RELIABILITY MODELING AND ANALYSIS OF CYBER ENABLED ELECTRIC POWER SYSTEMS

A Dissertation

by

HANGTIAN LEI

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Chanan Singh
Committee Members,	Le Xie
	Alex Sprintson
	Sergiy Butenko
Head of Department,	Miroslav M. Begovic

May 2016

Major Subject: Electrical Engineering

ABSTRACT

Cyber-induced failures affect power system reliability and thus are important to be considered in composite system reliability evaluation. This dissertation extends the scope of bulk power system reliability modeling and analysis with the consideration of cyber elements.

A novel methodology by introducing the concept of Cyber-Physical Interface Matrix (CPIM) is proposed. The failure modes of cyber components and their impact on transmission line tripping behaviors are modeled and numerically analyzed as an example to illustrate the construction and utility of the CPIM. The methodology is then enhanced and implemented on an extended Roy Billinton Test System (RBTS) with its applicability for large systems illustrated. The results clearly show the impact of cyber-induced failures on system-wide reliability indices. The CPIM is the critical idea in the proposed methodology. It decouples the analysis of the cyber part from the physical part and provides the means of performing the overall analysis in a tractable fashion. The overall methodology proposed in this dissertation also provides a scalable option for reliability evaluation of large cyber-physical power systems.

The efficiency of the overall methodology can be further improved with the use of non-sequential Monte Carlo techniques. However, the failure and repair processes in cyber-induced events are inherently sequential involving dependent failures, making it difficult to utilize non-sequential sampling methods as simply as when the components are independent. In this dissertation, the difficulties of using sampling when there are

dependent failures are thoroughly explored. An approach is proposed to overcome the difficulties by generating a representative state space and its probabilities from which states can be sampled. The proposed approach not only preserves the sequential and dependent features of cyber-induced events but also improves the efficiency, which is very beneficial for reliability evaluation of large power systems in the presence of cyber-induced dependent failures.

ACKNOWLEDGEMENTS

I would like to express my special thanks to my advisor, Dr. Chanan Singh, for his guidance and support throughout my research at Texas A&M University.

I gratefully appreciate the time, support, and comments from my committee members, Dr. Le Xie, Dr. Alex Sprintson, and Dr. Sergiy Butenko.

Sincere acknowledgements are extended to the faculty and staff, as well as my friends and colleagues, at Texas A&M University for their assistance and encouragement.

Also, I would like to thank my friends and colleagues at Entergy for their help during my two internships. The industry experience I gained at Entergy is very helpful.

This research was partly supported by the Power Systems Engineering Research Center (PSERC) under the grant "Reliability Assessment and Modeling of Cyber Enabled Power Systems with Renewable Sources and Energy Storage (T-53)" and by NPRP grant # NPRP 7-106-2-053 from the Qatar National Research Fund (a member of Qatar Foundation). I would like to acknowledge the support from all the sponsors.

NOMENCLATURE

CB	Circuit Breaker
CEM	Consequent Event Matrix
CPIM	Cyber-Physical Interface Matrix
CPU	Central Processing Unit
CT	Current Transformer
EENS	Expected Energy Not Supplied
EFLC	Expected Frequency of Load Curtailment
GOOSE	Generic Object Oriented Substation Event
HMI	Human Machine Interface
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
LOLE	Loss of Load Expectation
LOLP	Loss of Load Probability
MRT	Mean Repair Time
MTTF	Mean Time To Failure
MU	Merging Unit
PB	Process Bus
Prot. IED	Protection Intelligent Electronic Device

PT	Potential Transformer
RBTS	Roy Billinton Test System
RTS	Reliability Test System
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
λ_i	Failure rate of individual component *i*
μ_i	Repair rate of individual component *i*

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

1. INTRODUCTION*

1.1 Background and Scope

The quantitative reliability indices of bulk power systems are important to utility companies, vendors, and regulators for planning, operation, maintenance, and regulatory purposes. Studies of bulk power system reliability evaluation have been mostly focusing on the current-carrying part. The pertinent theories and methodologies are well established and documented [1]-[3].

Information and Communication Technologies (ICTs) are widely deployed in electric power systems to improve system control, protection, monitoring, and data processing capabilities. ICT functionalities are generally assumed to be perfectly reliable in the process of composite power system reliability evaluation. This assumption may have significant effect on the reliability indices calculated and result in too optimistic reliability evaluation. For realistic reliability evaluation, it is necessary to consider ICT failures and their impact on composite power systems.

This research aims at extending the scope of bulk power system reliability modeling and analysis with the consideration of cyber elements. In particular, a novel methodology with the use of *Cyber-Physical Interface Matrix* (*CPIM*) is proposed and

*Part of this section is reprinted from *Electric Power Systems Research*, vol. 129, Hangtian Lei and Chanan Singh, "Power system reliability evaluation considering cyber-malfunctions in substations", pp. 160-169, © 2015, with permission from Elsevier.

demonstrated. The CPIM decouples the analysis of cyber system from the evaluation of the physical system and provides the means of performing the overall analysis in a tractable fashion.

In this dissertation, the term “cyber” refers to the devices and activities residing in the secondary side of the power system, associated with the functionalities of measurement, control, monitoring, and protection. The term “physical” refers to the equipment and activities in the primary side of the power system, associated with the generation, transmission, and distribution of electric power and energy. A whole power system is also referred to as a “cyber-physical power system”, in which the communication networks and power components are interdependent [4]-[6]. The cyber-physical interdependencies exist extensively in power systems and associate with various aspects. This dissertation focuses on the aspect of protection as a facet to study such interdependencies since protection system hidden failures are recognized as common causes of multiple or cascading outages [7]-[10].

1.2 Literature Review

A protection system consists of circuit breakers, current and voltage transformers, communication cables, protective relays, and possibly some auxiliary devices [11]-[13]. With the advent of microprocessor-based relays and the rapid progress of communication technologies, modern protection panels are equipped with

multifunctional Intelligent Electronic Devices (IEDs) that are connected to communication networks [14]-[17].

Some studies [8], [10], [18]-[22] have been done to consider protection system failures in composite power system reliability evaluation. However, due to the variety of protection system architectures as well as the diversity of control and communication mechanisms, it is hard to explicitly model protection systems with detailed configurations. As a result, in most of the previous work, protection system failures were either concentrated on circuit breaker trip mechanisms [10], [18] or represented abstractly by multistate models [8], [19]-[22], in which the protection system was treated as a compact object. Some important technical details inside the protection system, such as the placement of cyber elements (e.g., CT/PTs, MUs, and IEDs) and their wire connections, were absent in those publications. Due to the absence of such details, the interdependencies between cyber elements and physical components were not sufficiently covered. In [4] and [5], to study the direct and indirect cyber-physical interdependencies, some mathematical terms and operations were defined and proposed with applications on small test systems including monitoring, control, and protection features. The results in [4] and [5] provide valuable information that indicates the impact of cyber element failures on physical system reliability indices. However, excessive self-defined reliability terms and tedious mathematical operations were introduced in [4] and [5]. These terms are hardly available from engineering practice, making it difficult to implement the overall methodology in practical applications. Therefore, it is necessary to develop a novel reliability evaluation methodology that is scalable for applications in

large cyber-physical power systems. Furthermore, non-sequential Monte Carlo methods are typically easier to implement and require much less CPU time and memory as compared to sequential methods [3], [23], [24]. It would be significantly beneficial for the application of developed methodology in large systems if the efficiency is further improved with the use of non-sequential techniques, although it is difficult to utilize non-sequential sampling methods as simply as when the components are independent due to the inherently chronological, causal and dependent features of the failure and repair processes in the presence of cyber-induced dependent events.

1.3 Research Objectives and Procedures

The major objective of this research is to develop novel methodologies to model and evaluate the reliability of composite cyber-physical power systems, which consist of current-carrying part and cyber components, in an integrative manner. The scope is to focus on substation protection systems as these are very critical to the success of power delivery. To illustrate and implement the methodologies, standard reliability test systems are extended with substation protection systems considering modern features. Furthermore, the possibilities of utilizing non-sequential techniques for efficiency improvement are researched. The following are detailed procedures of this research:

1) Formulate a novel methodology with the use of Cyber-Physical Interface Matrix (CPIM) which decouples the analysis of cyber part from the physical components, design a modern substation protection system with cyber and

physical components, analyze the cyber failure modes and their impact on physical part, obtain the interface matrix, and illustrate the utility of the interface matrix in a composite power system.

2) Include more technical considerations, such as cyber-link failures, in the substation protection system model.
3) Extend a standard reliability test system with modern substation protection configurations, enhance and implement the proposed reliability evaluation methodology with the use of CPIM to obtain numerical reliability indices.
4) Improve the efficiency of the proposed methodology with the use of non-sequential techniques.

1.4 Organization of the Dissertation

The remainder of this dissertation is organized as follows. Section 2 proposes a novel methodology with the use of Cyber-Physical Interface Matrix (CPIM) and performs reliability modeling and analysis at the substation level. Section 3 enhances the substation model with consideration of cyber-link failures. Section 4 enhances and implements the proposed methodology on an extended standard reliability test system to obtain system-wide reliability indices. Section 5 researches the major difficulties of applying conventional non-sequential sampling methods to generating appropriate state space in the presence of dependent failures and proposes a method to overcome these

difficulties. The conclusions and outlook are given in Section 6. References are attached at the end.

2. SUBSTATION LEVEL RELIABILITY MODELING AND ANALYSIS*

2.1 Introduction

The electric power substations are vital nodes among electric power generation, transmission, and distribution systems. In recent years, utilities, vendors, and research institutions have paid close attention to the reliability of substation automation systems (SASs) since the failure or malfunctioning of a SAS may have a huge impact on a power system.

The electric power SAS was designed in the past using control and protection schemes with electromechanical and hard-wired relay logic [15]. This architecture has undergone significant changes with the advent of multi-functional microprocessor-based Intelligent Electronic Devices (IEDs). Traditional panels with dedicated stand-alone relays, control switches, meters, and status indicators have been replaced by multi-functional, smart, and communicative IEDs [16].

IEC 61850, the international standard for substation automation, provides interoperability between IEDs from different vendors by standardizing the aspects of the information exchange between them [25]. The vision of IEC 61850 series is to define an

* Part of this section is reprinted from copyrighted material with permission from IEEE. © 2014 IEEE. Reprinted, with permission, from Hangtian Lei, Chanan Singh, and Alex Sprintson, "Reliability modeling and analysis of IEC 61850 based substation protection systems," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2194-2202, Sep. 2014.

interoperable communication system, which facilitates the implementation of functions that are distributed among various IEDs from different vendors [15].

Some progress has been made recently in the reliability evaluation of substation automation systems. In [26], reliability indices have been investigated and selected to identify the critical components in an all-digital protection system. The challenges for implementing IEC 61850 based new communication architecture were discussed and some possible solutions to several major implementation issues were suggested in [27]. In [28], the reliability block diagram approach was used to evaluate the reliability and availability of practical Ethernet switch architectures for the SASs.

However, most of the previous publications focused on either the physical components (e.g., transformers, circuit breakers, and transmission lines) or the cyber part separately. In [29], the cyber and physical parts of a SAS were integratively analyzed, but different bays were analyzed separately at a conceptual level, which may not be always true in practice. To overcome this shortcoming, a specific cyber-physical system of a typical substation is designed and analyzed using the methodology proposed in this section. Furthermore, the concept of Cyber-Physical Interface Matrix (CPIM) is introduced and its utility is illustrated. The CPIM depicts the inter-dependencies among the failures of different physical components due to various cyber failure modes. It decouples the analysis of the cyber part from the physical part and provides the means of performing the overall analysis in a computationally tractable way.

The remainder of this section is organized as follows. In Section 2.2, the overall architecture and main components of the IEC 61850 based SAS are described, a typical

IEC 61850 based substation layout, including both physical and cyber parts, is presented. In Section 2.3, a general technique for cyber-physical system reliability analysis is presented, the detailed analysis for a substation is performed, and the CPIM is obtained. The utilization of the interface matrix is then illustrated by incorporating this substation into a composite power system. Section 2.4 is the summary of Section 2.

