \mu_S & 0 & \mu_C & 0 & 0 & -\mu_C-\mu_{Str}-\lambda_H & \lambda_H \\ 0 & 0 & 0 & 0 & \mu_S & \mu_C & \mu_H & -\mu_C-\mu_H-\mu_{Str} \end{bmatrix} \tag{5.14}$$

Whether there is a cyber-intrusion, the availability calculation considers a 4-state Markov model (M_4) that involves sub-section 2 and 3. The sub-section 1 of heating system is considered as a control panel that has a capability of two-way communication and stores consumer reading data. Its statistical values of failure-recovery against cyber-intrusion plays a key role for availability analysis of all system. For this purpose, we introduce $P_{Cyber\text{-}attack}$ calculation in previous parts.

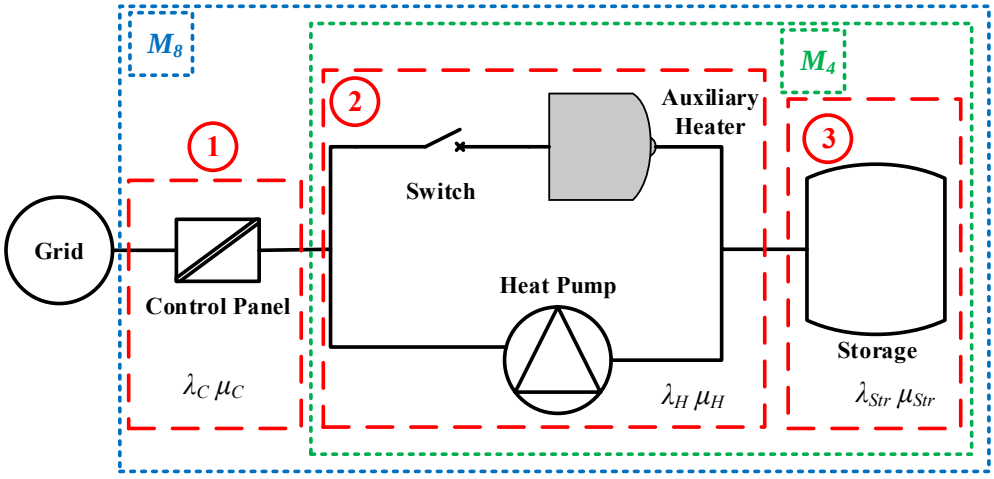


Figure 5.4 Single Line Block Diagram of Generic Heating System Configuration

By means of $P_{Cyber\text{-}attack}$, the study estimates λ_C, μ_C composite availability analysis of cyber-physical system. Following that, the sub-section 2 is composed of a heat pump (λ_{HP}, μ_{HP}), a switch ($\lambda_{Switch}, \mu_{Switch}$) and an auxiliary heater (λ_{AH}, μ_{AH}). In addition, the estimated availability of a heat pump is determined with its internal elements that includes an evaporator (λ_{Eva}, μ_{Eva}), a compressor ($\lambda_{Comp}, \mu_{Comp}$), a condenser ($\lambda_{Cond}, \mu_{Cond}$), and an expansion valve ($\lambda_{Evalve}, \mu_{Evalve}$) as a series internal system. One of the generic heat pump models [182] is demonstrated in Figure 5.5.

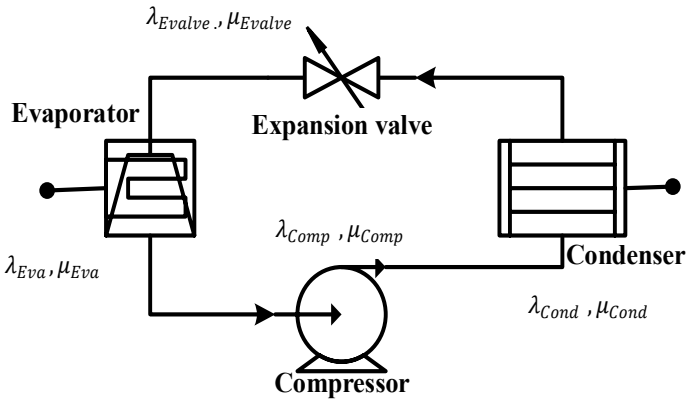


Figure 5.5 Single Line Blok Diagram of Generic Heat Pump's elements

Defining series or parallel arrangement of any system has a significant importance on reliability calculations [3]. Thus, formulas (5.15)-(5.18) are adapted as a fundamental part of the reliability calculation of a heat pump (λ_H, μ_H):

$$\frac{P_f}{P_r} = \frac{\lambda_{System}}{\mu_{System}} \Longrightarrow \lambda_{System} = \mu_{System} \times P_f \times {P_r}^{-1} \tag{5.15}$$

$$P_{r_{HP}} = \left(\frac{\mu_{Comp}}{\lambda_{Comp} + \mu_{Comp}} \times \frac{\mu_{Cond}}{\lambda_{Cond} + \mu_{Cond}} \times \frac{\mu_{Evalve}}{\lambda_{Evalve} + \mu_{Evalve}} \times \frac{\mu_{Eva}}{\lambda_{Eva} + \mu_{Eva}}\right) \Longrightarrow P_{f_{HP}} = 1 - P_{r_{HP}} \tag{5.16}$$

$$\lambda_{HP} = \lambda_{Comp} + \lambda_{Cond} + \lambda_{Evalve} + \lambda_{Eva} \tag{5.17}$$

$$\mu_{HP} = \lambda_{HP} \times P_{r_{HP}} \times {P_{f_{HP}}}^{-1} \tag{5.18}$$

Once the reliability of internal components of a heat pump is computed, a series arranged auxiliary heater with a switch must be involved in reliability calculations by (5.19)-(5.21):

$$P_{r_{AH}} = \left(\frac{\mu_{AH}}{\lambda_{AH} + \mu_{AH}} \times \frac{\mu_{Switch}}{\lambda_{Switch} + \mu_{Switch}}\right) \Longrightarrow P_{f_{AH}} = 1 - P_{r_{AH}} \tag{5.19}$$

$$\lambda_{AH_{Total}} = \lambda_{AH} + \lambda_{Switch} \tag{5.20}$$

$$\mu_{AH_{Total}} = \lambda_{AH_{Total}} \times P_{r_{AH}} \times {P_{f_{AH}}}^{-1} \tag{5.21}$$

After completion of reliability calculations for series arranged components (λ_{HP}, μ_{HP}-$\lambda_{AH_{Total}}, \mu_{AH_{Total}}$), a parallel arrangement of estimated failure-repair rates is used to reach the final calculation of(λ_H, μ_H) via (5.22)-(5.24):

$$P_{f_H} = \left(\frac{\lambda_{AH_{Total}}}{\lambda_{AH_{Total}} + \mu_{AH_{Total}}} \times \frac{\lambda_{HP}}{\lambda_{HP} + \mu_{HP}}\right) \Longrightarrow P_{r_H} = 1 - P_{f_H} \tag{5.22}$$

$$\mu_H = \mu_{AH_{Total}} + \mu_{HP} \tag{5.23}$$

$$\lambda_H = \mu_H \times P_{f_H} \times {P_{r_H}}^{-1} \tag{5.24}$$

The final sub-section is assumed as heat storage of which the, failure and repair rate are denoted by λ_{Str}, μ_{Str}.Taken together all, piecewise reliability calculation will incorporate the Markov model of heating system to compute the system availability at a top down level.

5.2.4 Availability Analysis for Heating System with Cyber-physical Component

In this study, a framework is presented to calculate overall system availability, and it is an indicator of system reliability. 4-state(M_4) and 8-state (M_8) stochastic transition matrices represent system state probabilities. To determine and simply these system state probability

vectors, Markov transition matrixes are implemented into the following equation (5.25) by means of: [183]

$$\overline{P(t)} = \sum_{i=1}^{n} S_i \overline{v_i} e^{v_i \tau} \tag{5.25}$$

where v represents the eigenvalues of a transpose matrix M, $\overline{v}$ is the eigenvectors of transpose matrix M and S denotes a constant that is calculated according to the initial system state. Afterwards, the general problem solution is the assayed for 4-state and 8-state transitions as given by in (5.26):

$$\overline{P(t)}_{n-state} = \sum_{i=1}^{n} S_i \overline{v_i} e^{v_i \tau} = S_1 \overline{v_1} e^{v_1 \tau} + \cdots + S_n \overline{v_n} e^{v_n \tau} \tag{5.26}$$

In general, the system availability is evaluated as a one of the factors for reliability analysis. Availability and unavailability of the system can be represented by operational and non-operational system state probabilities respectively. It is written as in (5.27):

$$\overline{P(t)} = P_1(t) + \cdots + P_n(t) = A(t) + U(t) \tag{5.27}$$

To calculate $S_1, \ldots, S_n$ constant values for the availability, considering the system at t=0 is in fully-operational state($P_1|_{t=0} = 1;\ P_2|_{t=0} = 0; \ldots;\ P_n|_{t=0} = 0$), (5.28) is expressed as:

$$\left(1 \underbrace{0 \cdots 0}_{n-1}\right)^{T}_{n-state} = \sum_{i=1}^{n} S_i \overline{v_i} e^{v_i \tau} = S_1 \overline{v_1} e^{v_1 \tau} + \cdots + S_n \overline{v_n} e^{v_n \tau} \tag{5.28}$$

The solution for any n-state Markov chain is as in (5.29):

$$\begin{array}{lllllllll} P_1(t) = & S_1 v_{11} e^{v_1 \tau} & + & S_2 v_{12} e^{v_2 \tau} & + & \cdots & + & S_n v_{1n} e^{v_n \tau} \\ P_2(t) = & S_1 v_{21} e^{v_1 \tau} & + & S_2 v_{22} e^{v_2 \tau} & + & \cdots & + & S_n v_{2n} e^{v_n \tau} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ P_n(t) = & S_1 v_{n1} e^{v_1 \tau} & + & S_2 v_{n2} e^{v_2 \tau} & + & \cdots & + & S_n v_{nn} e^{v_n \tau} \end{array} \quad (5.29)$$

5.2.5 Power System Reliability Assessment in a Smart Grid

This study has considered composite-system availability as a factor of power system reliability analysis with cyber-intrusion effects. If there are external effects on a power system from the latest system drivers which could be a control panel of heating system, then traditional power system reliability analysis should evolve to assess the impact of these cyber-physical components of control panel. It is assumed that the control panel of heating system is linked to smart meter. System designers and decision makers of power grids should examine the operational reliability even if there is not a cyber-intrusion through a heating system. Regular assessment can help to avoiding system loses and blackouts [184]. Composite system availability analysis and its reliability calculation procedure are described in the Figure 5.6 with following steps:

i. Select the relevant reliability data for each component of a heating system, generators, transformers, lines and buses; determine heat pump profile pool and time intervals for each cyber-layer transitions.

ii. Randomly select a day and a heat pump user for HP load profile.

iii. Extract HP load for time t from selected profile. Initialize number of intrusion attempts

iv. Model $MTTC_{Cyber}$ *and* $MTTD_{Cyber}$ according to sections 5.2.2.1 and 5.2.2.2 with given time intervals for each cyber-layer transitions.

v. Check the number of successful cyber-intrusions within the assumed 100 attempts in time t. This process is depicted as in (5.30):

$$F_{Cyber} = \begin{cases} 0, & r \leq P_{Cyber-attack} \\ 1, & r > P_{Cyber-attack} \end{cases} \quad (5.30)$$

Where F_{Cyber} denotes number of successful cyber-intrusion attempts within 100 attempts and r is a random number. F_{Cyber} is a function that helps to estimate failures of cyber-physical system. Initial condition of successful cyber-intrusion attempt $A_{successful}$ is zero. If the attempt success to be higher than r, $A_{successful}$ is increased. Estimated failure rate of control panel is expressed as $\lambda_1 = 1/A_{successful}$ for time t.

vi. By means of $r \leq P_{Cyber-attack}$, relevant stochastic transition matrix can be chosen.

vii. According to a relevant transition matrix system, calculate updated failure-repair rates of heating sub-systems as in section 5.2.3.

viii. Afterwards, compute the eigenvectors and the eigenvalues of the system as in section 5.2.4 and build relevant composite system availability function for at time t.

ix. Quantify availability function according the system state. The study assumes that the target of the attacker is to manipulate data on control panel readings. If the attacker has successfully intruded into the control panel, the attacker transforms the original load data of HP and increases meter reading in the unavailability level (%) of system at time t.

x. Re-generate HP load value and re-produce it for time t. Afterwards, Extract re-generated HP load profiles.

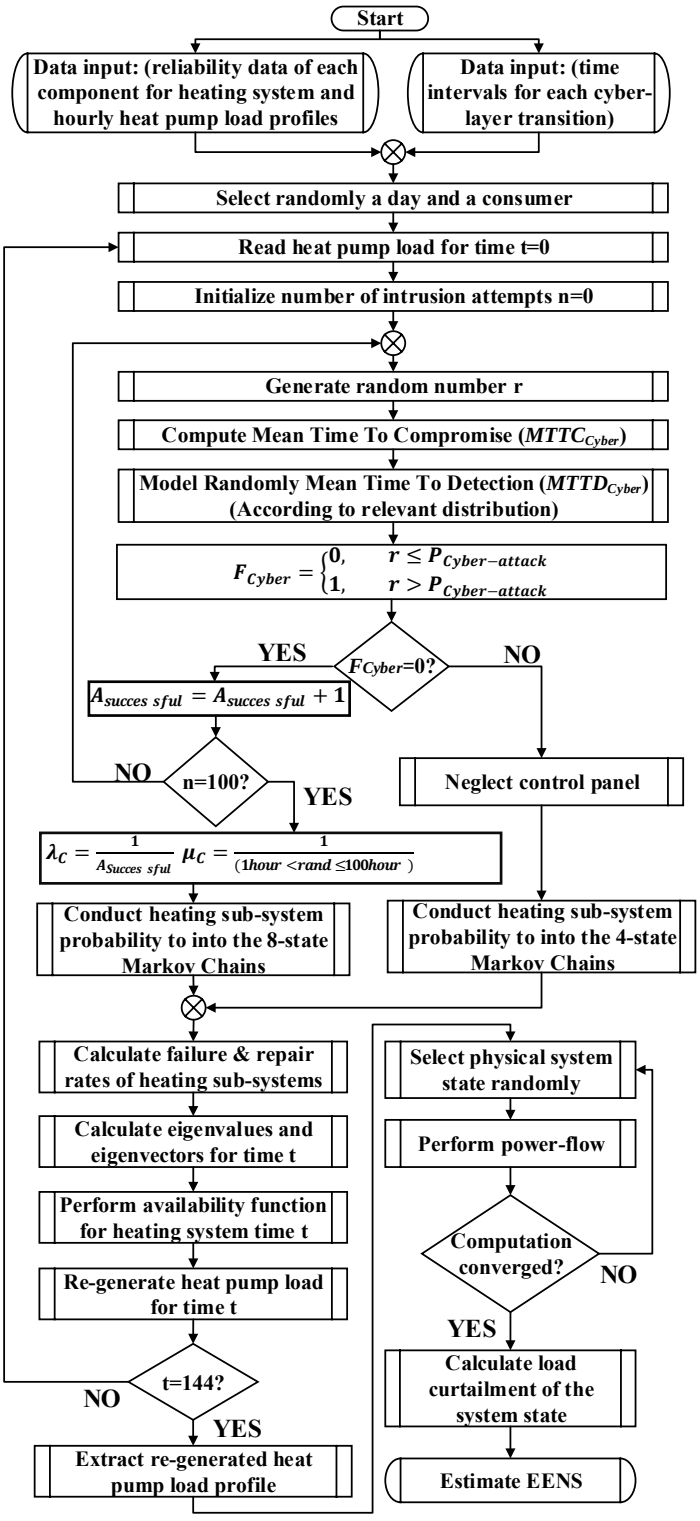


Figure 5.6 Power system reliability calculation framework with cyber-intrusion process

xi. Select physical system state randomly.

xii. Perform power flow considering power balance with global voltage limits.

xiii. If the computation is not converged, go to xi.

xiv. Compute load curtailment of the whole system.

xv. Estimate the EENS.

5.3 Case Studies and Analysis

In this section, the case studies are performed with the Roy Bilinton Test System (RBTS) [185]. The RBTS consists of six buses with 11 generators and 9 power transmission lines. The total installed generation capacity and peak load is 240 MW and 185 MW respectively. The RBTS topology is modified with 100 heat pump users' integrated on Bus 2 and Bus 3.

5.3.1 Input Data for Cyber-Intrusion Process in Smart Grid

This part explains the data utilized for reliability analysis of case studies. The reliability analysis of heating systems utilizes the data is shown in Table 5.1. This data is gathered from [186].

Table 5.1 Reliability Data for Heat Pump System [186]

Components	λ (Failure rate/y)	μ (Repair rate/y)
Compressor	0.01354	0.1153
Condenser	0.0268	0.1394
Evaporator	0.00404	0.068
Expansion valve	0.00027	0.3333
Storage	0.00404	0.0551
Switch	0.00628	0.2381
Auxiliary Heater	0.0536	0.3862

Table 5.2 Utilized Time Intervals for a Smart Distribution Systems

Cyber-layer Transitions	τ_s^{min}(h)	τ_a (h)	τ_s^{max}(h)	τ_a^{max}(h)
Secure to L_1	[1-4]	----	----	[50-60]
L_1 to L_2	[1-4]	[14-18]	[35-45]	[50-60]
L_2 to L_3	[1-4]	[14-18]	[50-60]	[60-70]
L_3 to L_4	[1-4]	[14-18]	[50-60]	[60-70]
L_4 to F	[1-4]	[14-18]	[50-60]	[60-70]
F to S	[1-4]	----	----	[50-60]

On the other hand, time intervals for calculation of $MTTC_{Cyber}$ are randomly selected from Table 5.2 for each phase. The study assumes that each cyber layer has its own time characteristic and the capability of the attacker will have a different approach on waiting (sojourn) time. As a result of this, time intervals of sojourn time should be carefully chosen according to the capability of each cyber-layer. These values are assumed as in Table 5.2 because of the data availability on sojourn time. Heat pump load profile data is allocated from open source [187]. This data consists of heat pump load profiles of 19 customer over a month during the heating season [187]. Since data accuracy and cleansing, the study only uses HP load data of 10 customers for re-generating HP load profiles. Utilized HP data has been randomly chosen from 350 HP load profile samples of data pool [187].

5.3.2 Scenario 1: Cyber-attack on HP during Peak Times

The aim of the attacker is to malfunction the heat pump user site and manipulate electricity usage of each HP user. It is assumed that the attacked HP site includes 100 end-users in total. Due to not being caught by a system operator, the hacker affects the operation of the HP during peak times with 20-minute ranges. It is selected because of the assumption of the heat pump cycle completion in 20 minutes. The scenario asks what happens on the system

reliability if a cyber-attack can intrude the heating system in a small discrete time range during peak hours. According to original HP load profiles, the peak hours are divided into two parts: morning (03:00-09:00) and night times (18:00-22:30). The detection-recovery time ($MTTD_{Cyber}$) calculations are developed with four different distribution techniques for this study. The availability calculation of heating system relies on random number generation of detection time ($MTTD_{Cyber}$) by means of following distributions. These are:

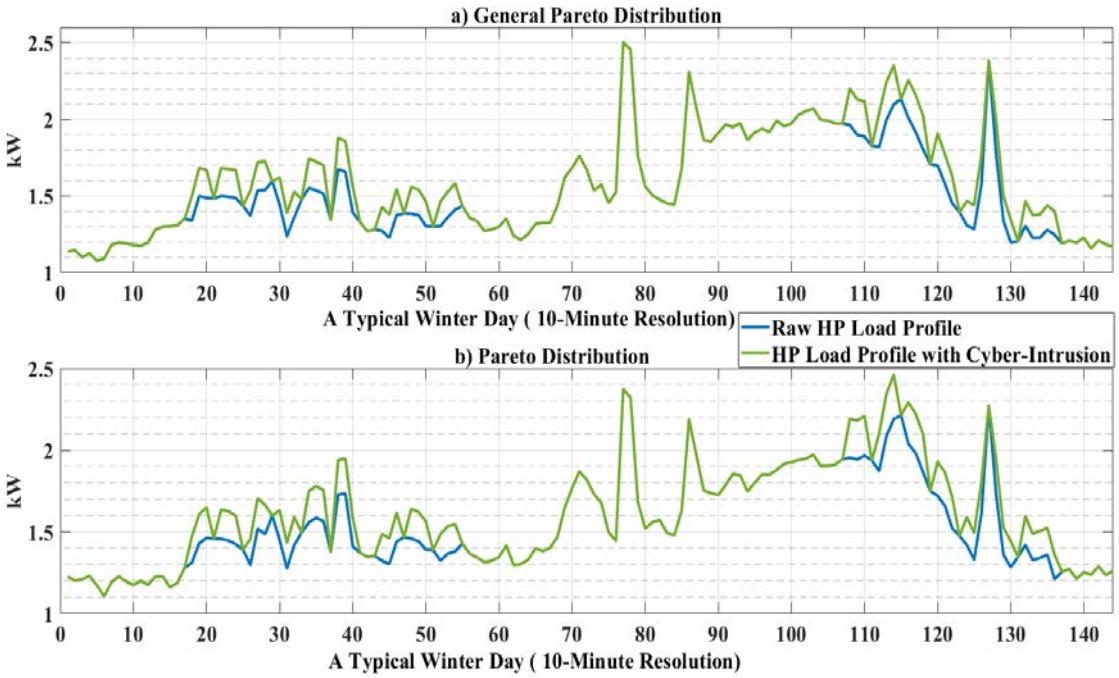


Figure 5.7 Comparison of raw aggregated HP load profile and HP load profile with cyber-intrusion (cyber-intrusion only during the peak times) - a) $MTTD_{Cyber}$ is considered as a General Pareto random number, b) $MTTD_{Cyber}$ is considered as a Pareto random number

Pareto, General Pareto, Gaussian and Stable distributions. Figure 5.7 and Figure 5.8 describe comparison of aggregated original HP load profile and HP load profile with cyber-intrusion in consideration of different distributions of $MTTD_{Cyber}$. As can be seen from Figure 5.7 and Figure 5.8, the main character of the threat's impact is to increase load demand of HP during morning and night peak times. The increment on utilized electricity in each aggregated

profile follows a slight change. There is a clear discrete upward trend of electricity utilization roughly 0.1-0.3 kW during peak hours. This is because of the unavailability ratio of the heating system that is the result of attacks. Figure 5.7 follows a similar pathway and the peak load demand reaches around 2.5 kW. On the other hand, aggregated HP load profiles with Gaussian (Figure 5.8) and Stable (Figure 5.8) distribution random numbers have higher peak (2.9 kW) than Pareto distributions related HP load profiles. Surprisingly, it seems that the impact of intrusion on electricity consumption remains in a low-level increase in all cases. Figure 5.7 and Figure 5.8 illustrate some of the main effects of the discrete time cyber-intrusion on power system reliability.

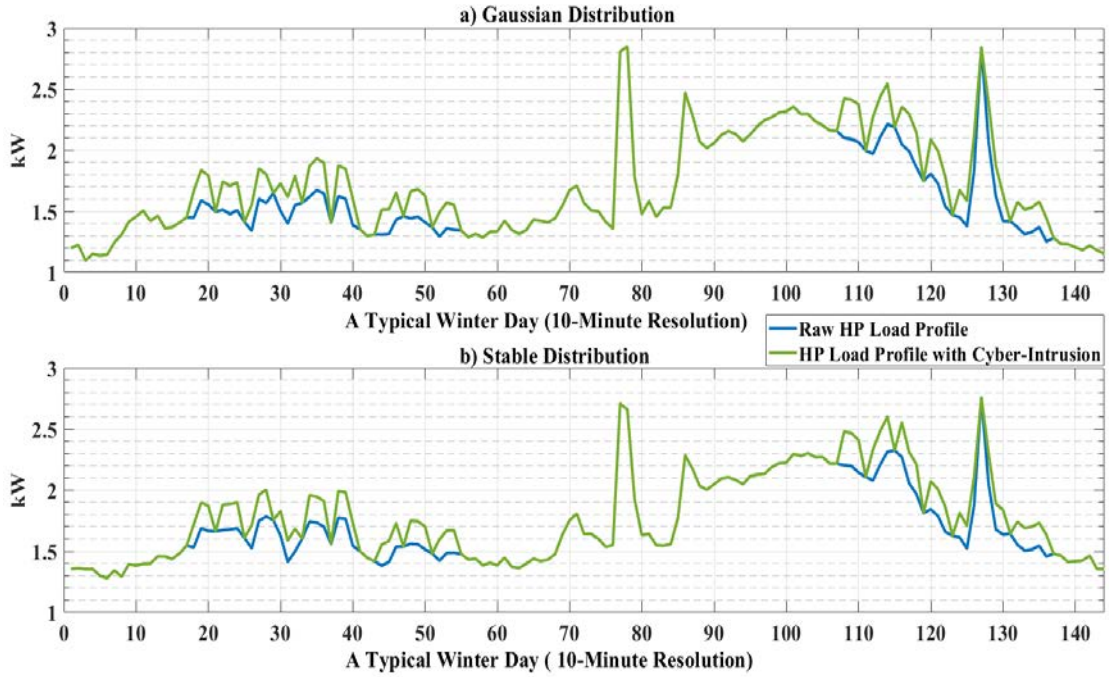


Figure 5.8 Comparison of raw aggregated HP load profile and HP load profile with cyber-intrusion (cyber-intrusion only during the peak times) - a) $MTTD_{Cyber}$ is considered as a Gaussian random number, b) $MTTD_{Cyber}$ is considered as a Stable random number

What stands out in the Table 5.3 is that the increment on Expected Energy Not Supplied (EENS) changes slightly for all cases. In all cases, disparity range of EENS between affected and original HP load profiles changes between 6.459 MWh/year and 35.407 MWh/year. By analysing Table 5.3 closely, the operational reliability diminishes range between 0.06 % and 0.4 % with 100 end-users. In the purview of operating status of the power systems, the implementation of Scenario 1 into large power demand sites with thousands end-users, the impact of the intrusions may trigger to potential frequency instability as well as leading to cascading failures. In addition, this change on EENS can boost operating costs for the system operator and increase financial losses for end-users.