2.2 Protection Systems Using IEC 61850

2.2.1 IEC 61850 Hierarchy and Architecture

A typical architecture of the IEC 61850 based SAS, which consists of three levels, is shown in Figure 1.

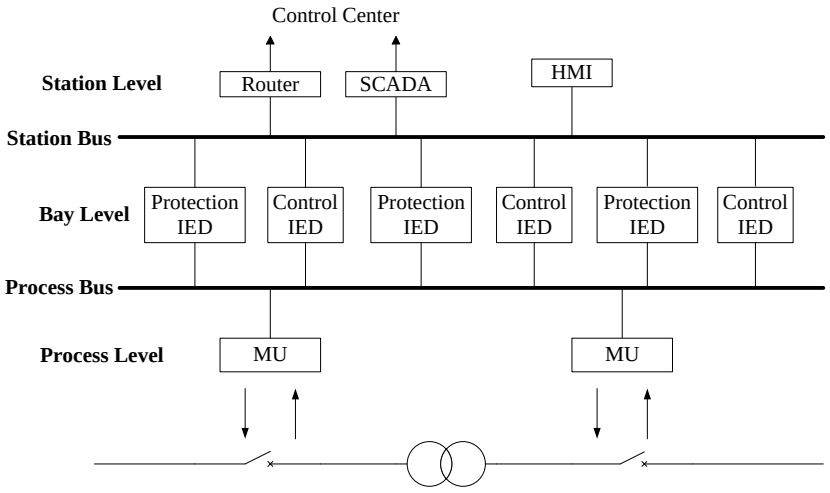

Figure 1. Typical architecture of an IEC 61850 based substation automation system.

Process level: This level includes Current Transformers (CTs) / Potential Transformers (PTs), Merging Units (MUs), actuators, etc. The voltage and currents signals acquired by CTs / PTs are digitized by MUs and sent over the Ethernet network to the bay level.

Bay level: This level includes microprocessor based relays (also known as protection IEDs) and bay controllers (control IEDs). Protection IEDs receive information coming from the process level, conduct elaborate calculations and send decision signals over the Ethernet network.

Station level: Station level includes the Human Machine Interface (HMI) and SCADA system. At this level, the status data of various components in the substation are available to operators for monitoring and operation purposes. Operators can also issue signals at this level to perform certain kinds of manual control.

Process bus: The process bus enables the time critical communication between the process level and the bay level, which builds a bridge for voltage and currents information going from MUs to protection IEDs, and for trip signals going the opposite direction.

Station bus: The station bus enables information exchange between the bay level and station level, which makes the status data of the entire substation available to the control center for monitoring and operation purposes.

2.2.2 IEC 61850 Based Protection System Layout and Configuration

An IEC 61850 based protection system for a typical 230-69 kV substation is designed for the reliability analysis. The integrated system, including physical components (e.g., transformers, transmission lines, and circuit breakers) and cyber components (e.g., merging units, Ethernet switches, and Prot. IEDs), is shown in Figure 2. The physical part has been used in [30] to illustrate the protection zones and schemes. The cyber part is designed according to IEC 61850 standards [31].

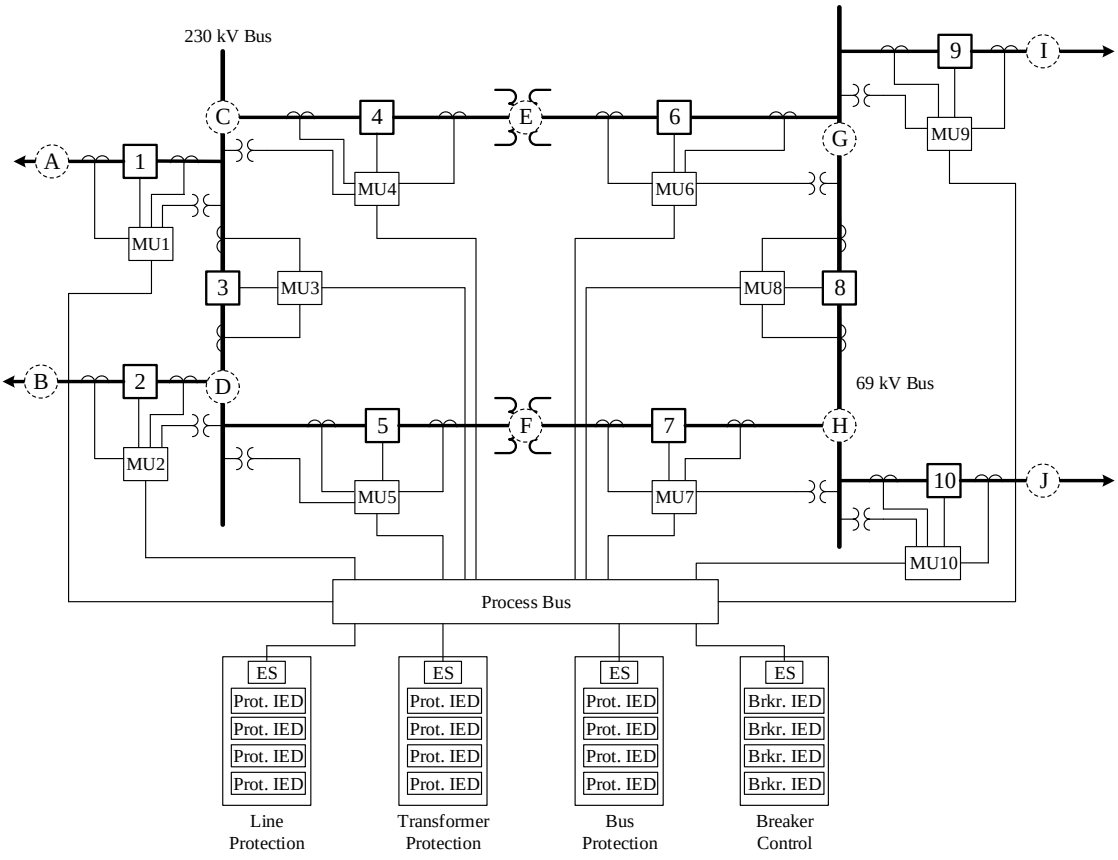

Figure 2. An IEC 61850 based protection system for a 230-69 kV substation.

The primary protection zones associated with various fault locations and the corresponding circuit breakers needed to trip for fault clearances are listed in Table 1.

The MTTF [32] values of individual components for reliability calculations are obtained from [15], [28], [33]-[35] and tabulated in Table 2.

Table 1 Substation protection zone division

Type	Fault Location	Associated Circuit Breakers
Line	A	Breaker 1
	B	Breaker 2
	I	Breaker 9
	J	Breaker 10
Transformer	E	Breakers 4, 6
	F	Breakers 5, 7
Bus	C	Breakers 1, 3, 4
	D	Breakers 2, 3, 5
	G	Breakers 6, 8, 9
	H	Breakers 7, 8, 10

The MTTF varies for CBs at different voltage levels, or serving different functions in the system [35], for the study in this section, a typical value of 100 years is chosen. Using MRT of 8 hours from [15] and [28], the failure and repair rates of individual components are tabulated in Table 2.

Table 2 Reliability data for individual components

	MTTF (year)	Failure Rate λ (/year)	MRT (h)	Repair Rate μ (/year)
CB	100	0.01	8	1095
MU	150	0.00667	8	1095
PB	100	0.01	8	1095
ES	50	0.02	8	1095
Prot. IED	150	0.00667	8	1095

For convenience of analysis, the ES and protection IEDs located at the same protection panel are combined into one line protection unit. Normally, for each protection unit, redundant protection IEDs are equipped, hence, in the reliability block diagram shown in Figure 3, both the protection IEDs are shown in parallel and then in series with the ES. The reliability data after combination is shown in Table 3.

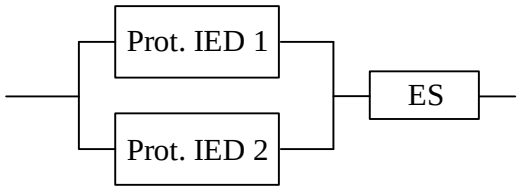

Figure 3. The reliability block diagram of the line protection unit.

Table 3 Reliability data for protection units

	Failure Rate λ (/year)	Mean Repair Time (h)	Repair Rate μ (/year)
Line Protection Unit	0.02000008	7.99998	1095.002
Transformer Protection Unit	0.02000008	7.99998	1095.002
Bus Protection Unit	0.02000008	7.99998	1095.002

2.3 Reliability Analysis of the Integrated System

2.3.1 A General Technique for Reliability Analysis of Cyber-Physical Systems

The complexity and dimensionality of substation automation systems make it difficult, if not impossible to conduct the reliability analysis of the whole system, physical and cyber, in a single step. Even for the current carrying part alone, it is not computationally efficient to model all the components distinctly and simultaneously. Therefore, it is necessary to perform the analysis sequentially.

Our proposed approach is formulated with the following steps:

1) Develop an interface matrix between the cyber and physical subsystems. This matrix is called *Cyber-Physical Interface Matrix* (*CPIM*). It defines the relationship between the cyber subsystems and physical subsystems in terms of failure modes and effects. In developing this matrix, the major interaction points between the cyber and physical part need to be identified.
2) Analyze the cyber part to determine parameters of the interface matrix.

3) Determine probabilities of interface events.

4) Analyze the physical system using the interface matrix.

An example of the Cyber-Physical Interface Matrix *M* is shown in (2.1). The elements of this matrix are the probabilities of interface events. In the following sections, the reliability analysis for the system shown in Figure 2 will be presented to illustrate the procedures of obtaining these probabilities.

$$M = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & & p_{2,n} \\ \vdots & & \ddots & \vdots \\ p_{m,1} & p_{m,2} & \cdots & p_{m,n} \end{bmatrix} \tag{2.1}$$

2.3.2 Individual Component Analysis

For each component (except the process bus) listed in Table 2, only two states, Up and Down, are considered in our study as shown in Figure 4.

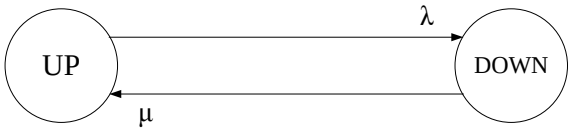

Figure 4. The states diagram for an individual component.

The probabilities of being in the UP and DOWN states can be calculated using equations (2.2) and (2.3), respectively.

$$p_{up} = \frac{\mu}{\lambda + \mu} \tag{2.2}$$

$$p_{down} = \frac{\lambda}{\lambda + \mu} \tag{2.3}$$

The calculated probabilities for Circuit Breaker (CB), Merging Unit (MU), Line Protection Unit, Transformer Protection Unit, and Bus Protection Unit are tabulated in Table 4.

In an ideal environment that utilizes non-blocking switches and has prioritization mechanisms, the time of delay is negligibly small. However, in practice, delays might occur due to the use of legacy technology, such as bus Ethernet, which is still used in some substations, or due to the use of wireless technology.

Table 4 Probability data for individual components

Component	p_{up}	p_{down}
Circuit Breaker (CB)	0.999990867	0.000009132
Merging Unit (MU)	0.999993912	0.000006088
Line Protection Unit	0.999981735	0.000018265
Transformer Protection Unit	0.999981735	0.000018265
Bus Protection Unit	0.999981735	0.000018265

Compared with fiber-optic communication, wireless communication technologies are more economically feasible for small-scale automation systems in rural areas. In wireless environments, the delays can be quite large due to the electromagnetic interference in high voltage environments. Meanwhile, the radio frequency interference from wireless equipment can also affect the functioning of equipment [36], and GOOSE packets might be occasionally dropped by the network due to errors. Therefore, there is some finite probability that delay may happen in the network. Taking into account this probability, delay is modeled as a state of the process bus. Of course, the delay probability can be set to zero if needed.

The state DELAY means that due to the temporarily heavy traffic, the process bus does not physically fail but the message transfer is delayed and the delay time is over the threshold value that causes the breakers associated with the primary protection zone fail to trip in time. The probability of delay given that the PB is not in the DOWN state is denoted by p_d (=0.003). The state transition diagram of the PB is shown in Figure 5.

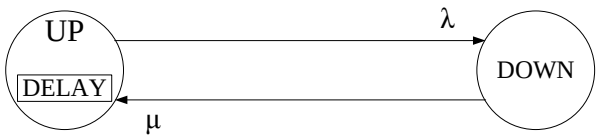

Figure 5. The states diagram of the process bus.

Thus, for the Process Bus (PB), the probabilities of being in the UP, DELAY, and DOWN states can be calculated using equations (2.4)-(2.6).

$$p_{up} = \frac{\mu}{\lambda + \mu}(1 - p_d) \tag{2.4}$$

$$p_{delay} = \frac{\mu}{\lambda + \mu} p_d \tag{2.5}$$

$$p_{down} = \frac{\lambda}{\lambda + \mu} \tag{2.6}$$

The reliability analysis of line, transformer, and bus fault clearances for the substation shown in Figure 2 are discussed in sections 2.3.3, 2.3.4, and 2.3.5, respectively.

Several assumptions are made:

1) The cable links between various devices and all the CT/PTs are assumed not to fail.
2) If the breaker(s) for the primary protection fail to trip correctly due to the message delay or due to the failure of the components other than the process bus, the trip signal can be transferred to an adjacent protection zone. However, if the process bus fails, the entire system is assumed to fail.
3) If the primary protection fails to trip correctly and the trip signal is transferred to an adjacent protection zone, the subsequent failure of the trip is not considered.
4) The fault events happening in different areas (e.g., areas A, E, and C) are analyzed independently. The possibility that faults occur simultaneously at different locations is not considered.

5) If the message delay at the process bus is beyond a threshold value, the breaker(s) for the primary protection will fail to trip and the trip signal will be transferred to an adjacent protection zone.

2.3.3 Reliability Analysis of Line Fault Clearance

As shown in Figure 2, line faults can happen in areas A, B, I, or J. Here, the line fault at area A is taken as an example for illustration. The same techniques can be applied to faults at B, I, or J.

When a line fault happens at A, the voltage/current information will be sensed by PT/CTs and will be sent to MU1. The information will be digitized at MU1 and then be sent to Line Protection Unit via the PB. Based on the information received, relay algorithms will be performed at the Line Protection Unit and a trip signal will be sent to Circuit Breaker 1 via the PB. There are 4 components associated with this procedure, namely, MU1, PB, Line Protection Unit, and CB1. One or more components' failure will result in malfunction. The detailed descriptions of different scenarios are listed as below.

1) All components operate as intended

If all aforementioned components operate as intended, CB1 will trip in time, and only the faulted line will be isolated. The rest of the substation will stay in service.

2) PB fails to work

Since PB is the hub of all the cyber links inside the substation, the failure of PB will cause all the relays to be unable to receive or send information. All breakers will fail to trip and the entire system will be affected by the fault.

3) One or more components of MU1, Line Protection Unit, CB1 fail to operate

CB1 will not trip at first. When the fault comes to affect area C, bus protection will be triggered and CB1, CB3, CB4 will trip. Areas A and C will be out of service.

4) PB is in UP state, but message delay happens due to temporarily heavy information traffic

In this case, the tripping signal will not arrive at CB1 in time and thus CB1 will not trip before the breaker failure timer expires, bus protection for area C will then be triggered and CB1, CB3, CB4 will trip.

The probabilities and effects corresponding to each case are shown in Table 5. These probabilities are conditional and are calculated given that a fault has already happened at location A. To obtain the actual probabilities, they need to be multiplied by the probability of this fault occurrence.

Table 5 Summary of scenarios of the line fault clearance at A

Scenario No.	Probability	Areas Affected
1	0.996957511	A
2	0.000009132	Entire Substation
3	0.000033384	A, C
4	0.002999973	A, C

Table 6 Summary of scenarios of the line fault clearance at B

Areas Affected	Probability
B	0.996957511
Entire Substation	0.000009132
B, D	0.003033357

Table 7 Summary of scenarios of the line fault clearance at I

Areas Affected	Probability
I	0.996957511
Entire Substation	0.000009132
G, I	0.003033357

Table 8 Summary of scenarios of the line fault clearance at J

Areas Affected	Probability
J	0.996957511
Entire Substation	0.000009132
H, J	0.003033357

Similarly, the probabilities and effects of line fault clearances at locations B, I, and J are shown in Tables 6-8, respectively.

2.3.4 Reliability Analysis of Transformer Fault Clearance

As shown in Figure 2, a transformer winding/ground fault can happen at areas E or F. Here, the transformer fault at E is taken as an example for illustration. The same techniques can be applied to faults at F.

When a transformer fault happens at E, the voltage/current information will be sensed by corresponding PT/CTs and will be sent to MU4 and MU6. The information will be digitized at these merging units and then will be sent to Transformer Protection Unit via the PB. Based on the information received, relay algorithms will be performed at Transformer Protection Unit and trip signals will be sent to CB4 and CB6 via the PB. There are 6 components associated with this procedure, namely, MU4, MU6, PB,

Transformer Protection Unit, CB4 and CB6. One or more components' failure will result in malfunction. The detailed descriptions of different scenarios are listed as below.

1) All components operate as intended

If all aforementioned components operate as intended, CB4 and CB6 will trip as intended, only the faulted part E will be isolated and the rest of this substation will stay in service.

2) PB fails to work

Since PB is the hub of all the cyber links inside the substation, the failure of PB will cause all the relays to be unable to receive or send information, all breakers will fail to trip and the entire system will be affected by this fault.

3) One or more components of MU4, CB4 fail, while all other components work as intended

CB6 will trip as intended, but CB4 will not. When the fault affects area C, the bus protection will be triggered and CB1 and CB3 will trip. Areas C and E will be out of service.

4) One or more components of MU6, CB6 fail, while all other components work as intended

CB4 will trip as intended, but CB6 will not. When the fault affects area G, the bus protection will be triggered and CB8 and CB9 will trip. Areas E, G and I will be out of service.

5) Both CB4 and CB6 fail to trip due to breakers failure or PB delay, or failure of Transformer Protection Unit, but PB is not down

When the fault comes to affect areas C and G, protection devices of these zones will be triggered. Areas C, E, G, and I will be isolated from the system.

The probabilities and effects corresponding to each scenario are shown in Table 9. These probabilities are calculated given that a fault has already happened at location E. The actual probabilities need to be multiplied by the probability of this fault occurrence.

Table 9 Summary of scenarios of the transformer fault clearance at E

Scenario No.	Probability	Areas Affected
1	0.996942336	E
2	0.000009132	Entire Substation
3	0.000015174	C, E
4	0.000015174	E, G, I
5	0.003018182	C, E, G, I

Similarly, the probabilities and effects of a transformer fault clearance at location F are shown in Table 10.

Table 10 Summary of scenarios of the transformer fault clearance at F

Areas Affected	Probability
F	0.996942336
Entire Substation	0.000009132
D, F	0.000015174
F, H, J	0.000015174
D, F, H, J	0.003018182

2.3.5 Reliability Analysis of Bus Fault Clearance

A bus fault can happen at locations C, D, G, or H. Here, the bus fault at C is taken as an example for illustration. The same techniques can be applied to faults at D, G, and H.

When a bus fault happens at C, the voltage/current information will be sensed by the corresponding PT/CTs and will be sent to MU1, MU3, and MU4. The information will be digitized at these merging units and then will be sent to Bus Protection Unit via the Process Bus. Based on the information received, relay algorithms will be performed at the Bus Protection Unit and trip signals will be sent to CB1, CB3, and CB4 via the PB. There are 8 components associated with this procedure, namely, MU1, MU3, MU4, PB, Bus Protection Unit, CB1, CB3, and CB4. One or more components' failure will result in malfunction. The detailed descriptions of different scenarios are listed as below.

1) All components operate as intended

If all components operate as intended, CB1, CB3, and CB4 will trip as intended, only the faulted bus will be cut off, and the rest of this substation will stay in service.

2) PB fails to work

Since PB is the hub of all the cyber links inside the substation, the failure of PB will cause all the relays to be unable to receive or send information, all breakers will fail to trip and the entire system will be affected by this fault.

3) One or more components of MU1, CB1 fail, while all other components work as intended

CB3 and CB4 will trip as intended, but CB1 will not. When the fault comes to affect area A, the breaker located at the substation on the other side of this line will trip. Areas A and C will go out of service.

4) One or more components of MU3, CB3 fail, while all other components work as intended

CB1, CB4 will trip as intended, but CB3 will not. When the fault comes to affect area D, the bus protection for D will be triggered and CB2 and CB5 will trip. Buses C and D will be out of service.

5) One or more components of MU4, CB4 fail, while all other components work as intended

CB1 and CB3 will trip as intended, but CB4 will not. When the fault affects area E, the transformer protection will be triggered and CB6 will trip. Bus C and transformer E will be out of service.

6) *One or more components of MU1, CB1 fail and one or more components of MU3, CB3 fail, while all other components work as intended*

Both CB1 and CB3 will not trip. When the fault comes to affect areas A and D, the protection IEDs for these zones will be triggered, CB2, CB5 as well as the breaker on the other side of line A will trip. Areas A, C, and D will go out of service.

7) *One or more components of MU1, CB1 fail and one or more components of MU4, CB4 fail, while all other components work as intended*

Both CB1 and CB4 will not trip. When the fault comes to affect areas A and E, the protection IEDs for these zones will be triggered, CB6 and the breaker on the other side of line A will trip. Areas A, C, and E will be cut off from the system.

8) *One or more components of MU3, CB3 fail and one or more components of MU4, CB4 fail, while all other components work as intended*

Both CB3 and CB4 will not trip as intended. When the fault comes to affect areas D and E, the protection IEDs for these zones will be triggered, CB2, CB5, and CB6 will trip. Areas C, D, and E will be cut off from the system.

9) *All of the CB1, CB3, and CB4 fail to trip due to breakers failure or PB delay or failure of Bus Protection Unit, but PB is not down*

When the fault comes to affect areas A, D and E, the protection IEDs for these zones will be triggered. Areas A, C, D, and E will be isolated from the system.

Table 11 Summary of scenarios of the bus fault clearance at C

Scenario No.	Probability	Affected Areas
1	0.996927163	C
2	0.000009132	Entire Substation
3	0.000015174	A, C
4	0.000015174	C, D
5	0.000015174	C, E
6	$2.31*10^{-10}$	A, C, D
7	$2.31*10^{-10}$	A, C, E
8	$2.31*10^{-10}$	C, D, E
9	0.003018182	A, C, D, E

The probabilities and effects corresponding to all the scenarios are shown in Table 11. These probabilities are calculated given that a fault has already happened at location C. The actual probabilities need to be multiplied by the probability of this fault occurrence.

Similarly, the probabilities and effects of bus fault clearances at locations D, G, and H are shown in Tables 12-14, respectively.

Table 12 Summary of scenarios of the bus fault clearance at D

Affected Areas	Probability
D	0.996927163
Entire Substation	0.000009132
B, D	0.000015174
C, D	0.000015174
D, F	0.000015174
B, C, D	$2.31*10^{-10}$
B, D, F	$2.31*10^{-10}$
C, D, F	$2.31*10^{-10}$
B, C, D, F	0.003018182

Table 13 Summary of scenarios of the bus fault clearance at G

Affected Areas	Probability
G	0.996927163
Entire Substation	0.000009132
G, I	0.000015174
G, H	0.000015174
E, G	0.000015174
G, H, I	$2.31*10^{-10}$
E, G, I	$2.31*10^{-10}$
E, G, H	$2.31*10^{-10}$
E, G, H, I	0.003018182

Table 14 Summary of scenarios of the bus fault clearance at H

Affected Areas	Probability
H	0.996927163
Entire Substation	0.000009132
H, J	0.000015174
G, H	0.000015174
F, H	0.000015174
G, H, J	$2.31*10^{-10}$
F, H, J	$2.31*10^{-10}$
F, G, H	$2.31*10^{-10}$
F, G, H, J	0.003018182

2.3.6 Construction and Utilization of Cyber-Physical Interface Matrix

The Cyber-Physical Interface Matrix (CPIM) *M* can be obtained by synthesizing the data from Table 5 to Table 14. The elements of this matrix are the probabilities of interface events. For the Cyber-Physical Interface Matrix (CPIM) *M* corresponding to the substation illustrated in previous sections, some elements are tabulated in Table 15. The CPIM shown in Table 15 can be improved by eliminating the off-diagonal zeros to make it more compact. Some examples of better developed CPIMs are presented in Section 4.4.1 of this dissertation.