Table 5.3 EENS Changes for Scenario 1

RBTS Bus 2				
Detection time Technique	General Pareto Distribution	Gaussian Distribution	Pareto Distribution	Stable Distribution
Original HP Profiles (MWh/year)	9500.447	9495.933	9594.718	9828.953
Affected HP Profiles (MWh/year)	9526.679	9504.201	9622.154	9835.412
EENS Disparity (MWh/year)	26.232	8.268	27.436	6.459
RBTS Bus 3				
Original HP Profiles (MWh/year)	9050.037	9174.407	9165.045	9333.123
Affected HP Profiles (MWh/year)	9078.541	9198.608	9200.452	9349.729
EENS Disparity (MWh/year)	28.504	24.201	35.407	16.606

For this scenario, Bus 3 is has greater impact than Bus 2 in the context of a reliability performance. The affected load profiles of General Pareto and Pareto distributions follow very similar pathways. However, the unavailability rate of the heating system with these distributions is higher than Stable and Gaussian methods in both buses. It is apparent from results that the unavailability rate of the heating system with stable distribution-detection time

technique is less than other techniques in both buses. It means the performance adaptation of stable detection time ($MTTD_{Cyber}$) on this cyber intrusion process is slightly better than Gaussian detection-time ($MTTD_{Cyber}$) method and others.

As previously mentioned in this chapter, several studies have indicated that intrusion detection process could obey heavy-tail distribution characteristics [175-177]. Detection time follows heavy-tail distribution nature, especially in [176] because of attack-detection process is accepted as extreme event process. Selection of these distribution functions depends on data rate of queuing system of sensors [176]. For instance, heavy tail distributions have been used understanding behaviour of unique electricity price spikes and their extreme volatility characteristics [189]. Optimal selection of heavy-tail distributions for attack-detection process can dependent upon experiences of data sensors of power system if the attack is previously foreseen. Thus, data experience of ICT sensors is going to play a key role in attack-detection time process.

5.3.3 Scenario 2: Cyber-attack on Heat Pump through All Day

Similarly, the target of the intruder is to disturb continuously HP consumers and re-shape the data with the unavailability of the HP system for this scenario. The number of HP users and detection-recovery time methods are same as the Scenario 1. Both Figure 5.9 and Figure 5.10 present an overview of an aggregated original HP load profile and HP load profile with continual effect of cyber-intrusion. Compared to Scenario 1, it can be clearly seen in Figure 5.9 and Figure 5.10 that there is certain amount of electricity rise on HP load demand with each detection time technique. This increase varies between 0.15 kW and 0.4 kW for each aggregated HP load profiles. After cyber-intrusion on the HP user site, the peak HP load reaches almost 3

kW in all cases, except in the Gaussian detection-time method. As shown in Figure 5.10, the peak load peaks at 3.1 kW in the afternoon.

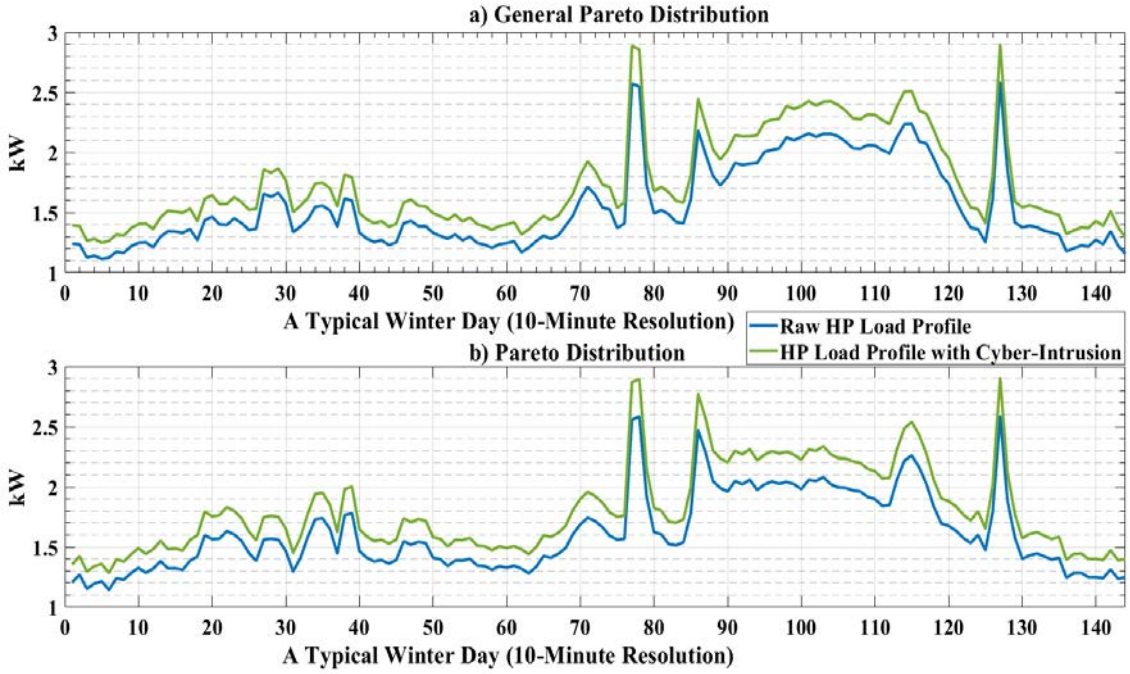


Figure 5.9 Comparison of raw aggregated HP load profile and HP load profile with cyber-intrusion (all day along) - a) $MTTD_{Cyber}$ is considered as a General Pareto random number, b) $MTTD_{Cyber}$ is considered as a Pareto random number

The most striking result to emerge from figures (Figure 5.7, Figure 5.8, Figure 5.9 and Figure 5.10) is that there is another peak time for this HP site, which is around 13:00-14:00. It is because of the small data pool. This increment can be decreased with a high number of end-users who uses HP technology. Table 5.4 provides EENS changes in between aggregated original HP load profile and HP load profile with cyber-intrusion. Table 5.4 also compares different detection-time distribution effect on the system reliability. EENS disparity ranges between 76.366 MWh/year and 161.703 MWh/year. The operational reliability decreases range between 0.8 % and 1.8 % with 100 end-users. The EENS disparity range is much higher than scenario 1 for both of buses. Nevertheless, Bus 2 is affected more than Bus 3 in regard to the

system reliability. The reaction of both the general Pareto and Pareto distribution related detection time method on EENS changes is similar as in Scenario 1.

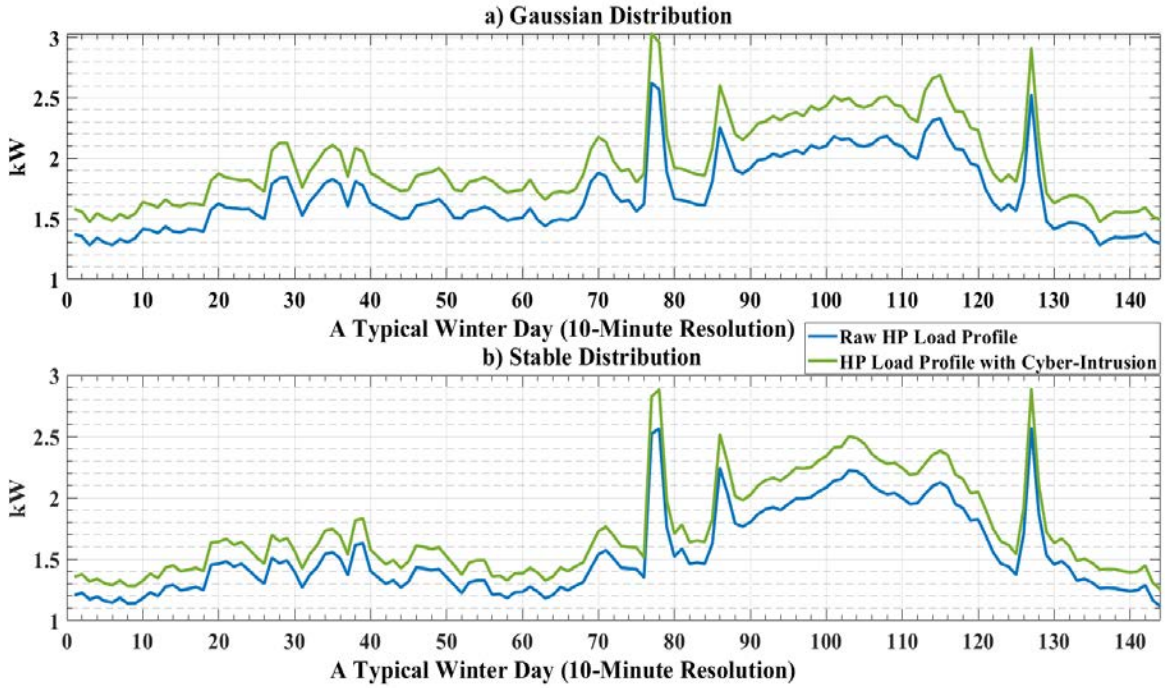


Figure 5.10 Comparison of raw aggregated HP load profile and HP load profile with cyber-intrusion (all day along) - a)$MTTD_{Cyber}$ is considered as a Gaussian random number, b) $MTTD_{Cyber}$ is considered as a Stable random number

However, General Pareto and Pareto distributions have a better EENS performance on detection time compared to others. It shows that unavailability of the heating system with Pareto distribution is less than other methods. These results suggest that General Pareto detection time technique on cyber intrusion process has a better performance on reliability calculations. These scenarios are quite revealing in some ways. First, performance efficacy of detection time techniques can rely on discrete or continuous impact of cyber-intrusions due to the number of data points of detection time analysis.

Table 5.4 EENS Changes for Scenario 2

RBTS Bus 2				
Detection time Technique	General Pareto Distribution	Gaussian Distribution	Pareto Distribution	Stable Distribution
Original HP Profiles (MWh/year)	9610.035	9344.22	9246.872	9267.607
Affected HP Profiles (MWh/year)	9706.609	9489.473	9349.74	9429.31
EENS Disparity (MWh/year)	96.574	145.253	102.868	161.703
RBTS Bus 3				
Original HP Profiles (MWh/year)	9155.525	9094.714	9109.013	9047.479
Affected HP Profiles (MWh/year)	9231.891	9194.847	9186.262	9178.57
EENS Disparity (MWh/year)	76.366	100.133	77.249	131.091

A high number of data points increases the performance of the Pareto distribution technique on the reliability assessment framework and brings less impact on EENS. Secondly, different HP site connections might have a different impact on cyber-intrusion into system power reliability. It is apparent from both scenarios that the impact of cyber-intrusion can be escalated with detection-time durations on the system unavailability. However, the performance of detection time distributions can differ according to data pool size and affected site location characteristics. These factors can be limitations of this study. The most obvious finding to emerge from this study is that the variable $MTTD_{Cyber}$ is well-suited into the estimation of attack probability for the realistic availability assessment of control panel compared to the constant $MTTD_{Cyber}$ due to the stochastic characteristics of the cyber-threats. The attack process with the constant $MTTD_{Cyber}$ in any power system reliability analysis can be limited and bring short-coming for robust assessments.

It is widely acknowledged in power systems that the sudden changes on load demand with high levels, such as demand data manipulations on power infrastructure, can result in

serious consequences with high economic loss. Nevertheless, data manipulation intrusions with load-altering on HPs has remained a challenge until this chapter. Therefore, one of the most essential contributions of this chapter is to reveal such cyber-intrusions' impact with HPs on power system reliability and power system operating perspective.

5.4 Summary

This chapter proposes a composite availability analysis framework for cyber-physical interactive operation with heat pump systems. It is capable of analysing the cyber-intrusion impacts on power system reliability. To evaluate the system reliability, an innovative mathematical framework of the cyber-intrusion process in a smart grid environment for power system applications is presented. Having smart characteristics in a cyber-intrusion process is aimed to illustrate how futuristic characteristics can change calculation of attack-time duration. In addition, a sensitivity analysis of cyber-intrusion detection-time distributions on cyber-physical interactive power system reliability is proposed in order to disclose their compatibility on Mean Time to Detection for Cyber-attack ($MTTD_{Cyber}$). The case study is carried out on the RBTS (Roy Bilinton Test System) for simulating cyber malfunctioning on the control panel of heat pumps (HPs). Scenario 1 evaluates the impact of cyber-intrusions on heating system with discrete time durations within peak times of the day. Scenario 2 analyses the impact of cyber-intrusion on heating system throughout the day (continuous time). According to EENS results, applied heavy tail distributions on detection-time calculations reveal their necessity and adaptability levels on cyber-physical interactive operations of power systems. Not to mention, cyber-intrusion effects on heating system brings noteworthy vulnerability on operational reliability of power systems.

Chapter 6: Conclusions and Future Work

6.1 General Overview

Power systems are usually susceptible to operational malfunctions and faults. These faults are expected to be increased by high-level penetrations of low carbon technologies with Information and Communication Technologies (ICT). It is mainly because of unpredictable behaviours and features of these innovative technologies, escalating the complexity of power grid, its ageing power infrastructure, and accelerating the power system transformation towards smarter concepts.

Power system reliability has been studied by many researchers using different techniques. Reliability assessment techniques are based on the proposed objectives by assessors. Hence, power system reliability assessment methods can change objective by objective. There is no multi-purpose technique in order to solve all power system reliability issues. In general, power system reliability assessment methods can be classified into analytical and Monte Carlo simulation based methods. Also, there are a considerable amount of hybrid reliability study in power systems. This thesis focused on hybrid methodologies to evaluate power system reliability considering Photovoltaic (PV) and Heat Pump (HP) systems with Cyber-physical System (CPS) operation.

As well as the reliability of power systems is already one of the concerns of power system operation, so far, its related evaluation studies consider power systems mostly as a physical property. Nevertheless, by the increasing portion of communication infrastructure integration, power systems have evolved into cyber-physical assets. As a consequence, the

vulnerability of power systems has changed, and brought new additional internal and external concepts such as cyber-vulnerabilities and cyber-malfunctions. This transformation could increase challenges, uncertainties, and affect more reliable operating conditions of power systems. Thus, power system reliability assessment studies without CPS operation and the effects of cyber threats are deficit analysis, and even they are wide of the target of efficient evaluations.

There are several difficulties on the power system reliability assessment with CPS operation. These are mainly: 1) the unpredictability of cyber threats, 2) the severity or intensity of cyber-event, 3) time duration of the cyber event, 4) the damage level of the event, 5) the uncertainty on failure rate and repair times, and 6) the lack of data availability on cyber-threats, their impact and consequences. In general, these difficulties could associate with the inexperience of power sector on cyber-intrusion effects and limitations on the data-sharing of experienced cyber-breaching events due to they are seen as national security issue. As a result, these external factors also increase reliability analysis challenges and complexity on the simulations of CPS availability estimations.

This thesis provided research frameworks associate with the reliability concept of power systems with CPS operation by availability models of PV and HP systems in terms of simplicity and effectiveness.

6.2 Conclusion

6.2.1 Power System Reliability Assessment without CPS Interactive Operation

An analysis framework is proposed for the power system reliability assessment without taking into account CPS components in Chapter 3. The procedural steps of traditional power system reliability analysis is presented in order to examine general effects of PV power generation and load demand. Furthermore, it considers that an increasing amount of centralised & decentralised renewable generation is penetrated into the IEEE RTS79 with different case studies.

Increasing load demand leads to decrease in the system reliability in both original and linerarised load demand scenarios. Linearised load demand has slightly associated with greater EENS values compared to original load demand profiles due to design disparity of load profiles. It can be interpreted that intermittency on load demand can diminish the system reliability up to 1.33%. Results also show that the installation capacity of PV system in the power grid varies with available load capacity. The integration limits of PV generation in the power grid were around 14.75 % and 13.15 % of the base case for linearised and original PV generation profiles when implementing maximum load scale. In addition, PV system installed capacity limits escalated 19.75 % and 17.5 % of base case load capacity with minimum load scale. As a consequence, minimum load scaling factor is more favourable for implementing PV generators compared to maximum load scaling factor, and the location of load in the test system could be another influencing factor for the occurrence of higher penetration of PV generation with minimum load scaling factor.

Not only the intermittent characteristics, but also the location of PV systems have an essential effect on their installed generation capacity in power grid. The results suggest that it does not necessarily mean maximum load capacity can lead to higher penetration levels of PV systems in power grids. Thus, the research emphasises the importance of demand and generation curve selections for power system reliability assessments that can affect the accuracy and robustness of results, accordingly.

6.2.2 Availability model for PV systems with CPS operation in Power System Reliability

A novel stochastic reliability assessment framework is proposed for PV powered systems with cyber-physical interactive operations in order to quantify the degree of risk caused by randomly generated cyber-threats in chapter 4. In addition, the sensitivity of CPS's repair time strategy is presented. Case studies showed that the impact of cyber-threats were variable and unstable against different PV generation levels. Even though the integration of distributed PV generation systems is more beneficial than centralised PV generation systems, the propagation of cyber-intrusions can be constrained by centralised PV connection nodes with substation protection elements. Adding protection elements into substations can improve the system reliability by up to 1.4% for IEEE RTS79. On the other hand, ICT protection scheme with RBTS decreases EENS between 13% and 25% level compared to conventional RBTS. Also, the deployment of large-scale centralised PV generation systems can be restricted, if traditional power system operation practices contain a cyber-physical network. Proposed approach mitigates the complexity of the assessment process. Proposed hybrid framework can be utilised in a vulnerability evaluation in a power system with interactive operation of intermittent generations.

6.2.3 Availability model for HP systems with CPS operation in Power System Reliability

A novel availability-reliability analysis framework is proposed for cyber-physical interactive operation with HPs. This model presents an all-encompassing cyber-intrusion process for data manipulation of the electricity demand of end-users, via various Markov-chain transition models. The major cyber-attack pathways and fundamental intrusion phases are also presented for smart power networks. The proposed cyber-intrusion process is developed with random selection of attack and detection time. By means of this model, the failure rate of the cyber-physical component is estimated in each random intrusion attempt in order to conduct a comprehensive availability analysis of heat pump systems as part of a power system reliability assessment. In addition, a sensitivity analysis of detection-time ($MTTD_{Cyber}$) distributions on the calculation of cyber-attack probability ($P_{Cyber\text{-}attack}$) is proposed in order to evaluate the availability of cyber-physical component of HPs. EENS results show that the implemented detection-time distributions have considerable effects on the cyber-attack probability ($P_{Cyber\text{-}attack}$) as well as on the system availability. Because of the calculation of $P_{Cyber\text{-}attack}$, the operational reliability is unstable. The selection of randomized detection time has significant effects on the statistical calculation of the probability of cyber-intrusions, as well as on power system reliability. Randomised detection time leads to a decrease in operational reliability by up to 1.8%, when only considering 100-heat pump users site. In order to carry out an authentic availability analysis of the CPS component, especially randomized detection time ($MTTD_{Cyber}$) takes an essential role due to cyber-threats' unpredictable features. The most obvious finding to emerge from this research is that the variable $MTTD_{Cyber}$ is well-suited into the estimation of attack probability for the realistic availability assessment of control panel compared to the

constant $MTTD_{Cyber}$ due to the stochastic characteristics of the cyber-threats. The attack process with the constant $MTTD_{Cyber}$ in any power system reliability analysis can be limited and bring short-coming for robust assessments. The insights gained from this study can be of assistance in many avenues including vulnerability analysis for extreme events, and the proposed availability-reliability framework can be useful in the feasibility studies of CPS component integration for power system planning and operation.

Overall, this thesis presents the pathways of the availability calculation of CPS components and essentiality of cyber-intrusion process on complete power system reliability assessments. Applied techniques also reveal necessities and adaptability levels of detection-time approximations in order to calculate cyber-intrusion probability when estimating operational reliability of power systems. Multi-pronged analysis of $MTTD_{Cyber}$ is continuously needed for power system reliability due to random cyber-attack characteristics.

6.3 Recommendations for Future Work

The possible future work is presented as follows:

- *A reliability model with all the cyber-physical components of smart grids in a cyber-physical test bed:* This thesis has proposed the availability modelling for cyber-physical systems and reliability assessment frameworks considering distributed energy resource technologies with their cyber-physical operations. Nevertheless, a complete reliability evaluation needs to consider all cyber, physical and cyber-physical elements with their electrical, communication, operating and control interdependency factors in a real time

with cyber-physically operated test bed. Proposed reliability models in this thesis could be utilized as a baseline for the generalized cyber-physical reliability framework.

- *A value analysis framework for cyber-physical interactive operation of low-carbon technologies:* Power system adequacy analysis plays a key role in a comprehensive power system reliability assessment, and the adequacy analysis with availability frameworks are presented to be utilized in decision-making process. In addition, a value analysis of power systems is another part of the decision making process that alternatively assess power system reliability with economic terms for system operators and planners. In the context of minimum investment maximum profit for energy companies, the value analysis framework including cyber-physical system operations could be beneficial to evaluate the future investment cost of power and communication infrastructure before any decision-making process.
- *A cyber-insurance framework in the context of power system risk assessment:* The reliability-risk studies of power systems mainly remain limited in perspective of cyber-physical system interactions within related studies, and most of them are hardly associated with economy indicators of power systems. As previously mentioned, power systems with cyber-physical components are more vulnerable to cyber-malfunctions and cyber-intrusions. These failures and interruptions can cause high level economic loses during the system operations. The effects of cyber-threats can be minimized but cannot be avoided. Cyber-insurance framework can be referred to as cyber-risk assessment framework and can also be a form of cover to preserve power system utilities from threats, such as data breaches or malicious cyber hacks on work computer systems. As a result, a cyber-insurance framework for utility companies could help to get financial reimbursement for any cyber threats during the system operations. This framework may

be cost-effective and it can positively affect the power system operations. Proposed availability-reliability models in this thesis can also be used as a base for a cyber-insurance risk assessment framework.

Chapter 7: Appendix

7.1 The IEEE Reliability Test System (IEEE-RTS)

In this section, the information of the IEEE Reliability Test System (IEEE-RTS) which was utilised for illustrating the proposed frameworks of Chapter 4 and Chapter 5 is presented [148].

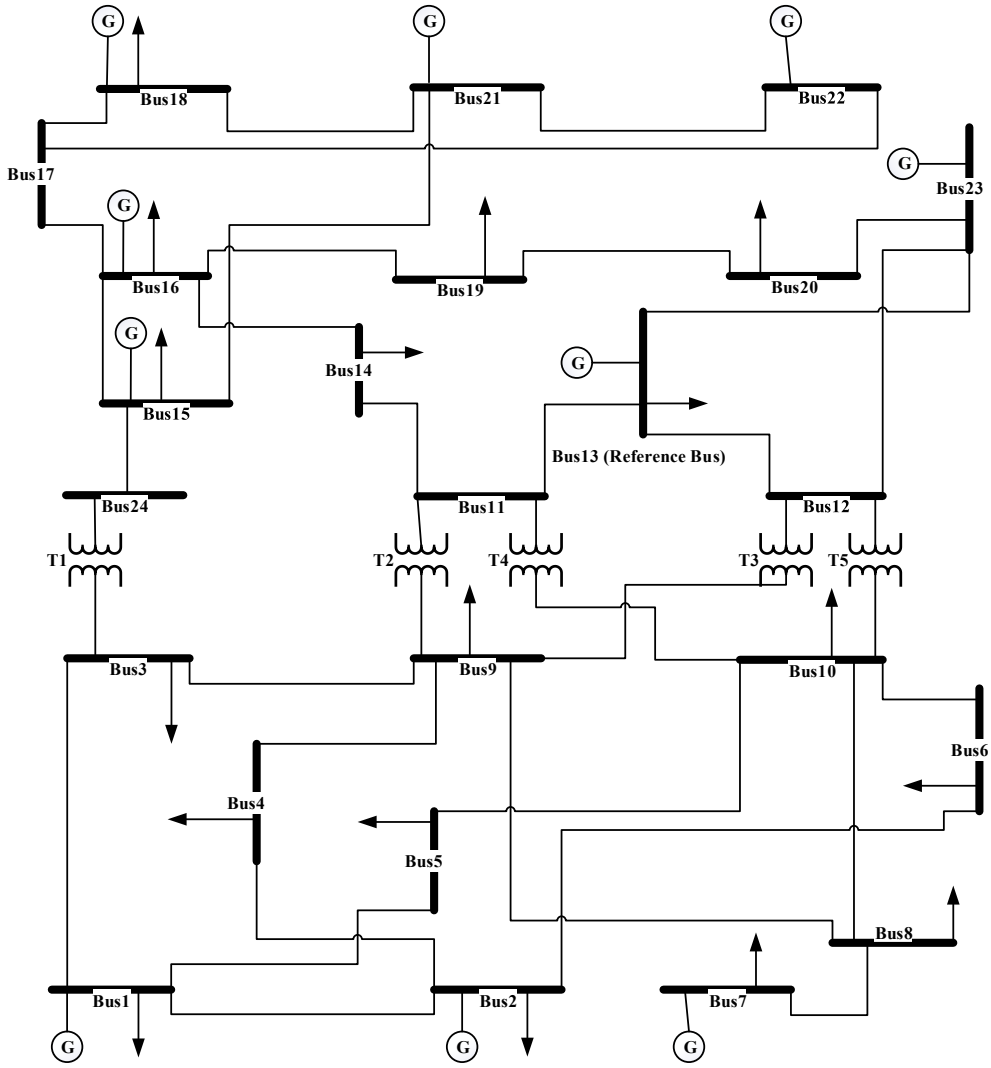


Figure 7.1 IEEE Reliability Test System (IEEE-RTS-24 bus)