Table 15 Elements of matrix M

	Column 1	Column 2	Column 3	…	Column 58
Row 1	0.996958	0	0	…	0
Row 2	0	$9.1*10^{-6}$	0	…	0
Row 3	0	0	0.003033357	…	0
…	…	…	…	…	…
Row 58	0	0	0	…	0.00301818

Once the CPIM is obtained, its results can be utilized for the reliability analysis of a wider area by incorporating this substation into a larger system without considering the details of the cyber part.

To illustrate the utility of the interface matrix, the Monte Carlo simulation process for a composite system shown in Figure 6 is explained in the following example. The simulation process is for illustration only. Its specific implementation will be presented in section 4 of this dissertation.

Since the CPIM, which depicts the inter-dependencies among the failures of different physical components due to various cyber failure modes, is already obtained, the simulation process can be performed without considering the details of the cyber part. Therefore, only the physical components are shown in Figure 6. All these components are numbered in Table 16.

The next event sequential simulation [37], in which the time is advanced to the occurrence of the next event, is used. For each individual component in this composite system, two states, UP and DOWN, are considered.

The simulation process for the composite system can be formulated in the following steps:

1) Step 1

Set the initial state of all components as UP and set the simulation time *t* to 0.

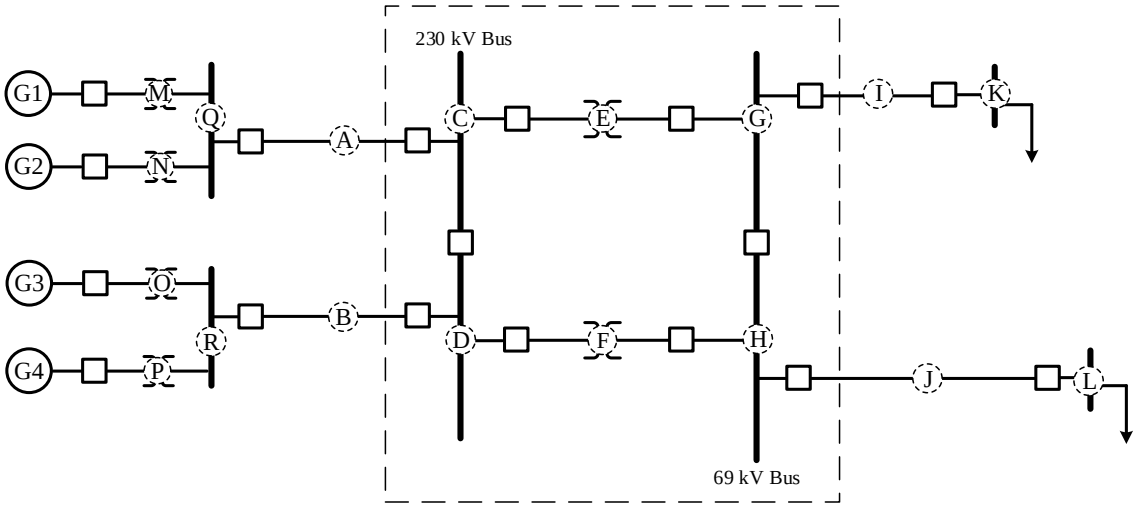

Figure 6. A composite system consisting of a substation and other components.

Table 16 Components in the composite system

Number	Component Name
1	Generator G1
2	Generator G2
3	Generator G3
4	Generator G4
5	Transformer M
6	Transformer N
7	Transformer O
8	Transformer P
9	Bus Q
10	Bus R
11	Line A
12	Line B
13	Bus C
14	Bus D
15	Transformer E
16	Transformer F
17	Bus G
18	Bus H
19	Line I
20	Line J
21	Bus K
22	Bus L

2) Step 2

For each individual component, draw a random decimal number between 0 and 1 to compute the time to the next event.

In this section, the distributions of UP and DOWN times for all components are assumed to be exponential. Let N_c be the total number of components, z_i ($0 < z_i < 1$, $1 \leq i \leq N_c$) be the random number drawn for the i^{th} component. The time to the next transition of this component is given by:

$$T_i = -\frac{ln(z_i)}{\rho_i} \tag{2.7}$$

In (2.7), depending on whether the i^{th} component is UP or DOWN, λ_i or μ_i is used in place of ρ_i.

3) Step 3

Find the minimum time, change the state of the corresponding component, and update the total time.

The time to the next system transition is given by:

$$T = \min\{T_i\}, 1 \leq i \leq N_c \tag{2.8}$$

If this T corresponds to T_q, that is, the q^{th} component, then the next transition takes place by the change of state of this component. The total simulation time t is increased by T.

4) Step 4

Change the q^{th} component's state accordingly. For each component i, $1 \leq i \leq N_c$, subtract T from T_i

$$T_{i,res} = T_i - T \tag{2.9}$$

where $T_{i,\,res}$ is the residual time to transition of component i. The time T_i is updated to:

$$T_i = T_{i,res} \tag{2.10}$$

Since the residual time for component q causing transition becomes 0, therefore, the time to its next transition T_q is determined by drawing a new random number and using (2.7).

5) Step 5

If the state of the q^{th} component transits from UP to DOWN, which means a primary fault happens to this component, then the CPIM is used to determine if there are some subsequent failures causing more components out of service due to the cyber part's malfunction.

Let n_q be the number of possible scenarios if a primary fault happens to the q^{th} component, and $p_{q,\,j}$ $(1 \le j \le n_q)$ be the probability of the j^{th} scenario given that a primary fault already happened at the q^{th} component. These probabilities are directly available from the CPIM. According to the analysis in sections 2.3.3-2.3.5, the following relationship exists:

$$\sum_{j=1}^{n_q} p_{q,j} = 1 \tag{2.11}$$

For the convenience of further illustration, a zero probability $p_{q,0}$ is added to the left side of (2.11), which yields:

$$\sum_{j=0}^{n_q} p_{q,j} = 1 \tag{2.12}$$

Draw a random decimal number y $(0 < y \le 1)$. Let s $(1 \le s \le n_q)$ be an integer which satisfies (2.13).

$$\sum_{j=0}^{s-1} p_{q,j} < y \leq \sum_{j=0}^{s} p_{q,j} \quad (2.13)$$

Then the s^{th} scenario is determined to happen. Let S be the set of components that would go out of service if the s^{th} scenario happens, and S_2 be the set such that:

$$S_2 = \{k | k \in S, k \neq q\} \quad (2.14)$$

For every component k whose state is currently UP and in S_2, change its state to DOWN, draw a new random number, and calculate the time to its next transition T_k using (2.7). Since the failure of component k is caused by the cyber failure rather than a primary fault, therefore, an expedited repair rate $\mu_{k,\,exp}$ instead of μ_k is used in (2.7). The value of $\mu_{k,\,exp}$ is normally available from engineering practice and is called a switching rate.

The following specific case is shown as an example to illustrate the details from step 3 to step 5. For the system shown in Figure 6, in the first iteration of Monte Carlo simulation, if q = 11 is obtained in step 3, which means a primary fault happens at Line A, then T_{11} is updated in step 4. In step 5, from the CPIM shown in Table 15, n_{11} = 3, $p_{11,1}$ = 0.996958, $p_{11,2}$ = 9.1*10^{-6}, and $p_{11,3}$ = 0.003033357 can be obtained.

If the random number y is generated to be 0.9177, as shown in Figure 7, then the 1st scenario is determined to happen, which means only Line A is going out of service. Thereby, S = {11} and S_2 = {} can be obtained.

If the random number y is generated to be 0.9987, also as shown in Figure 7, then the 3rd scenario is determined to happen, which means both Line A and Bus C would go out of service. S = {11, 13} and S_2 = {13} can be obtained, a new random number z_{13} is generated and $\mu_{13,\,exp}$ is used in (2.7) to calculate the time to its next transition T_{13}.

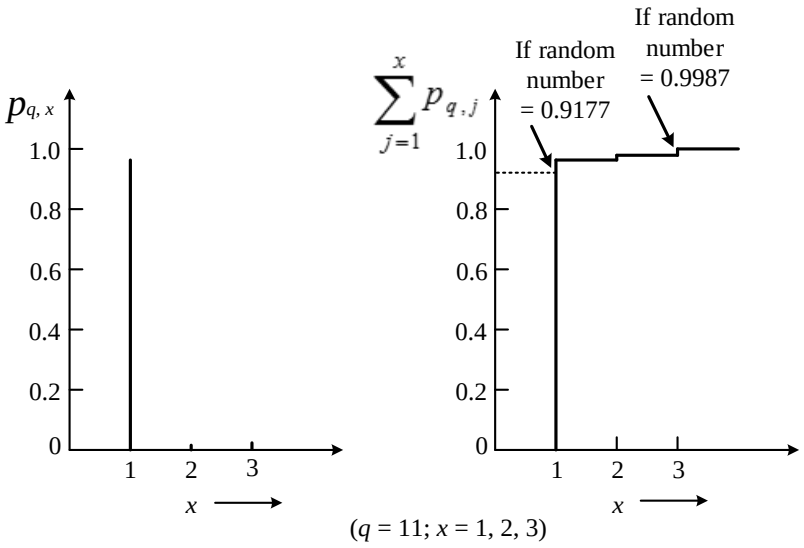

Figure 7. An example of random number mapping.

6) Step 6

Perform the network power flow analysis to assess system operation states. Update reliability indices.

7) Convergence

Steps 3–6 are iteratively continued until a convergence criterion is satisfied. The simulation is said to have converged when the reliability indices attain stable values. For any index *i*, the convergence is measured by its standard error, defined as:

$$\eta = \frac{\sigma_i}{\sqrt{N_y}} \tag{2.15}$$

where σ_i is the standard deviation of the index *i* and N_y is the number of years simulated.

Convergence is said to occur when the standard error in (2.15) drops below a preselected value, ε_i, as shown in (2.16).

$$\eta < \varepsilon_i \tag{2.16}$$

When the simulation finishes, reliability indices, such as the Loss of Load Expectation, can be finally obtained.

2.4 Summary

A novel methodology for modeling and analysis of cyber enabled substation protection systems is presented. A typical protection system based on the IEC 61850 concepts, incorporating both physical and cyber components, is designed. The probabilities of various faults and tripping scenarios are calculated. General techniques for reliability analysis of cyber-physical systems are presented. The concept of Cyber-Physical Interface Matrix (CPIM) is introduced and its utility is illustrated. The CPIM decouples the analysis of the cyber part from the physical part and provides the means of performing the overall analysis of a composite system in a more tractable fashion.

This methodology of finding the CPIM also applies to the reliability analysis of substation automation systems with more complex configuration and larger scale. In such systems, more effort is needed in detailed analysis of various cyber failure modes as well as effects on the physical side.

3. RELIABILITY ANALYSIS OF MODERN SUBSTATIONS CONSIDERING CYBER-LINK FAILURES[*]

3.1 Introduction

This section enhances the substation protection system reliability model with the consideration of cyber-link failures.

A substation protection system is a typical cyber-physical system. It consists of circuit breakers, current/potential transformers, merging units, and protection panels with intelligent electronic devices. These components are connected in an Ethernet-based environment [38]-[41]. In recent years, numerous research efforts have been devoted to study the reliability considerations and implementation issues of modern substation automation systems [28], [38]-[44].

Due to the complexity of monitoring, control, and communication functions as well as the variety of cyber-physical interdependencies, it is challenging to model and analyze the complete cyber-physical system with explicit technical details. Therefore, most research work focuses either on the cyber part or on the physical part. To cover the whole cyber-physical system, it is necessary to divide the overall analysis into subsections and proceed sequentially. A tractable methodology of performing the overall

[*] Part of this section is reprinted from copyrighted material with permission from IEEE. © 2015 IEEE. Reprinted, with permission, from Hangtian Lei, Chanan Singh, and Alex Sprintson, "Reliability analysis of modern substations considering cyber link failures," in *Proc. IEEE Power and Energy Society Innovative Smart Grid Technologies 2015 Asian Conference*, Bangkok, Thailand, Nov. 2015.

analysis by decoupling the cyber part from the physical part has been proposed in Section 2 [42] of this dissertation by introducing the concept, *Cyber-Physical Interface Matrix* (*CPIM*).