Table 7.1 Generator reliability data for IEEE-RTS

Unit Group	Unit Size (MW)	Unit Type	Forced Outage Rate	MTTF (Hours)	MTTR (Hours)	Scheduled Maintenance Weeks per year
U12	12	Oil/Steam	0.02	2940	60	2
U20	20	Oil/CT	0.10	450	50	2
U50	50	Hydro	0.01	1980	20	2
U76	76	Coal/Steam	0.02	1960	40	3
U100	100	Oil/Steam	0.04	1200	50	3
U155	155	Coal/Steam	0.04	960	40	4
U197	197	Oil/Steam	0.05	950	50	4
U350	350	Coal/Steam	0.08	1150	100	5
U400	400	Nuclear	0.12	1100	150	6

Table 7.2 Bus load data for IEEE-RTS

Area/Bus number			% of System Load	Load		If peak load 10% higher	
1	2	3		MW	MVar	MW	MVar
101	201	301	3.8	108	22	118.8	24.2
102	202	302	3.4	97	20	106.7	22.0
103	203	303	6.3	180	37	198.0	40.7
104	204	304	2.6	74	15	81.4	16.5
105	205	305	2.5	71	14	78.1	15.4
106	206	306	4.8	136	28	149.6	30.8
107	207	307	4.4	125	25	137.5	27.5
108	208	308	6.0	171	35	188.1	38.5
109	209	309	6.1	175	36	192.5	39.6
110	210	310	6.8	195	40	214.5	44.0
113	213	313	9.3	265	54	291.5	59.4
114	214	314	6.8	194	39	213.4	42.9
115	215	315	11.1	317	64	348.7	70.4
116	216	316	3.5	100	20	110.0	22.0

118	218	318	11.7	333	68	366.3	74.8
119	219	319	6.4	181	37	199.1	40.7
120	220	320	4.5	128	26	140.8	28.6
Total			100	2850	580	3135	638

Table 7.3 Branch Data for the IEEE-RTS

ID #	From Bus	To Bus	R (p.u.)	X (p.u.)	B (p.u.)	Con (MVA)	LTE (MVA)	STE (MVA)	Tr (p.u.)
1	1	2	0.003	0.14	0.461	175	193	200	0
2	1	3	0.055	0.211	0.057	175	208	220	0
3	1	5	0.022	0.085	0.023	175	208	220	0
4	2	4	0.033	0.127	0.034	175	208	220	0
5	2	6	0.05	0.192	0.052	175	208	220	0
6	3	9	0.031	0.119	0.032	175	208	220	0
7	3	24	0.002	0.084	0	400	510	600	1.015
8	4	9	0.027	0.104	0.028	175	208	220	0
9	5	10	0.023	0.088	0.024	175	208	220	0
10	6	10	0.014	0.061	2.459	175	193	200	0
11	7	8	0.016	0.061	0.017	175	208	220	0
12	8	9	0.043	0.165	0.045	175	208	220	0
13	8	10	0.043	0.165	0.045	175	208	220	0
14	9	11	0.0002	0.084	0	400	510	600	1.03
15	9	12	0.0002	0.084	0	400	510	600	1.03
16	10	11	0.0002	0.084	0	400	510	600	1.015
17	10	12	0.0002	0.084	0	400	510	600	1.015
18	11	13	0.006	0.048	0.1	500	600	625	0
19	11	14	0.005	0.042	0.088	500	600	625	0
20	12	13	0.006	0.048	0.1	500	600	625	0
22	12	23	0.012	0.097	0.203	500	600	625	0
23	13	23	0.011	0.087	0.182	500	600	625	0
24	15	16	0.002	0.017	0.036	500	600	625	0
25	15	21	0.006	0.049	0.103	500	600	625	0
26	15	21	0.006	0.049	0.103	500	600	625	0
27	15	24	0.007	0.052	0.109	500	600	625	0
28	16	17	0.003	0.026	0.055	500	600	625	0
29	16	19	0.003	0.023	0.049	500	600	625	0
30	17	18	0.002	0.014	0.03	500	600	625	0
31	17	22	0.014	0.105	0.221	500	600	625	0
32	18	21	0.003	0.026	0.055	500	600	625	0
33	18	21	0.003	0.026	0.055	500	600	625	0

34	19	20	0.005	0.04	0.083	500	600	625	0
35	19	20	0.005	0.04	0.083	500	600	625	0
36	20	23	0.003	0.022	0.046	500	600	625	0
37	20	23	0.003	0.022	0.046	500	600	625	0
38	21	22	0.009	0.068	0.142	500	600	625	0

CON = Continuous rating

LTE = Long-term emergency rating (24 hour)

STE = Short-term emergency rating (15 min)

Tr = Transformer off-nominal tap ratio

Table 7.4 Branch Reliability Data for the IEEE-RTS

ID #	**From Bus**	**To Bus**	**Permanent**		**Transient**
			λ_p	**Duration**	λ_t
1	1	2	0.24	16	0.0
2	1	3	0.51	10	2.9
3	1	5	0.33	10	1.2
4	2	4	0.39	10	1.7
5	2	6	0.48	10	2.6
6	3	9	0.38	10	1.6
7	3	24	0.02	768	0.0
8	4	9	0.36	10	1.4
9	5	10	0.34	10	1.2
10	6	10	0.33	35	0.0
11	7	8	0.30	10	0.8
12	8	9	0.44	10	2.3
13	8	10	0.44	10	2.3
14	9	11	0.02	768	0.0
15	9	12	0.02	768	0.0
16	10	11	0.02	768	0.0
17	10	12	0.02	768	0.0
18	11	13	0.40	11	0.8
19	11	14	0.39	11	0.7
20	12	13	0.40	11	0.8
22	12	23	0.52	11	1.6
23	13	23	0.49	11	1.5
24	15	16	0.33	11	0.3
25	15	21	0.41	11	0.8
26	15	21	0.41	11	0.8
27	15	24	0.41	11	0.9

28	16	17	0.35	11	0.4
29	16	19	0.34	11	0.4
30	17	18	0.32	11	0.2
31	17	22	0.54	11	1.8
32	18	21	0.35	11	0.4
33	18	21	0.35	11	0.4
34	19	20	0.38	11	0.7
35	19	20	0.38	11	0.7
36	20	23	0.34	11	0.4
37	20	23	0.34	11	0.4
38	21	22	0.45	11	1.2

λ_p = Permanent Outage Rate (outages/year)

Duration = Permanent Outage Duration (hours)

λ_t = Transient Outage Rate (outages/year)

7.2 The Roy Billinton Test System (RBTS)

In this section, the information of the Roy Billinton Test System (RBTS) that was used for demonstrating the proposed framework of Chapter 6 is presented [185].

Table 7.5 Load data for the RBTS

Bus No.	**Load**	
	Active (MW)	**Reactive (MVAR)**
1	0	0
2	20	7
3	85	28
4	40	13
5	20	7
6	20	7

Table 7.6 Line Data for the RBTS

Line No.	Bus		R	X	B/2	Tap	Current Rating (p.u.)	Failure rate (occ/yr)	Repair rate (hrs)
	I	J							
1	1	3	0.0342	0.1800	0.0106	1.00	0.85	1.50	10.0
2	2	4	0.1140	0.6000	0.0352	1.00	0.71	5.00	10.0
3	1	2	0.0912	0.4800	0.0282	1.00	0.71	4.00	10.0
4	3	4	0.0228	0.1200	0.0071	1.00	0.71	1.00	10.0
5	3	5	0.0228	0.1200	0.0071	1.00	0.71	1.00	10.0
6	1	3	0.0342	0.1800	0.0106	1.00	0.71	1.50	10.0
7	2	4	0.1140	0.6000	0.0352	1.00	0.85	5.00	10.0
8	4	5	0.0228	0.1200	0.0071	1.00	0.71	1.00	10.0
9	5	6	0.0228	0.1200	0.0071	1.00	0.71	1.00	10.0

Table 7.7 Generator data for the RBTS

Unit No.	Bus No.	Rating (MW)
1	1	40.0
2	1	40.0
3	1	10.0
4	1	20.0
5	2	5.0
6	2	5.0
7	2	40.0
8	2	20.0
9	2	20.0
10	2	20.0
11	2	20.0

References

[1] H. Gunduz, Z. A. Khan, A. Altamimi, and D. Jayaweera, "An Innovative Methodology for Load and Generation Modelling in a Reliability Assessment with PV and Smart Meter Readings," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*, 2018, pp. 1-5.

[2] W. Li, Reliability assessment of electric power systems using Monte Carlo Methods. Springer Science & Business Media, 2013.

[3] H. Gunduz and D. Jayaweera, "Reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems," *International Journal of Electrical Power & Energy Systems,* vol. 101, pp. 371-384, 2018.

[4] MIT, "Utility of the Future: An MIT Energy Initiative response to an industry in transition " December 2016, Available: energy.mit.edu/uof, Accessed on: 01/05/2019.

[5] Department for Business, Energy & Industrial Strategy, Updated Energy and Emissions Projections 2018, April 2019, Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/794590/updated-energy-and-emissions-projections-2018.pdf, Accessed on: 18/09/2019.

[6] Energy UK, "Pathways for the GB Electricity Sector to 2030," February 2016, Available: https://www.energy-uk.org.uk/publication.html?task=file.download&id=5722, Accessed on: 18/09/2019.

[7] M. Čepin, *Assessment of Power System Reliability*, 1 ed. Springer-Verlag London, 2011, p. 300.

[8] H. Haes Alhelou, M. E. Hamedani-Golshan, T. C. Njenda, and P. Siano, "A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges," vol. 12, no. 4, p. 682, 2019.

[9] H. Farhangi, "The Path of the Smart Grid,", *IEEE Power & Energy Magazine,* vol. 8, no. 1, pp. 18-28, Jan-Feb 2010.

[10] P. Chongfuangprinya, J. Spare, J. R. Aguero, J. H. R. Enslin, and H. Al-Atrash, "Integration of Micro-Scale Photovoltaic Distributed Generation on Power Distribution Systems: Steady-State Analyses," *IEEE PES Transmission and Distribution Conference and Exposition (T&D),* 2012.

[11] A. Ipakchi and F. Albuyeh, "Grid of the Future,", *IEEE Power & Energy Magazine,* vol. 7, no. 2, pp. 52-62, Mar-Apr 2009.

[12] Department of Energy & Climate Change (DECC), August 2010, 2050 Pathways Analysis, Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/68816/216-2050-pathways-analysis-report.pdf , Accessed on: 18/09/2019.

[13] Department of Energy & Climate Change (DECC), August 2013, UK Renewable Energy Roadmap Update 2013. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/255182/UK_Renewable_Energy_Roadmap_-_5_November_-_FINAL_DOCUMENT_FOR_PUBLICATIO___.pdf , Accessed on: 18/09/2019.

[14] REN21, "Renewables 2018 Global Status Report," Paris 2018, Available: http://www.ren21.net/gsr-2018/, Accessed on: 01/05/2019.

[15] International Energy Agency (IEA), "Solar Photovoltaic Energy," 2010, Available: https://www.oecd-ilibrary.org/content/publication/9789264088047-en, Accessed on: 18/09/2019.

[16] Department for Business, Energy & Industrial Strategy, "Digest of UK Energy Statistics (DUKES) 2018: main report and annexes," National Statistics 26 July 2018, Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/736148/DUKES_2018.pdf, Accessed on: 18/09/2019.

[17] F. Katiraei and J. R. Aguero, "Solar PV Integration Challenges," *IEEE Power & Energy Magazine,* vol. 9, no. 3, pp. 62-71, May-Jun 2011.

[18] Department of Energy & Climate Change (DECC), Renewable Heat Incentive, 2011, Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/48041/1387-renewable-heat-incentive.pdf, Accessed on: 18/09/2019.

[19] Delta Energy & Environment (DELTA), "IEA HPP Annex 42: Heat Pumps in Smart Grids, Task 1 (i): Market Overview," 22/01/2014, Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/341742/Delta-ee_Task_1_UK_Market_Report_-_Final.pdf, Accessed on: 18/09/2019.

[20] H. Singh, A. Muetze, and P. C. Eames, "Factors influencing the uptake of heat pump technology by the UK domestic sector," *Renewable Energy,* vol. 35, no. 4, pp. 873-878, 2010.

[21] A. Navarro-Espinosa, N. Good, L. Zhang, P. Mancarella, and L. F. Ochoa, "EHP in low voltage networks: Understanding the effects of heat emitters and room temperatures," in *PowerTech, 2015 IEEE Eindhoven*, 2015, pp. 1-5.

[22] D. Fischer, J. Scherer, A. Flunk, N. Kreifels, K. Byskov-Lindberg, and B. Wille-Haussmann, "Impact of HP, CHP, PV and EVs on households' electric load profiles," in *PowerTech, 2015 IEEE Eindhoven*, 2015, pp. 1-6.

[23] P. Mancarella, G. Chin Kim, and G. Strbac, "Evaluation of the impact of electric heat pumps and distributed CHP on LV networks," in *PowerTech, 2011 IEEE Trondheim*, 2011, pp. 1-7.

[24] Department for Business, Energy & Industrial Strategy, 2018, *Smart Meters*. Available: https://www.gov.uk/government/collections/smart-meters-statistics, Accessed on: 18/09/2019.

[25] Robert M. Lee, Michael J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC2016, Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf, Accessed on: 13/02/2018.

[26] R. Billinton and R. N. Allan, *Reliability Evaluation of Engineering Systems*. New York: Plenum press, 1992.

[27] M. Tortorella, *Reliability, Maintainability, and Supportability: Best Practices for Systems Engineers* (Wiley Series in Systems Engineering and Management). John Wiley & Sons, 2015, p. 430.

[28] "IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries," *IEEE Std 610,* pp. 1-217, 1991.

[29] H. Pham, *System Software Reliability* (Springer Series in Reliability Engineering). Springer-Verlag London, 2006, pp. XIV, 440.

[30] *Fault Tree Analysis (FTA)*, IEC 61025, 2006, Avaliable: https://webstore.iec.ch/publication/4311, Accessed on: 18/09/2019.

[31] *Standard for probabilistic risk assessment for nuclear power plant applications*, ASME *RA-S-2002,* 2002, Avaliable: https://www.nrc.gov/docs/ML0037/ML003733342.pdf, Accessed on: 18/09/2019.

[32] *Standard for Level 1 / Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications*, ASME-RA-S-2008, 2008, Avaliable: https://www.asme.org/codes-standards/find-codes-standards/ra-s-standard-level-1-large-early-release-frequency-probabilistic-risk-assessment-nuclear-power-plant-applications, Accessed on: 18/09/2019.

[33] A. Villemeur, *Reliability, availability, maintainability and safety assessment: methods and techniques*. Newyork: Wiley, 1992.

[34] A. Atputharajah and T. K. Saha, "Power system blackouts - literature review," in *2009 International Conference on Industrial and Information Systems (ICIIS)*, 2009, pp. 460-465.

[35] Robert M. Lee, Michael J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC 2016, Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf, Accessed on: 13/02/2018.

[36] J. A. P. Lopes, F. J. Soares, and P. M. R. Almeida, "Integration of Electric Vehicles in the Electric Power System", *Proceedings of the IEEE,* vol. 99, no. 1, pp. 168-183, Jan 2011.

[37] D. S. Kirschen and D. Jayaweera, "Comparison of risk-based and deterministic security assessments," *IET Generation, Transmission & Distribution,* vol. 1, no. 4, p. 527, 2007.

[38] R. Billinton and R. N. Allan, *Reliability Assessment of Large Electric Power Systems*. Kluwer, Boston, 1988.

[39] "IEEE Standard Terms for Reporting and Analyzing Outage Occurrences and Outage States of Electrical Transmission Facilities," *IEEE Std 859-1987,* p. 0_1, 1988.

[40] "IEEE Standard Definitions for Use in Reporting Electric Generating Unit Reliability, Availability, and Productivity," *IEEE Std 762-2006 (Revision of IEEE Std 762-1987),* pp. 1-75, 2007.

[41] "IEEE Guide for Electric Power Distribution Reliability Indices," *IEEE Std 1366-2012 (Revision of IEEE Std 1366-2003),* pp. 1-43, 2012.

[42] R. Billinton and J. Satish, "Effect of rotational load shedding on overall power system adequacy indices," *IEE Proceedings - Generation, Transmission and Distribution,* vol. 143, no. 2, pp. 181-187, 1996.

[43] A. A. Chowdhury and D. O. Koval, "Value-based power system reliability planning," *IEEE Transactions on Industry Applications,* vol. 35, no. 2, pp. 305-311, 1999.

[44] M. Moeini-Aghtaie, H. Farzin, M. Fotuhi-Firuzabad, and R. Amrollahi, "Generalized Analytical Approach to Assess Reliability of Renewable-Based Energy Hubs," *IEEE Transactions on Power Systems,* vol. 32, no. 1, pp. 368-377, 2017.

[45] M. Moeini-Aghtaie, A. Abbaspour, and M. Fotuhi-Firuzabad, "Incorporating Large-Scale Distant Wind Farms in Probabilistic Transmission Expansion Planning—Part II: Case Studies," *IEEE Transactions on Power Systems,* vol. 27, no. 3, pp. 1594-1601, 2012.

[46] M. Moeini-Aghtaie, A. Abbaspour, and M. Fotuhi-Firuzabad, "Incorporating Large-Scale Distant Wind Farms in Probabilistic Transmission Expansion Planning—Part I: Theory and Algorithm," *IEEE Transactions on Power Systems,* vol. 27, no. 3, pp. 1585-1593, 2012.

[47] R. Billinton, Y. Gao, and R. Karki, "Application of a Joint Deterministic-Probabilistic Criterion to Wind Integrated Bulk Power System Planning," *IEEE Transactions on Power Systems,* vol. 25, no. 3, pp. 1384-1392, 2010.

[48] Y.-Y. Hong and L.-H. Lee, "Reliability assessment of generation and transmission systems using fault-tree analysis," *Energy Conversion and Management,* vol. 50, no. 11, pp. 2810-2817, 2009/11/01/ 2009.

[49] W. Peng and R. Billinton, "Reliability assessment of a restructured power system considering the reserve agreements," *IEEE Transactions on Power Systems,* vol. 19, no. 2, pp. 972-978, 2004.

[50] L. Goel and R. Billinton, "Impacts of pertinent factors on reliability worth indices in an electric power system," *Electric Power Systems Research,* vol. 41, no. 2, pp. 151-158, 1997/05/01/ 1997.

[51] H. Abunima, J. Teh, C.-M. Lai, and H. Jabir, "A Systematic Review of Reliability Studies on Composite Power Systems: A Coherent Taxonomy Motivations, Open Challenges, Recommendations, and New Research Directions," *Energies,* vol. 11, no. 9, p. 2417, 2018.

[52] R. Allan, "Power system reliability assessment—A conceptual and historical review," *Reliability Engineering & System Safety,* vol. 46, no. 1, pp. 3-13, 1994/01/01/ 1994.

[53] A. D. Patton, J. H. Blackstone, and N. J. Balu, "A Monte Carlo simulation approach to the reliability modeling of generating systems recognizing operating considerations," *IEEE Transactions on Power Systems,* vol. 3, no. 3, pp. 1174-1180, 1988.

[54] J. Juan and I. Ortega, "Reliability analysis for hydrothermal generating systems including the effect of maintenance scheduling," *IEEE Transactions on Power Systems,* vol. 12, no. 4, pp. 1561-1568, 1997.

[55] A. K. Ayoub and A. D. Patton, "A frequency and duration method for generating system reliability evaluation," *IEEE Transactions on Power Apparatus and Systems,* vol. 95, no. 6, pp. 1929-1933, 1976.

[56] C. L. Wee and R. Billinton, "A frequency and duration method for looped configuration generating capacity reliability evaluation," *IEEE Transactions on Power Systems,* vol. 3, no. 2, pp. 698-705, 1988.

[57] N. Amjady and M. Ehsan, "Evaluation of power systems reliability by an artificial neural network," *IEEE Transactions on Power Systems,* vol. 14, no. 1, pp. 287-292, 1999.

[58] F. Pourahmadi, M. Fotuhi-Firuzabad, and P. Dehghanian, "Application of Game Theory in Reliability-Centered Maintenance of Electric Power Systems," *IEEE Transactions on Industry Applications,* vol. 53, no. 2, pp. 936-946, 2017.

[59] J. Setreus, P. Hilber, S. Arnborg, and N. Taylor, "Identifying Critical Components for Transmission System Reliability," *IEEE Transactions on Power Systems,* vol. 27, no. 4, pp. 2106-2115, 2012.

[60] B. Alizadeh and S. Jadid, "A dynamic model for coordination of generation and transmission expansion planning in power systems," *International Journal of Electrical Power & Energy Systems,* vol. 65, pp. 408-418, 2015/02/01/ 2015.

[61] E. N. Dialynas and D. G. Michos, "Impact of supply restoration procedures on the reliability performance of power distribution systems," *Electric Power Systems Research,* vol. 39, no. 2, pp. 111-121, 1996/11/01/ 1996.

[62] H. Zheng, Y. Cheng, B. Gou, D. Frank, A. Bern, and W. E. Muston, "Impact of automatic switches on power distribution system reliability," *Electric Power Systems Research,* vol. 83, no. 1, pp. 51-57, 2012/02/01/ 2012.

[63] R. Arya, "Estimation of distribution system reliability indices neglecting random interruption duration incorporating effect of distribution generation in standby mode," *International Journal of Electrical Power & Energy Systems,* vol. 63, pp. 270-275, 2014/12/01/ 2014.

[64] D. Zhu, R. P. Broadwater, T. Kwa-Sur, R. Seguin, and H. Asgeirsson, "Impact of DG placement on reliability and efficiency with time-varying loads," *IEEE Transactions on Power Systems,* vol. 21, no. 1, pp. 419-427, 2006.

[65] D. Kumar, S. R. Samantaray, I. Kamwa, and N. C. Sahoo, "Reliability-constrained Based Optimal Placement and Sizing of Multiple Distributed Generators in Power Distribution Network Using Cat Swarm Optimization," *Electric Power Components and Systems,* vol. 42, no. 2, pp. 149-164, 2014/01/25 2014.

[66] S. Conti, R. Nicolosi, and S. A. Rizzo, "Generalized Systematic Approach to Assess Distribution System Reliability With Renewable Distributed Generators and Microgrids," *IEEE Transactions on Power Delivery,* vol. 27, no. 1, pp. 261-270, 2012.

[67] M. Mosadeghy, R. Yan, and T. K. Saha, "A Time-Dependent Approach to Evaluate Capacity Value of Wind and Solar PV Generation," *IEEE Transactions on Sustainable Energy,* vol. 7, no. 1, pp. 129-138, 2016.

[68] J. R. Aguero, E. Takayesu, D. Novosel, and R. Masiello, "Modernizing the Grid: Challenges and Opportunities for a Sustainable Future," *IEEE Power and Energy Magazine,* vol. 15, no. 3, pp. 74-83, 2017.

[69] N. Hatziargyriou, H. Asano, R. Iravani, and C. Marnay, "Microgrids," *IEEE Power and Energy Magazine,* vol. 5, no. 4, pp. 78-94, 2007.

[70] F. Li *et al.*, "Smart Transmission Grid: Vision and Framework," *IEEE Transactions on Smart Grid,* vol. 1, no. 2, pp. 168-177, 2010.

[71] R. Billinton and G. Singh, "Application of adverse and extreme adverse weather: modelling in transmission and distribution system reliability evaluation," *IEE Proceedings - Generation, Transmission and Distribution,* vol. 153, no. 1, pp. 115-120, 2006.

[72] D. Fischer and H. Madani, "On heat pumps in smart grids: A review," *Renewable and Sustainable Energy Reviews,* vol. 70, pp. 342-357, 2017/04/01/ 2017.