The example provided in Section 2 is for the purpose of illustration and some technical details have been simplified in modeling the cyber network. For example, the traffic delay is modeled as a state with a predefined probability value and the links in the communication network are assumed to never fail.

This section applies the methodology proposed in Section 2 to a 4-bus power system with the consideration of more technical details in the cyber part. Unlike some previous publications [38], [39] performing simulations to study the issue of packet delay, this section mathematically models delay as the unavailability of communication links. The remainder of this section is organized as follows. Section 3.2 presents the test system configuration and parameters. The issue of link unavailability due to packet delay is also discussed and modeled in Section 3.2. Section 3.3 outlines the overall procedures. In Section 3.4, the results and discussions are provided. Section 3.5 is the summary of this section.

3.2 System Configuration and Parameters

To illustrate the interactions between cyber and physical components, the reliability of a 4-bus power system with Ethernet-based protection configurations is analyzed in this section as an example. The physical part of the system is taken from

[45]. The cyber part is designed according to the typical configurations of modern substation protection systems.

3.2.1 Configuration and Parameters of the Physical Part

The physical part of the system shown in Figure 8 is as described in [45]. The load and generation capacities are tabulated in Table 17, of which the loads are directly obtained from [45]. The generation capacities at substations (buses) 1 and 4 are assumed to be 250 MW and 300 MW, respectively. This assumption is based on the consideration of a 10% capacity reserve for the whole system. Compared to line faults, bus faults are relatively rare and thus are not considered in the reliability analysis of this section.

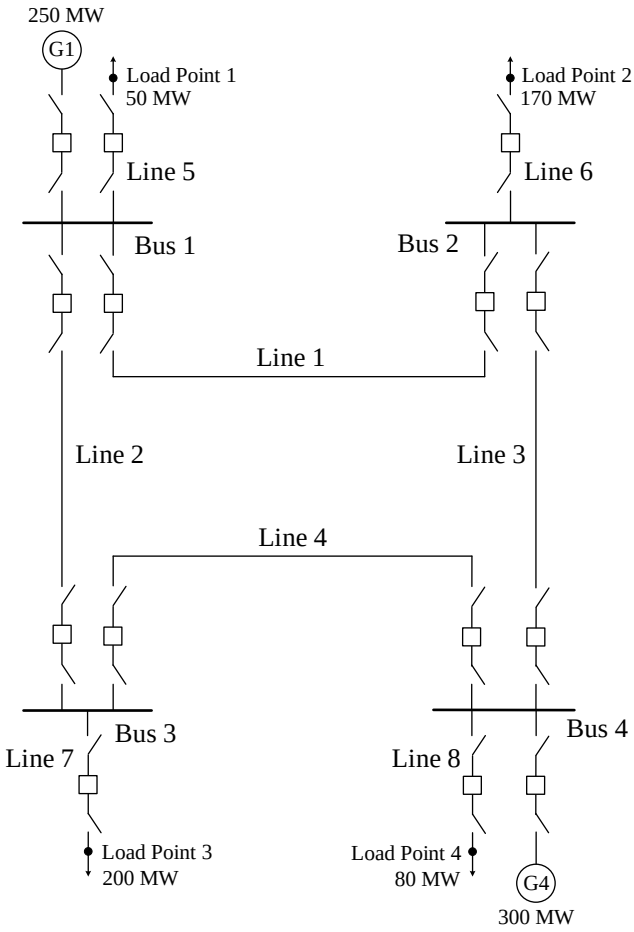

Figure 8. The physical part of the test system.

Table 17 Generation and load capacities

Bus No.	Generation Capacity (MW)	Load Capacity (MW)
1	250	50
2	0	170
3	0	200
4	300	80
Total	550	500

3.2.2 Configuration and Parameters of the Cyber Part

The Ethernet-based protection system is designed for each substation (bus), as shown in Figure 9. For the protection system at each substation, three Ethernet switches are used and they are connected in a ring topology. Take substation 1 as an example, the cyber component names and their meanings are tabulated in Table 18.

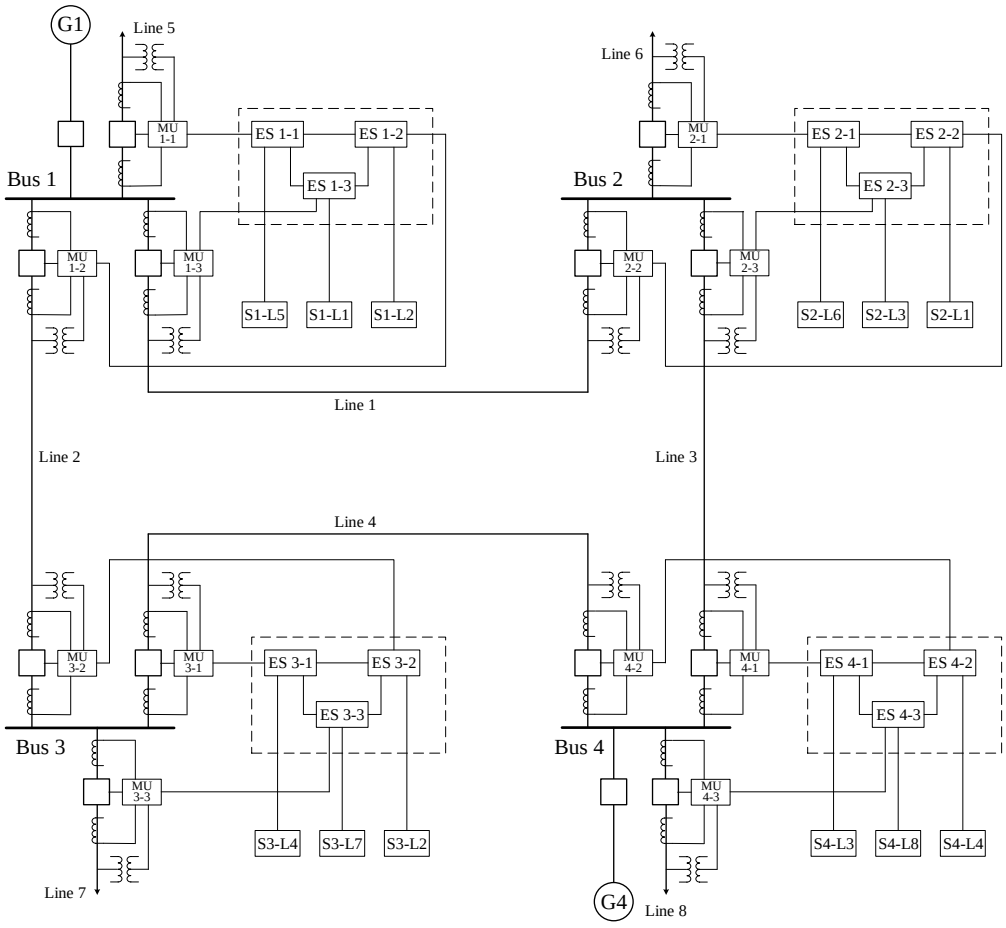

Figure 9. The integrated test system.

Table 18 Cyber component names and meanings

Component Name	Meaning
MU 1-1	Merging Unit 1 at Substation 1
MU 1-2	Merging Unit 2 at Substation 1
MU 1-3	Merging Unit 3 at Substation 1
ES 1-1	Ethernet Switch 1 at Substation 1
ES 1-2	Ethernet Switch 2 at Substation 1
ES 1-3	Ethernet Switch 3 at Substation 1
S1-L5	Line 5 Protection Panel at Substation 1
S1-L1	Line 1 Protection Panel at Substation 1
S1-L2	Line 2 Protection Panel at Substation 1

The circuit breaker reliability data for this section are based on the data from [28], [35]. The reliability data for merging units, Ethernet switches, and line protection panels are not widely available. Based on [28], [33], [34], the failure rates and Mean Repair Times are tabulated in Table 19. Components of the same category are assumed identical and therefore have the same reliability data. In this section, the current and potential transformers are assumed to never fail.

Table 19 Reliability data for components

Component	Failure Rate (/year)	Mean Repair Time (h)
Circuit Breaker	0.01	8
Merging Unit	0.02	8
Ethernet Switch	0.01	8
Line Protection Panel	0.02	8

3.2.3 Link Failure in the Cyber Network

Generally, there are two types of cyber link failures: (a) A link is unavailable due to packet delay resulting from traffic congestion or queue failure; (b) A link is physically damaged. Failure type (b) is relatively rare and thus only failure type (a) is considered in this section.

To illustrate how to model the cyber link unavailability, the cyber part of substation 1 is separated from the physical part and the cyber links are numbered from 1 to 21, as shown in Figure 10.

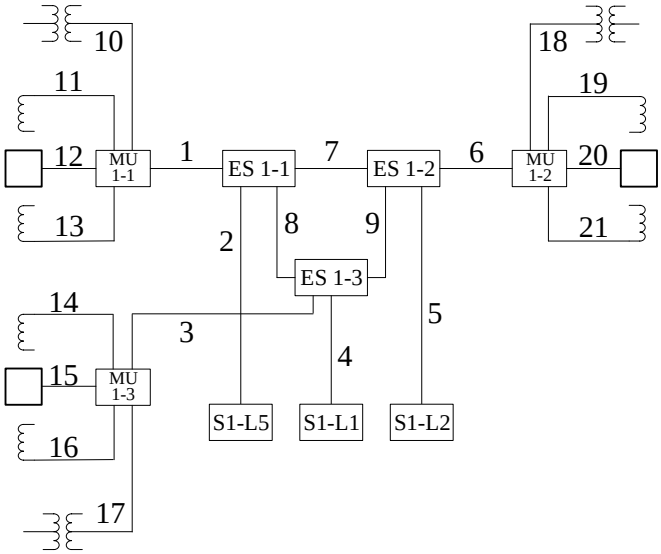

Figure 10. The cyber part of substation 1.

In Figure 10, the traffic on links 10-21 is relatively light compared with other links. Therefore, links 10-21 are considered congestion free.

Each link is bidirectional and each direction has a queue. Consider a link *i* connecting components *a* and *b*. The time it takes for a packet to travel from component *a* to *b* is a random variable denoted by $t_{i.1}$. For the reverse direction (from *b* to *a*), the random time is denoted by $t_{i.2}$. Depending on the arrival and departure stochastic processes associated with each queue on link *i*, the values of $t_{i.1}$ and $t_{i.2}$ follow some probability distribution functions.

Consider the communication from component *a* to *x*. We say this communication is unavailable if the time it takes on every possible path from *a* to *x* is greater than a predefined threshold delay value.

For example, consider the communication from MU 1-1 to S1-L1. There are two possible paths, 1-8-4 and 1-7-9-4. Assuming that all associated links are in forward directions, the probability of communication path failure is:

$$p_{fail} = \Pr[(t_{1.1} + t_{8.1} + t_{4.1} > T_{tsd})\ and\ (t_{1.1} + t_{7.1} + t_{9.1} + t_{4.1} > T_{tsd})] \quad (3.1)$$

where T_{tsd} is a predefined threshold delay value for the two paths.

Therefore, the effects of link failures can be modeled as the probabilities of "communication path failure" between any two components. These probabilities can be obtained by modeling and analyzing the queueing process at both the link and the path levels. The detailed procedures are based on queueing theory and are beyond the scope of this dissertation. These probabilities are assumed directly at the path level. Only the paths between merging units and protection panels are of our interest and the corresponding probabilities are tabulated in Table 20. The probabilities given are an example. The methodology of modeling link failures proposed in this section is general and also applicable for other probability values. For each cyber link, we assume its forward queue and reverse queue are independent. Therefore, for each path, it is assumed that the forward failure and reverse failure are independent.

Table 20 Communication path failure probabilities

From	To	Forward Path Failure Probability	Reverse Path Failure Probability
MU 1-1	S1-L5	0.002	0.002
MU 1-1	S1-L1	0.001	0.001
MU 1-1	S1-L2	0.001	0.001
MU 1-2	S1-L5	0.001	0.001
MU 1-2	S1-L1	0.001	0.001
MU 1-2	S1-L2	0.002	0.002
MU 1-3	S1-L5	0.001	0.001
MU 1-3	S1-L1	0.002	0.002
MU 1-3	S1-L2	0.001	0.001

3.3 Reliability Analysis

The overall procedures can be divided into two stages: (a) Reliability analysis of the cyber part; (b) Reliability evaluation for the entire power system.

In stage (a), the failure modes of individual cyber components and their combinations are examined and analyzed. For each cyber component, only two states, Up and Down, are considered. Besides, there are some assumptions:

1) If the primary protection fails to isolate the fault and the trip signal is transferred to adjacent protection zones, this fault can always be isolated by adjacent protection zones.
2) The current and potential transformers are assumed to always work.

3) Only the first-order primary faults are considered. The situations in which multiple primary faults occur concurrently on different lines are not considered.
4) All the cyber components in this system are considered statistically independent and thus common-mode failures are not considered.
5) A successful operation requires that neither the forward path nor the reverse path is in failure mode.

The objective of stage (a) is to obtain the Consequent Event Matrix (CEM) and the Cyber-Physical Interface Matrix (CPIM), in which the consequent events and their probabilities are summarized. To obtain these probabilities, the consequent events after a primary fault occurs at each line are analyzed. Two states, Up and Down, are considered for each component. The probability of a consequent event can be obtained by multiplying the Up/Down probabilities of the components associated with this event. To illustrate the analysis in stage (a), the procedures of obtaining the probabilities in the first row (corresponding to the primary fault occurring at line 1) are provided as follows. The procedures are similar for primary faults occurring at other lines.

When a primary fault occurs at line 1, there are four possible scenarios.

1) Both of the two terminal circuit breakers operate as intended.

For the convenience of further illustration, the circuit breaker on line 1 at bus 1 side is referred to as “breaker 1-1” and the circuit breaker on line 1 at bus 2 side is referred to as “breaker 1-2”. The operation of breaker 1-1 associates with these components: breaker 1-1, MU 1-3, ES 1-3, Line Protection Panel S1-L1, forward

communication path, and reverse communication path. The Up and Down probabilities of each component can be calculated from the data in Tables 19 and 20. Therefore, the successful operation probability of breaker 1-1, denoted by p_1, can be obtained by multiplying the Up probabilities of all associated components. Similarly, the successful operation probability of breaker 1-2, denoted by p_2, can be obtained by multiplying the Up probabilities of the associated components in bus 2. The product of p_1 and p_2 would be the probability of this consequent event, in which only line 1 will be isolated after the primary fault.

2) Breaker 1-2 operates as intended while breaker 1-1 does not.

In this case, at least one associated component in bus 1 is in Down state while all associated components in bus 2 are in Up state. As a result, lines 1, 2, and 5 will be isolated. The probability of this consequent event is therefore $(1 - p_1)p_2$.

3) Breaker 1-1 operates as intended while breaker 1-2 does not.

In this case, at least one associated component in bus 2 is in Down state while all associated components in bus 1 are in Up state. As a result, lines 1, 3, and 6 will be isolated. The probability of this consequent event is therefore $(1 - p_2)p_1$.

4) Neither breaker 1-1 nor breaker 1-2 operates as intended.

This consequent event is a result from the failure of at least one associated component in bus 1 and at least one associated component in bus 2. The probability of this event is therefore $(1 - p_1)(1 - p_2)$. In this event, lines 1, 2, 3, 5, and 6 will be isolated.

Following similar procedures as performed above, the results of a primary fault occurring at each line are obtained and tabulated in Tables 21 and 22.

After the probabilities of all cyber induced consequent events are obtained in stage (a), the analysis proceeds to stage (b), in which the reliability evaluation is performed at the power system level. Using the two matrices obtained in stage (a), the effects of protection malfunctions can be taken into account without considering the details of the cyber part. The procedures of a Monte Carlo simulation for the reliability evaluation in stage (b) have been formulated in Section 2 [42] of this dissertation. The detailed implementation will be presented in Section 4 of this dissertation. The reliability indices at load points can be obtained after the two stages of analysis.

3.4 Results and Discussions

3.4.1 Results

After the analysis of the cyber part, the Consequent Event Matrix (CEM) and the Cyber-Physical Interface Matrix (CPIM) are obtained, as shown in Tables 21 and 22, respectively.

In the CEM, each entry is an 8-digit binary code in which each digit corresponds to the status of a line. A “1” means that the corresponding line is going out of service after a primary fault whereas a “0” means that the corresponding line is not affected. For example, an entry “11001000” in the first row means that lines 1, 2, and 5 are going out

of service after a primary fault occurs on line 1. It should be noted that the CEM is a result of the failure of cyber part. If the cyber part worked as it is meant to, then a primary fault on a line will not result in the isolation of other lines.

In the CPIM, each entry gives the probability of a consequent event given that a primary fault occurs on a particular line. Each row corresponds to the location of a primary fault. For example, the probability corresponding to the event "11001000" in the first row is the probability of lines 1, 2, and 5 going out of service given that a primary fault already occurred on line 1. If the cyber part had perfect reliability, then column 1 would have probabilities 1 and other columns zero.

Table 21 The consequent event matrix

Primary Fault Location	Consequent Events			
Line 1	10000000	11001000	10100100	11101100
Line 2	01000000	11001000	01010010	11011010
Line 3	00100000	10100100	00110001	10110101
Line 4	00010000	01010010	00110001	01110011
Line 5	00001000	11001000	00000000	00000000
Line 6	00000100	10100100	00000000	00000000
Line 7	00000010	01010010	00000000	00000000
Line 8	00000001	00110001	00000000	00000000

Table 22 The cyber-physical interface matrix

Primary Fault Location	Probabilities of Consequent Events			
Line 1	0.9919152	0.0040342	0.0040342	0.0000164
Line 2	0.9919152	0.0040342	0.0040342	0.0000164
Line 3	0.9919152	0.0040342	0.0040342	0.0000164
Line 4	0.9919152	0.0040342	0.0040342	0.0000164
Line 5	0.9959494	0.0040506	0	0
Line 6	0.9959494	0.0040506	0	0
Line 7	0.9959494	0.0040506	0	0
Line 8	0.9959494	0.0040506	0	0

3.4.2 The Effect of Path Failure Probability

In section 3.2.3, a probability with value 0.002 is assumed as both the forward and the reverse path failure probabilities for the communication path between a merging unit and the corresponding line protection panel. For the convenience of illustration, this probability is called the probability of main path failure. In practice, its value may vary due to data traffic or some other factors. Its value also has an important impact on the probability of successful operations (such as the event “10000000”).

Table 23 shows the relationship between the probability of main path failure and the probability of only line 1 being isolated given that a primary fault already occurred

on line 1. Consider the symmetry of the system configuration, similar relationships exist for the primary faults on other lines.

Table 23 Effect of main path failure on successful operation for line 1

Main Path Failure Probability	Probability of Successful Operation	Compared to 0.9919152
0.002	0.9919152	0.000%
0.004	0.9839879	- 0.799%
0.006	0.9761082	- 1.594%
0.008	0.9682758	- 2.383%
0.01	0.9604907	- 3.168%
0.02	0.9222671	- 7.022%
0.04	0.8492535	- 14.382%

3.4.3 Discussions

From the results shown in Tables 21 and 22, it can be seen that the probabilities of undesired trips due to cyber failures are relatively small. However, such events have significant impact on system reliability. For example, when a primary fault occurs on line 1, the probability of lines 1, 2, 3, 5, and 6 being isolated concurrently is only 0.0000164. But if this consequent event happens, buses 1 and 2 will be isolated from the system with significant amount of load affected. Furthermore, such events may possibly cause severe stability issues. Therefore, the impact of cyber failures on power system

reliability is significant. More detailed evaluation of such impact will be performed in Section 4 of this dissertation.

The results shown in Table 23 indicate a close relationship between the link failure and successful operation probability. The probability of successful operation decreases drastically with increasing communication path failure probability. In some severe cases, for instance, when the main path failure probability increases to 0.02 due to heavy data traffic or queue failure, the probability of successful operation drops below 0.95, which is not acceptable.

3.5 Summary

In this section, a power system configuration is extended to include the Ethernet-based protection architectures with the consideration of cyber link failures. A systematic methodology is implemented to evaluate the reliability of this extended system. The analysis performed in this section is mostly at the substation level. In the following section, reliability evaluation at the composite system level will be performed.

4. COMPOSITE POWER SYSTEM RELIABILITY EVALUATION CONSIDERING CYBER-MALFUNCTIONS IN SUBSTATIONS*

4.1 Introduction

In composite power system reliability evaluation, due to the variety of protection system architectures as well as the diversity of control and communication mechanisms, it is hard to explicitly model protection systems with detailed configurations. As a result, in most of the previous work, protection system failures were either concentrated on circuit breaker trip mechanisms [10] or represented abstractly by multistate models [8], [19]-[21], in which the protection system was treated as a compact object. Some important technical details inside the protection system, such as the placement of cyber elements (e.g., CT/PTs, MUs, and IEDs) and their wire connections, were absent in those publications. Due to the absence of such details, the interdependencies between cyber elements and physical components were not sufficiently covered. In [4] and [5], to study the direct and indirect cyber-physical interdependencies, some mathematical terms and operations were defined and proposed with applications on small test systems including monitoring, control, and protection features. The results in [4] and [5] provide valuable information that indicates the impact of cyber element failures on physical

*Part of this section is reprinted from *Electric Power Systems Research*, vol. 129, Hangtian Lei and Chanan Singh, "Power system reliability evaluation considering cyber-malfunctions in substations", pp. 160-169, ©2015, with permission from Elsevier.

system reliability indices. However, excessive self-defined reliability terms and tedious mathematical operations were introduced in [4] and [5]. These terms are hardly available from engineering practice, making it difficult to implement the overall methodology in practical applications.

A more systematic and scalable methodology was proposed in Section 2 [42] of this dissertation. This methodology performs the overall analysis in a tractable fashion with the use of *Cyber-Physical Interface Matrix* (*CPIM*). In Section 2, a typical substation protection system with detailed architecture was designed and analyzed as an example to illustrate the procedures of obtaining a CPIM. The steps on how to use a CPIM in composite power system reliability evaluation were also formulated. The substation model was further enhanced in Section 3 with the consideration of cyber-link failures.

The composite power system displayed in Section 2 is simple and is used for illustration only. The overall methodology with the use of CPIM needs to be further demonstrated with its implementation on a standard test system so that the impact of protection failures on system-wide reliability indices can be numerically validated. Also, the scalability of the overall methodology needs further illustration as this is very important to its application for large power systems. Moreover, the unavailability of a standard reliability test system containing practical protection features is an obstacle for validation of the impact of protection failures on system-wide reliability indices. Extending a standard reliability test system with detailed descriptions on the cyber part would be beneficial for future studies in this area. With these objectives, this section

continues and enhances the work that has been performed in Section 2. The remainder of this section is organized as follows. Section 4.2 outlines the overall methodology. Section 4.3 presents the test system configuration and parameters. In Section 4.4, the overall analysis, including the reliability analysis at the substation level and the reliability evaluation at the composite system level, is performed. Also, the results are presented and summarized. The scalability of the overall methodology is illustrated in Section 4.5. Some major considerations in software implementation for large power systems are discussed in Section 4.6. Section 4.7 is the summary of this section.

4.2 Methodology Outline and Objectives

The cyber-physical interdependencies exist in many aspects of power systems, including but not limited to supervisory control, protection, monitoring, and metering. This section focuses on the aspect of protection since protection hidden failures are recognized as common causes of expanded outages and have significant impact on power system reliability [7]-[10], [19]-[21].

In this section, reliability evaluation is performed in a composite power system consisting of current-carrying components and protection systems. The Roy Billinton Test System (RBTS) [46] is used as the test system with extensions at load buses to include detailed configuration in terms of protection system elements.

The size of this system is small to permit reasonable time for extension of cyber part and development of interface matrices but the configuration of this system is

sufficiently detailed to reflect the actual features of a practical system [47]. The methodology performed in this section also applies for large systems. For large systems, in spite of more efforts needed in detailed analysis of cyber failure modes as well as effects on the physical side, the main procedures are identical to those performed in this section. In short, the selected system is adequate to illustrate the methodology and extension to larger systems is more mechanical effort rather than illustrating the validity of the technique.