[73] M. J. Moran and H. N. Shapiro, *Fundamentals of engineering thermodynamics: SI version*, 5th ed. John Wiley & Sons, 2006.

[74] T. Fawcett, "The future role of heat pumps in the domestic sector," presented at the ECEEE 2011 SUMMER STUDY, 2011, Avaliable: https://www.eci.ox.ac.uk/publications/downloads/fawcett11b.pdf, Accessed on: 18/09/2019.

[75] J. Cockroft and N. Kelly, "A comparative assessment of future heat and power sources for the UK domestic sector," *Energy Conversion and Management,* vol. 47, no. 15, pp. 2349-2360, 2006/09/01/ 2006.

[76] UK Power Networks, "Impact of Electric Vehicles and Heat Pump loads on network demand profiles," 2014, vol. B2 Available: https://innovation.ukpowernetworks.co.uk/wp-content/uploads/2019/05/B2-Impact-of-Electric-Vehicles-and-Heat-Pump-Loads-on-Network-Demand-Profiles.pdf, Accessed on: 18/09/2019.

[77] A. Navarro-Espinosa and P. Mancarella, "Probabilistic modeling and assessment of the impact of electric heat pumps on low voltage distribution networks," *Applied Energy,* vol. 127, pp. 249-266, 2014.

[78] A. Arteconi, N. J. Hewitt, and F. Polonara, "Domestic demand-side management (DSM): Role of heat pumps and thermal energy storage (TES) systems," *Applied Thermal Engineering,* vol. 51, no. 1-2, pp. 155-165, 2013.

[79] S. Nykamp, A. Molderink, V. Bakker, H. A. Toersche, J. L. Hurink, and G. J. M. Smit, "Integration of heat pumps in distribution grids: Economic motivation for grid control," in *Innovative Smart Grid Technologies (ISGT Europe), 2012 3rd IEEE PES International Conference and Exhibition on*, 2012, pp. 1-8.

[80] N. Good, L. Zhang, A. Navarro-Espinosa, and P. Mancarella, "High resolution modelling of multi-energy domestic demand profiles," *Applied Energy,* vol. 137, pp. 193-210, 2015.

[81] N. Good, L. X. Zhang, A. Navarro-Espinosa, and P. Mancarella, "Physical modeling of electro-thermal domestic heating systems with quantification of economic and environmental costs," (in English), *2013 Ieee Eurocon,* pp. 1164-1171, 2013.

[82] N. J. Kelly and J. Cockroft, "Analysis of retrofit air source heat pump performance: Results from detailed simulations and comparison to field trial data," *Energy and Buildings,* vol. 43, no. 1, pp. 239-245, 2011.

[83] R. Rocchetta and E. Patelli, "Stochastic analysis and reliability-cost optimization of distributed generators and air source heat pumps," in *2017 2nd International Conference on System Reliability and Safety (ICSRS)*, 2017, pp. 31-35.

[84] S. Zhang, M. Wen, H. Cheng, X. Hu, and G. Xu, "Reliability evaluation of electricity-heat integrated energy system with heat pump," *CSEE Journal of Power and Energy Systems,* vol. 4, no. 4, pp. 425-433, 2018.

[85] J. Jiang, X. Wei, W. Gao, S. Kuroki, and Z. Liu, "Reliability and Maintenance Prioritization Analysis of Combined Cooling, Heating and Power Systems," *Energies,* vol. 11, no. 6, p. 1519, 2018.

[86] J.-J. Wang, C. Fu, K. Yang, X.-T. Zhang, G.-h. Shi, and J. Zhai, "Reliability and availability analysis of redundant BCHP (building cooling, heating and power) system," *Energy,* vol. 61, pp. 531-540, 2013.

[87] C. C. Bendea and G. V. Bendea, "Predictive Reliability Analysis of Ground Coupled Heat Pumps Using Markov Chains," presented at the World Geothermal Congress 2010, Bali, Indonesia, 25-29 April 2010, 2010. Available: https://www.geothermal-energy.org/pdf/IGAstandard/WGC/2010/2926.pdf, Accessed on: 18/09/2019.

[88] P. G. V. Sampaio and M. O. A. González, "Photovoltaic solar energy: Conceptual framework," *Renewable and Sustainable Energy Reviews,* vol. 74, pp. 590-601, 2017/07/01/ 2017.

[89] IEA, "Technology Roadmap: Solar Photovoltaic Energy," International Energy Agency, 2014, Available: http://www.iea.org/publications/freepublications/publication/technology-roadmap-solar-photovoltaic-energy---2014-edition.html, Accessed on: 18/09/2019.

[90] J. R. Aguero and S. J. Steffel, "Integration Challenges of Photovoltaic Distributed Generation on Power Distribution Systems," (in English), *2011 IEEE Power and Energy Society General Meeting,* 2011.

[91] A. Soroudi, M. Aien, and M. Ehsan, "A Probabilistic Modeling of Photo Voltaic Modules and Wind Power Generation Impact on Distribution Networks," *IEEE Systems Journal,* vol. 6, no. 2, pp. 254-259, 2012.

[92] L. F. O. Alejandro Navarro, Dan Randles,Pierluigi Mancarella, "Impacts of Photovoltaics on Low Voltage Networks: A Case Study for the North West of England," presented at the 22nd International Conference on Electricity Distribution(CIRED), Stockholm-Sweden, 2013.

[93] L. F. O. Alejandro Navarro, Dan Randles, "Monte Carlo-Based Assessment of PV Impacts on Real UK Low Voltage Networks," presented at the Power and Energy Society, 2013.

[94] W. S. Ho, H. Hashim, M. H. Hassim, Z. A. Muis, and N. L. M. Shamsuddin, "Design of distributed energy system through Electric System Cascade Analysis (ESCA)," *Applied Energy,* vol. 99, pp. 309-315, 2012/11/01/ 2012.

[95] G. Petrone, G. Spagnuolo, R. Teodorescu, M. Veerachary, and M. Vitelli, "Reliability Issues in Photovoltaic Power Processing Systems," *IEEE Transactions on Industrial Electronics,* vol. 55, no. 7, pp. 2569-2580, 2008.

[96] X. Yuan and Y. Zhang, "Status and Opportunities of Photovoltaic Inverters in Grid-Tied and Micro-Grid Systems," in *2006 CES/IEEE 5th International Power Electronics and Motion Control Conference*, 2006, vol. 1, pp. 1-4.

[97] N. G. Dhere, "Reliability of PV modules and balance-of-system components," in *Conference Record of the Thirty-first IEEE Photovoltaic Specialists Conference, 2005.*, 2005, pp. 1570-1576.

[98] Ankit, S. K. Sahoo, S. Sukchai, and F. F. Yanine, "Review and comparative study of single-stage inverters for a PV system," *Renewable and Sustainable Energy Reviews,* vol. 91, pp. 962-986, 2018/08/01/ 2018.

[99] R. Alonso, E. Roman, A. Sanz, V. E. Mart, S. nez, and P. Ibanez, "Analysis of Inverter-Voltage Influence on Distributed MPPT Architecture Performance," *IEEE Transactions on Industrial Electronics,* vol. 59, no. 10, pp. 3900-3907, 2012.

[100] A. Ristow, M. Begovic, A. Pregelj, and A. Rohatgi, "Development of a Methodology for Improving Photovoltaic Inverter Reliability," *IEEE Transactions on Industrial Electronics,* vol. 55, no. 7, pp. 2581-2592, 2008.

[101] P. Zhang, W. Li, S. Li, Y. Wang, and W. Xiao, "Reliability assessment of photovoltaic power systems: Review of current status and future perspectives," *Applied Energy,* vol. 104, pp. 822-833, 2013.

[102] V. Smet *et al.*, "Ageing and Failure Modes of IGBT Modules in High-Temperature Power Cycling," *IEEE Transactions on Industrial Electronics,* vol. 58, no. 10, pp. 4931-4941, 2011.

[103] A. D. Sairaj V. Dhople, Patrick L. Chapman, and Alejandro D. Domínguez-García, "Integrating Photovoltaic Inverter Reliability into Energy Yield Estimation with Markov Models," in *Control and Modeling for Power Electronics (COMPEL)*, 2010.

[104] R. K. Varma and E. M. Siavashi, "PV-STATCOM: A New Smart Inverter for Voltage Control in Distribution Systems," *IEEE Transactions on Sustainable Energy,* vol. 9, no. 4, pp. 1681-1691, 2018.

[105] S. V. Dhople and A. D. Dominguez-Garcia, "Estimation of Photovoltaic System Reliability and Performance Metrics," *IEEE Transactions on Power Systems,* vol. 27, no. 1, pp. 554-563, 2012.

[106] H. Wang, N. Zhu, and X. Bai, "Reliability model assessment of grid-connected solar photovoltaic system based on Monte-Carlo," *Applied Solar Energy,* vol. 51, no. 4, pp. 262-266, 2015.

[107] Z. Esau and D. Jayaweera, "Reliability assessment in active distribution networks with detailed effects of PV systems," *Journal of Modern Power Systems and Clean Energy,* vol. 2, no. 1, pp. 59-68, 2014.

[108] A. T. Procopiou, J. Quirós-Tortós, and L. F. Ochoa, "HPC-Based Probabilistic Analysis of LV Networks With EVs: Impacts and Control," *IEEE Transactions on Smart Grid,* vol. 8, no. 3, pp. 1479-1487, 2017.

[109] A. T. Procopiou, L. Chao, and L. F. Ochoa, "Voltage control in LV networks: An initial investigation," in *Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2014 IEEE PES*, 2014, pp. 1-6.

[110] R. Bayindir, I. Colak, G. Fulli, and K. Demirtas, "Smart grid technologies and applications," *Renewable and Sustainable Energy Reviews,* vol. 66, pp. 499-516, 2016/12/01/ 2016.

[111] MIT, "Utility of The Future," MIT Energy Initiative 2016, Available: https://energy.mit.edu/wp-content/uploads/2016/12/Utility-of-the-Future-Full-Report.pdf, Accessed on: 18/09/2019.

[112] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems,* vol. 99, pp. 45-56, 2018/07/01/ 2018.

[113] U.S. Department of Homeland Security, NCCIC/ICS-CERT 2015 year in review, 2015, Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf, Accessed on: 18/09/2019.

[114] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in Distributed Power Systems," *Proceedings of the IEEE,* vol. 105, no. 7, pp. 1367-1388, 2017.

[115] H. Wu and M. Shahidehpour, "Applications of Wireless Sensor Networks for Area Coverage in Microgrids," *IEEE Transactions on Smart Grid,* vol. 9, no. 3, pp. 1590-1598, 2018.

[116] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 6, pp. 2442-2451, 2018.

[117] L. Che, X. Liu, Z. Shuai, Z. Li, and Y. Wen, "Cyber Cascades Screening Considering the Impacts of False Data Injection Attacks," *IEEE Transactions on Power Systems,* vol. 33, no. 6, pp. 6545-6556, 2018.

[118] Y. Chen, J. Hong, and C. Liu, "Modeling of Intrusion and Defense for Assessment of Cyber Security at Power Substations," *IEEE Transactions on Smart Grid,* vol. 9, no. 4, pp. 2541-2552, 2018.

[119] K. R. Davis *et al.*, "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," *IEEE Transactions on Smart Grid,* vol. 6, no. 5, pp. 2464-2475, 2015.

[120] T. B. Rasmussen, G. Yang, A. H. Nielsen, and Z. Dong, "Effects of centralized and local PV plant control for voltage regulation in LV feeder based on cyber-physical simulations," *Journal of Modern Power Systems and Clean Energy,* journal article vol. 6, no. 5, pp. 979-991, September 01 2018.

[121] P. Srikantha and D. Kundur, "A DER Attack-Mitigation Differential Game for Smart Grid Security Analysis," *IEEE Transactions on Smart Grid,* vol. 7, no. 3, pp. 1476-1485, 2016.

[122] C. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems," *IEEE Transactions on Smart Grid,* vol. 9, no. 5, pp. 4405-4425, 2018.

[123] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *International Journal of Electrical Power & Energy Systems,* vol. 104, pp. 169-177, 2019/01/01/ 2019.

[124] Y. Xiang, L. Wang, and N. Liu, "A Robustness-Oriented Power Grid Operation Strategy Considering Attacks," *IEEE Transactions on Smart Grid,* vol. 9, no. 5, pp. 4248-4261, 2018.

[125] Z. Yang, C. Ten, and A. Ginter, "Extended Enumeration of Hypothesized Substations Outages Incorporating Overload Implication," *IEEE Transactions on Smart Grid,* vol. 9, no. 6, pp. 6929-6938, 2018.

[126] B. Falahati and Y. Fu, "Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies," *IEEE Transactions on Smart Grid,* vol. 5, no. 4, pp. 1677-1685, 2014.