The overall analysis mainly consists of two stages: 1) Reliability analysis of protection systems at the substation level; 2) Reliability evaluation from the system-wide perspective.

4.2.1 Reliability Analysis at the Substation Level

The failure modes of protection systems in terms of basic cyber elements and their relationships to transmission line tripping scenarios are analyzed in this stage. The CPIMs, which depict the interdependencies among the failures of physical components due to various cyber failure modes, are obtained at the end of this stage.

4.2.2 Reliability Evaluation from the System-wide Perspective

In this stage, a sequential Monte Carlo simulation is performed on the composite system to obtain system-wide reliability indices. The results of CPIMs obtained in the

previous stage are directly utilized in this stage without the necessity of considering protection system configuration details. At the end of this stage, system-wide reliability indices, such as Loss of Load Probability (LOLP), Loss of Load Expectation (LOLE), Expected Energy Not Supplied (EENS), and Expected Frequency of Load Curtailment (EFLC), for each bus and for the overall system, can be obtained.

4.2.3 System-wide Reliability Indices

The following system-wide reliability indices [8], [20], [47] are defined and used in this section.

4.2.3.1 Loss of Load Probability (LOLP)

$$LOLP = \sum_{i=1}^{N_s} \frac{H_i t_i}{t_{total}} \tag{4.1}$$

where,

N_s Total number of iterations simulated;

H_i Equals 1 if load curtailment occurs in the i^{th} iteration; otherwise it equals 0;

t_i Simulated time in the i^{th} iteration, with the unit of year;

t_{total} Total simulated time, with the unit of year.

Since a sequential Monte Carlo simulation is performed, "iteration" here means a time period between two instants of system state change.

4.2.3.2 Loss of Load Expectation (LOLE)

$$LOLE = LOLP \cdot 8760 \tag{4.2}$$

with the unit of hours/year.

4.2.3.3 Expected Energy not Supplied (EENS)

$$EENS = \sum_{i=1}^{N_s} \frac{8760 R_i t_i}{t_{total}} \tag{4.3}$$

with the unit of MWh/year,

where,

N_s Total number of iterations simulated;

R_i Load curtailment during the i^{th} iteration, with the unit of MW;

t_i Simulated time in the i^{th} iteration, with the unit of year;

t_{total} Total simulated time, with the unit of year.

4.2.3.4 Expected Frequency of Load Curtailment (EFLC)

$$EFLC = \sum_{i=2}^{N_s} \frac{Z_i}{t_{total}} \tag{4.4}$$

with the unit of (/year),

where,

N_s Total number of iterations simulated;

Z_i Equals 1 if load curtailment does not happen in the $(i\text{-}1)^{th}$ iteration AND load curtailment happens at the i^{th} iteration; otherwise it equals 0;

t_{total} Total simulated time, with the unit of year.

4.3 Test System Configuration

The Roy Billinton Test System (RBTS) [46] is used as the test system in this section. The single line diagram of the RBTS is shown in Figure 11. The bus, generation, load, and transmission line data are also provided in this section. 100 MVA and 230 kV are used as the base values of power and voltage throughout this section.

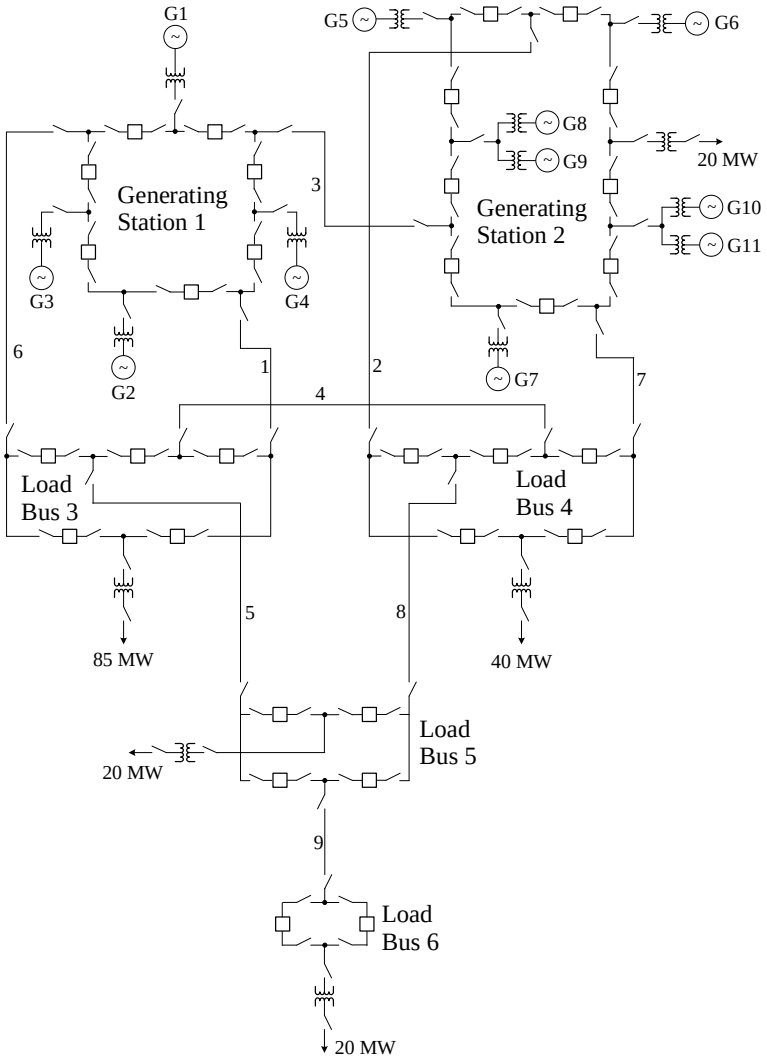

Figure 11. Single line diagram of the RBTS.

4.3.1 Bus, Generation, and Load Data

The data for all the buses and generating units are obtained from [46] and are tabulated in Tables 24 and 25, respectively. A DC optimal power flow model is used in case of load curtailment. Therefore, only the real power data are considered.

Table 24 Bus data

Bus No.	Name in Figure 11	Peak Load (p.u.)	Generation Capacity (p.u.)
1	Generating Station 1	0.00	1.10
2	Generating Station 2	0.20	1.30
3	Load Bus 3	0.85	0
4	Load Bus 4	0.40	0
5	Load Bus 5	0.20	0
6	Load Bus 6	0.20	0

Table 25 Generating unit data

Unit No.	Bus	Rating (MW)	Failure Rate (per year)	MRT (hours)
1	1	40	6.0	45
2	1	40	6.0	45
3	1	10	4.0	45
4	1	20	5.0	45
5	2	5	2.0	45
6	2	5	2.0	45
7	2	40	3.0	60
8	2	20	2.4	55
9	2	20	2.4	55
10	2	20	2.4	55
11	2	20	2.4	55

4.3.1.1 Generation Variation

The generators are represented by reliability models with two states, up and down. The corresponding failure rate and Mean Repair Time (MRT) are obtained from [46] and are tabulated in Table 25.

4.3.1.2 Load Variation

The annual peak load data for each bus are obtained from [46] and are shown in Table 24. The hourly load profile is created based on the information in Tables 1, 2, and 3 of the IEEE Reliability Test System [48].

4.3.2 Transmission Line Data

The transmission line physical parameters and outage data are obtained from [46] and are tabulated in Tables 26 and 27, respectively.

A DC optimal power flow model with simplified line parameters is used in case of load curtailment. Therefore, the line resistance (R) as well as the charging susceptance (B) are not considered in the transmission line model and only the line reactance (X) is provided in Table 26. Furthermore, in the DC optimal power flow model, since the voltage magnitude at each bus is assumed to be 1.0 p.u., the current rating for each line shown in Table 26 is numerically equal to the power rating.

For the transmission line outage data, compared with [46], the transient outage (normally with duration of less than one minute) is not considered in this section. Instead, a new term *switching time* is defined. The switching time for each transmission line, which is tabulated in Table 27, defines the time needed to switch a line back to service when this line is tripped due to a protection failure rather than resulting from a primary fault occurs at this line. The reciprocal of a switching time is called a *switching rate* and has been illustrated in Section 2 of this dissertation.

Table 26 Transmission line physical parameters

Line No.	Buses		Reactance X (p.u.)	Current Rating (p.u.)
	From	To		
1	1	3	0.180	0.85
2	2	4	0.600	0.71
3	1	2	0.480	0.71
4	3	4	0.120	0.71
5	3	5	0.120	0.71
6	1	3	0.180	0.85
7	2	4	0.600	0.71
8	4	5	0.120	0.71
9	5	6	0.120	0.71

Table 27 Transmission line outage data

Line No.	Buses		Permanent Outage Rate (per year)	Outage Duration (hours)	Switching Time (hours)
	From	To			
1	1	3	1.5	10.0	4.0
2	2	4	5.0	10.0	4.0
3	1	2	4.0	10.0	4.0
4	3	4	1.0	10.0	4.0
5	3	5	1.0	10.0	4.0
6	1	3	1.5	10.0	4.0
7	2	4	5.0	10.0	4.0
8	4	5	1.0	10.0	4.0
9	5	6	1.0	10.0	4.0

4.3.3 Protection System Architecture and Reliability Data

For bus 6, since it is connected with only one transmission line (line 9), even if its own protection system fails, line 9 will always be de-energized by opening the breakers at bus 5 without isolating any other lines. Therefore, the protection system configuration at bus 6 is not considered and only buses 3, 4, and 5 in the RBTS are extended to include detailed protection system configurations, as shown in Figures 12, 13, and 14, respectively.

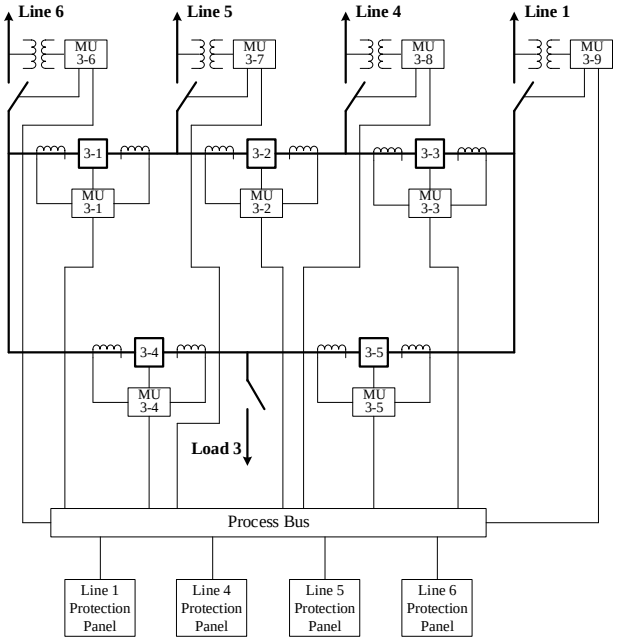

Figure 12. The protection system for bus 3.

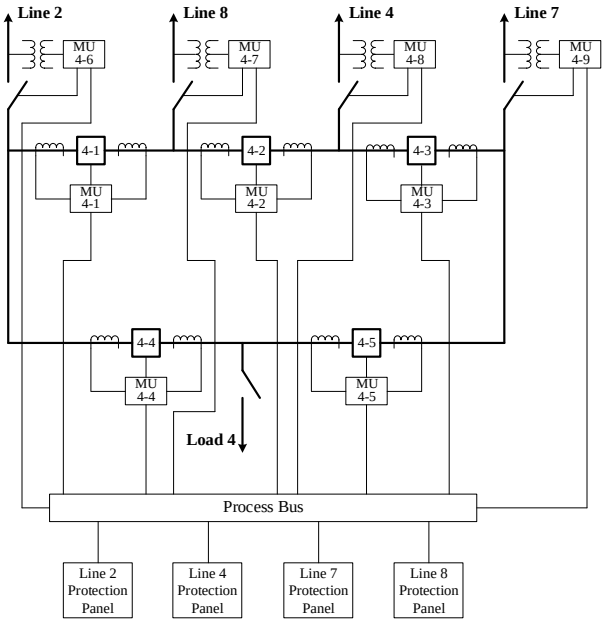

Figure 13. The protection system for bus 4.