[127] B. Falahati, Y. Fu, and L. Wu, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," *IEEE Transactions on Smart Grid,* vol. 3, no. 3, pp. 1515-1524, 2012.

[128] M. H. Kapourchali, M. Sepehry, and V. Aravinthan, "Fault Detector and Switch Placement in Cyber-Enabled Power Distribution Network," *IEEE Transactions on Smart Grid,* vol. 9, no. 2, pp. 980-992, 2018.

[129] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," *Applied Energy,* vol. 235, pp. 204-218, 2019/02/01/ 2019.

[130] H. Lei and C. Singh, "Non-Sequential Monte Carlo Simulation for Cyber-Induced Dependent Failures in Composite Power System Reliability Evaluation," *IEEE Transactions on Power Systems,* vol. 32, no. 2, pp. 1064-1072, 2017.

[131] W. Liu, Q. Gong, H. Han, Z. Wang, and L. Wang, "Reliability Modeling and Evaluation of Active Cyber Physical Distribution System," *IEEE Transactions on Power Systems,* vol. 33, no. 6, pp. 7096-7108, 2018.

[132] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power System Reliability Evaluation Considering Load Redistribution Attacks," *IEEE Transactions on Smart Grid,* vol. 8, no. 2, pp. 889-901, 2017.

[133] Y. Xiang and L. Wang, "A game-theoretic study of load redistribution attack and defense in power systems," *Electric Power Systems Research,* vol. 151, pp. 12-25, 2017/10/01/ 2017.

[134] Y. Xiang, L. Wang, and Y. Zhang, "Adequacy evaluation of electric power grids considering substation cyber vulnerabilities," *International Journal of Electrical Power & Energy Systems,* vol. 96, pp. 368-379, 2018/03/01/ 2018.

[135] Y. Zhang, L. Wang, and Y. Xiang, "Power System Reliability Analysis With Intrusion Tolerance in SCADA Systems," *IEEE Transactions on Smart Grid,* vol. 7, no. 2, pp. 669-683, 2016.

[136] Y. Zhang, L. Wang, Y. Xiang, and C. Ten, "Power System Reliability Evaluation With SCADA Cybersecurity Considerations," *IEEE Transactions on Smart Grid,* vol. 6, no. 4, pp. 1707-1721, 2015.

[137] Y. Zhang, L. Wang, Y. Xiang, and C. Ten, "Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation," *IEEE Transactions on Power Systems,* vol. 31, no. 6, pp. 4379-4394, 2016.

[138] Y. Zhang, Y. Xiang, and L. Wang, "Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems," *IEEE Transactions on Smart Grid,* vol. 8, no. 5, pp. 2343-2357, 2017.

[139] X. Liu and Z. Li, "False Data Attacks Against AC State Estimation With Incomplete Network Information," *IEEE Transactions on Smart Grid,* vol. 8, no. 5, pp. 2239-2248, 2017.

[140] B. Moussa, P. Akaber, M. Debbabi, and C. Assi, "Critical Links Identification for Selective Outages in Interdependent Power-Communication Networks," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 2, pp. 472-483, 2018.

[141] H. Wang *et al.*, "Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 11, pp. 4766-4778, 2018.

[142] A. Arif, Z. Wang, J. Wang, B. Mather, H. Bashualdo, and D. Zhao, "Load Modeling—A Review," *IEEE Transactions on Smart Grid,* vol. 9, no. 6, pp. 5986-5999, 2018.

[143] Z. A. Khan and D. Jayaweera, "Approach for smart meter load profiling in Monte Carlo simulation applications," *IET Generation, Transmission & Distribution,* vol. 11, no. 7, pp. 1856-1864, 2017.

[144] Z. A. Khan, D. Jayaweera, and H. Gunduz, "Smart meter data taxonomy for demand side management in smart grids," in *2016 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, 2016, pp. 1-8.

[145] "CER Smart Metering Project - Electrical Customer Behaviour Trial," ed: Irish Social Science Data Archive, 2009-2010.

[146] S. Sobri, S. Koohi-Kamali, and N. A. Rahim, "Solar photovoltaic generation forecasting methods: A review," *Energy Conversion and Management,* vol. 156, pp. 459-497, 2018/01/15/ 2018.

[147] A. Altamimi and D. Jayaweera, "Reliability performances of grid-integrated PV systems with varying climatic conditions," in *IET International Conference on Resilience of Transmission and Distribution Networks (RTDN 2017)*, 2017, pp. 1-6.

[148] C. Grigg *et al.*, "The IEEE Reliability Test System-1996. A report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee," *IEEE Transactions on Power Systems,* vol. 14, no. 3, pp. 1010-1020, 1999.

[149] NIST, "National Institute of Standards and Technology Special Publication 1500-201," in "Natl. Inst. Stand. Technol. Spec. Publ. 1500-201," Smart Grid and Cyber-Physical Systems Program Office, Engineering Laboratory2017, vol. 1 Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf, Accessed on: 18/09/2019.

[150] B. Kang *et al.*, "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," in *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, 2015, pp. 1-8.

[151] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid Risk Analysis Considering the Impact of Cyber Attacks on Solar PV and ESS Control Systems," *IEEE Transactions on Smart Grid,* vol. 8, no. 3, pp. 1330-1339, 2017.

[152] A. W. Miranda and S. Goldsmith, "Cyber-physical risk management for PV photovoltaic plants," in *2017 International Carnahan Conference on Security Technology (ICCST)*, 2017, pp. 1-8.

[153] M. Uslar and R. Bleiker, "Automation for the Smart Grid: IEC 61850 - Substation Automation and DER Communication," in *Standardization in Smart Grids: Introduction to IT-Related Methodologies, Architectures and Standards*Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 115-128.

[154] E. Zio, "Practical Applications of Monte Carlo Simulation for System Reliability Analysis," in *The Monte Carlo Simulation Method for System Reliability and Risk Analysis*London: Springer London, 2013, pp. 83-107.

[155] M. D. Smith and M. E. Paté-Cornell, "Cyber Risk Analysis for a Smart Grid: How Smart is Smart Enough? A Multiarmed Bandit Approach to Cyber Security Investment," *IEEE Transactions on Engineering Management,* vol. 65, no. 3, pp. 434-447, 2018.

[156] R. K. Abercrombie and F. T. Sheldon, "Security Analysis of Smart Grid Cyber Physical Infrastructures Using Game Theoretic Simulation," presented at the IEEE Symposium Series on Computational Intelligence, 2015.

[157] N. J. Daras, "Stochastic Analysis of Cyber-Attacks," in *Applications of Mathematics and Informatics in Science and Engineering*, N. J. Daras, Ed. Cham: Springer International Publishing, 2014, pp. 105-129.

[158] R. E. Brown, *Electric Power Distribution Reliability*, Second ed. Taylor & Francis Group, LLC, 2009.

[159] D. GmbH, "DIgSILENT PowerFactory 15, tutorial.," ed. Germany, 2013.

[160] H. Lei and C. Singh, "Developing a benchmark test system for electric power grid cyber-physical reliability studies," in *2016 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, 2016, pp. 1-5.

[161] "IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems (Gold Book)," *IEEE Std 493-1997 [IEEE Gold Book],* pp. 1-464, 1998.

[162] W. Li, *Risk Assessment of Power Systems: Models, Methods, and Applications*, second ed. 2014.

[163] J. N. S. Dr Rebecca Klahr, Paul Sheriffs, Tom Rossington, Gemma Pestell, Professor Mark Button and Dr Victoria Wang, "Cyber security breaches survey 2017," Ipsos MORI Social Research Institute and Institute for Criminal Justice Studies, University of

Portsmouth, Department for Digital, Culture, Media & Sport of UK Government2017, Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017, Accessed on: 18/09/2019.

[164] M. Hashem Eiza and Q. Ni, "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity," *IEEE Vehicular Technology Magazine,* vol. 12, no. 2, pp. 45-51, 2017.

[165] J. Almasizadeh and M. A. Azgomi, "Intrusion Process Modeling for Security Quantification," *2009 International Conference on Availability, Reliability and Security*, Fukuoka, 2009, pp. 114-121.

[166] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power System Reliability Evaluation Considering Load Redistribution Attacks," *IEEE Transactions on Smart Grid,* pp. 1-1, 2016.

[167] K. S. Trivedi, *Probability & statistics with reliability, queuing and computer Science applications*. New Delhi: PHI Learning Pvt. Ltd., 2011.

[168] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation," *IEEE Transactions on Power Systems,* vol. 31, no. 6, pp. 4379-4394, 2016.

[169] F.Cleveland and A. Lee, "Cyber Security for DER Systems," Electric Power Research Institute (EPRI)2013, Available: http://smartgrid.epri.com/doc/der%20rpt%2007-30-13.pdf, Accessed on: 18/09/2019.

[170] D. Mashima and A. A. Cárdenas, "Evaluating Electricity Theft Detectors in Smart Grid Networks," Berlin, Heidelberg, 2012, pp. 210-229: Springer Berlin Heidelberg.

[171] B. B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems," *Performance Evaluation,* vol. 56, no. 1-4, pp. 167-186, 2004.

[172] Y. Zhang, L. Wang, and Y. Xiang, "Power System Reliability Analysis With Intrusion Tolerance in SCADA Systems," *IEEE Transactions on Smart Grid,* pp. 1-1, 2015.

[173] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys,* vol. 46, no. 4, pp. 1-29, 2014.

[174] H. Song, X. Miao, C. Hsiao-Hwa, and L. Yun, "Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges," *IEEE Systems Journal,* vol. 8, no. 4, pp. 1052-1062, 2014.

[175] P. X. Zheng, B. Chen, L. J. Zheng, G. L. Zhang, Y. L. Fan and T. Pei, "Key issues and technical route of cyber physical distribution system", *International Conference on*

Recent Trends in Physics 2016 (ICRTP2016), Journal of Physics: Conference Series, vol. 755, p. 011001, 2016.

[176] Haining Wang, Danlu Zhang and Kang G. Shin, "Detecting SYN flooding attacks," *Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, New York, NY, USA, 2002, pp. 1530-1539.

[177] J. B. D. Cabrera, J. Gosar, W. Lee and R. K. Mehra, "On the statistical distribution of processing times in network intrusion detection," *2004 43rd IEEE Conference on Decision and Control (CDC) (IEEE Cat. No.04CH37601)*, Nassau, 2004, pp. 75-80 Vol.1.

[178] Kuypers, Marshall A., Thomas Maillart and Elisabeth Paté-Cornell, "An Empirical Analysis of Cyber Security Incidents at a Large Organization," 2016.

[179] P. Y. Chen, S. S. Yang, J. A. McCann, J. Lin, and X. Y. Yang, "Detection of False Data Injection Attacks in Smart-Grid Systems," *IEEE Communications Magazine,* vol. 53, no. 2, pp. 206-213, Feb 2015.

[180] W. Yu, D. Griffith, L. Ge, S. Bhattarai, and N. Golmie, "An integrated detection system against false data injection attacks in the Smart Grid," *Security and Communication Networks,* vol. 8, no. 2, pp. 91-109, 2015.

[181] J. Love *et al.*, "The addition of heat pump electricity load profiles to GB electricity demand: Evidence from a heat pump field trial," *Applied Energy,* vol. 204, pp. 332-342, 2017.

[182] K. J. Chua, S. K. Chou, and W. M. Yang, "Advances in heat pump systems: A review," *Applied Energy,* vol. 87, no. 12, pp. 3611-3624, 2010.

[183] M. S. Alvarez-Alvarado and D. Jayaweera, "Aging Reliability Model for Generation Adequacy," in *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, 2018, pp. 1-6.

[184] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT Botnet of high wattage devices can disrupt the power grid," presented at the Proceedings of the 27th USENIX Conference on Security Symposium, Baltimore, MD, USA, 2018.

[185] R. Billinton and S. Jonnavithula, "A test system for teaching overall power system reliability assessment," *IEEE Transactions on Power Systems,* vol. 11, no. 4, pp. 1670-1676, 1996.

[186] P. S. Hale and R. G. Arno, "Survey of reliability and availability information for power distribution, power generation, and HVAC components for commercial, industrial, and utility installations," *IEEE Transactions on Industry Applications,* vol. 37, no. 1, pp. 191-196, 2001.

[187] UK Power Networks, "Low Carbon London Heat Pump Load Profiles," UK Power Networks, 2014, Avaliable: https://data.london.gov.uk/dataset/low-carbon-london-heat-pump-load-profiles, Accessed :18/09/2019.

[188] J. Qi, A. Hahn, X. Lu, J. Wang and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," in *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28-39, 12 2016.

[189] R. Weron, "Heavy tails and electricity prices." In *The Deutsche Bundesbank's 2005 Annual Fall Conference (Eltville)*. 2005.