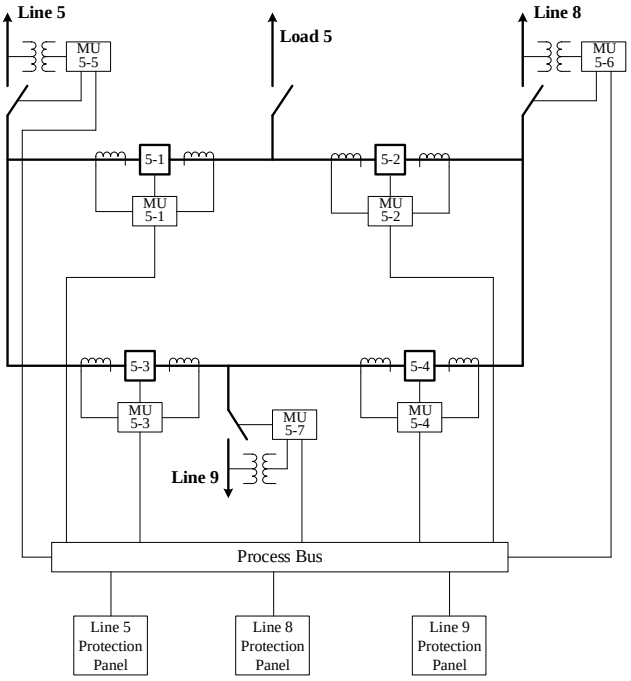

Figure 14. The protection system for bus 5.

The reliability data for Circuit Breakers (CBs), Merging Units (MUs), Process Buses (PBs), and Line Protection Panels are tabulated in Table 28. We assume that a same type of elements at different substations are identical and thereby have the same reliability data.

According to engineering practice, the Mean Time to Failure (MTTF) varies for Circuit Breakers at different voltage levels, or serving different functions in the system [35]. For the study in this section, a typical value of 100 years is chosen for the MTTF and a value of 8 hours is used for the Mean Repair Time (MRT).

The reliability data for MUs, PBs, and Line Protection Panels are reasonably chosen based on the information from [15], [28], [33], and [34].

Table 28 Reliability data for protection system elements

Element Name	MTTF (year)	Failure Rate λ (/year)	MRT (h)	Repair Rate μ (/year)
CB	100	0.01	8	1095
MU	50	0.02	8	1095
PB	100	0.01	8	1095
Line Protection Panel	50	0.02	8	1095

In this study, only two states, UP and DOWN, are considered for each protection system element (except the process bus) listed in Table 28. The state transition diagram is shown in Figure 15. The failure and repair rates are denoted by λ and μ, respectively.

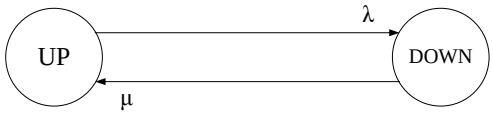

Figure 15. State transition diagram of individual element.

The exponential distribution is assumed for state residence times of each element, the probabilities of UP and DOWN can be calculated using equations (4.5) and (4.6), respectively.

$$p_{UP} = \frac{\mu}{\lambda+\mu} \tag{4.5}$$

$$p_{DOWN} = \frac{\lambda}{\lambda+\mu} \tag{4.6}$$

For the Process Bus (PB), an additional state representing DELAY is included as shown in Figure 16. The probability of delay given that the PB is not in the DOWN state is denoted by p_d (=0.003). The illustration of this reliability model as well as the discussion regarding delay issues in substation communication networks have been presented in Section 2 of this dissertation.

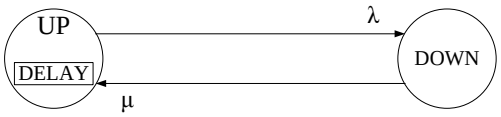

Figure 16. State transition diagram of the process bus.

Therefore, for the Process Bus, the UP, DELAY and DOWN probabilities can be calculated using equations (4.7)-(4.9).

$$p_{UP.PB} = \frac{\mu}{\lambda+\mu}(1 - p_d) \tag{4.7}$$

$$p_{DELAY.PB} = \frac{\mu}{\lambda+\mu}p_d \tag{4.8}$$

$$p_{DOWN.PB} = \frac{\lambda}{\lambda+\mu} \tag{4.9}$$

In reality, the process bus is a network consisting of basic elements that are connected with each other in various topologies and thus more sophisticated technical details are involved [34], [38]-[41]. The consideration of these technical details in composite system reliability evaluation is beyond the scope of this dissertation.

The assumptions regarding other protection elements (e.g., CTs, PTs, and cable links) and protection issues such as backup tripping follow those stated in Section 2 of

this dissertation. The CTs, PTs, and cable links are assumed not to fail. In addition, based on the features of this particular test system, several more assumptions are made:

1) The failure of an MU that is connected to a PT will result in the failure of acquired voltage information and thus will disable the primary protection of this line. As a result, multiple breakers associated with the primary protection will fail to trip and backup protections will be triggered. For example, in the bus 3 protection system (shown in Figure 12), if a primary fault happens at Line 6 but MU 3-6 fails, then the Line 6 Protection Panel will fail to issue trip signals to both breakers 3-1 and 3-4. As a result, backup protection zones will be triggered and breakers 3-2 and 3-5 will trip to isolate Line 6.
2) Since this study focuses on transmission system reliability evaluation and the details of a load branch can be extended in the distribution system. Therefore, primary faults that occur at load branches are not considered. However, the isolation of a load branch resulting from undesired trips due to primary faults that occur at adjacent transmission lines will be considered.

4.4 Reliability Analysis

The overall analysis mainly consists of two stages: the reliability analysis of protection systems at the substation level and the reliability evaluation from the system-wide perspective. The CPIM, which bridges the two stages, is a critical idea of this

methodology. It decouples the analysis at the substation level from the evaluation of the composite system and makes the overall analysis more tractable.

4.4.1 Substation Level Reliability Analysis

The substation level reliability analysis follows the procedures described in Section 2 of this dissertation with the objective of obtaining CPIMs.

This section improves the CPIM that was described in Section 2 by eliminating the off-diagonal zeros to make it more compact. In this section, each row in a CPIM represents a physical component (transmission line). Each column provides the probability of a consequent event given that a primary fault occurred on this physical component. Therefore, the probabilities in each row sum up to 1. If the protection system is perfectly reliable, then the first column would have probabilities 1 and other columns zero.

In addition, another matrix, Consequent Event Matrix (CEM), is developed in accordance with a CPIM. A CEM provides detailed information about consequent events in which some lines go out of service while some are not affected. In a CEM, each event is coded as a 12-digit binary number, of which the left 9 digits correspond to the 9 transmission lines and the last 3 digits correspond to load branches 3, 4, and 5, respectively. A "1" digit indicates the corresponding component is going out of service whereas a "0" means this component is not affected. For example, an entry "100001100110" denotes a consequent event in which line 1, line 6, line 7, load branch

3, and load branch 4 are going out of service. A complete row of a CEM summarizes all possible consequent events when a primary fault occurs at this transmission line.

To illustrate how the malfunctions of cyber elements affect transmission line tripping behaviors, the detailed analysis for the consequent events resulting from cyber element failures at substation (bus) 3 following a primary fault occurs at line 1 is shown below as an example. The analysis for the primary faults at other lines can be performed similarly. In the analysis, the failure modes of individual cyber elements are assumed independent since they are located in different units in a substation. Therefore, the probability of a consequent event can be obtained by multiplying the probabilities of individual element states in this event.

Suppose a primary fault occurs at line 1, all possible consequent events can be categorized as follows.

1) All protection elements operate as intended.

If all protection elements operate as intended, then only line 1 will be isolated. The action of line 1 tripping associated with these elements at substation 3: MU 3-9, CB 3-3, MU 3-3, CB 3-5, MU 3-5, Process Bus, and Line 1 Protection Panel. Multiply the UP probabilities of all these elements, the corresponding probability of this consequent event can be obtained, which is 0.996899850569.

2) The Process Bus (PB) fails.

If the PB fails, then the entire substation will be affected by this fault. All lines connected to this substation will be isolated by tripping the breakers at remote substations. The corresponding probability of this consequent event can be calculated

using Equation (4.9). This is an extreme case therefore the probability is very low. However, once this event happens, the impact is tremendous.

3) One or both of MU 3-3, CB 3-3 fail(s), while all other associated elements operate as intended.

In this case, CB 3-3 fails to trip while CB 3-5 trips as intended. The fault will be cleared by opening CB 3-2 and CB 3-5. As a result, Lines 1 and 4 will be isolated.

4) One or both of MU 3-5, CB 3-5 fail(s), while all other associated elements operate as intended.

In this case, CB 3-5 fails to trip while CB 3-3 trips as intended. The fault will be cleared by opening CB 3-3 and CB 3-4. As a result, Line 1 and load branch 3 will be isolated.

5) The Process Bus (PB) doesn't fail, but both CB 3-3 and CB 3-5 fail to trip due to various combinations of element states, such as Line 1 Protection Panel fails or the PB is in a DELAY state.

In this case, the fault will be cleared by opening CB 3-2 and CB 3-4. As a result, Line 1, Line 4, and load branch 3 will be isolated.

The results of all the 5 cases above are summarized in the first row of Table 29 and Table 30. It should be noted that these consequent events are the results from cyber element failures. If the all associated cyber elements are perfectly reliable, then the first case would have probability one while all other cases zero.

Following similar procedures performed above, the complete Cyber-Physical Interface Matrices (CPIMs) and Consequent Event Matrices (CEMs) for buses 3, 4, and 5 are obtained and are shown from Table 29 to Table 34.

Table 29 The cyber-physical interface matrix for bus 3

Fault Location	Probabilities				
Line 1	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112
Line 4	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112
Line 5	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112
Line 6	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112

Table 30 The consequent event matrix for bus 3

Fault Location	Events				
Line 1	100000000000	100111000000	100100000000	100000000100	100100000100
Line 4	000100000000	100111000000	000110000000	100100000000	100110000000
Line 5	000010000000	100111000000	000011000000	000110000000	000111000000
Line 6	000001000000	100111000000	000001000100	000011000000	000011000100

Table 31 The cyber-physical interface matrix for bus 4

Fault Location	Probabilities				
Line 2	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112
Line 4	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112
Line 7	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112
Line 8	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112

Table 32 The consequent event matrix for bus 4

Fault Location	Events				
Line 2	010000000000	010100110000	010000000010	010000010000	010000010010
Line 4	000100000000	010100110000	000100010000	000100100000	000100110000
Line 7	000000100000	010100110000	000100100000	000000100010	000100100010
Line 8	000000010000	010100110000	010000010000	000100010000	010100010000

Table 33 The cyber-physical interface matrix for bus 5

Fault Location	Probabilities				
Line 5	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112
Line 8	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112
Line 9	0.996899850569	0.000009132337	0.000027312491	0.000027312491	0.003036392112

Table 34 The consequent event matrix for bus 5

Fault Location	Events				
Line 5	000010000000	000010011000	000010001000	000010000001	000010001001
Line 8	000000010000	000010011000	000000010001	000000011000	000000011001
Line 9	000000001000	000010011000	000000011000	000010001000	000010011000

4.4.2 System-wide Reliability Evaluation

The next event sequential Monte Carlo simulation [37] forms the main framework for the reliability evaluation at this stage. The detailed steps, including illustrations on how to utilize the results of a CPIM in the composite system reliability evaluation, have been illustrated in Section 2 and are summarized as follows.

1) Initialize.
2) Determine a primary event: Find the minimum time to the next event, update the corresponding element's state, and update the total time.
3) Determine consequent events: If the state change in step 2) indicates a primary fault occurring at a transmission line, then use CPIMs and CEMs to determine the consequent events and update elements' states accordingly. If a CPIM row corresponding to this transmission line has n consequent events, the probabilities of these events (p_1, p_2, …, p_n) sum up to 1. Draw a random number ranging from 0 to 1. The value of this random number determines which consequent event is going to happen. It should be noted that a

transmission line connects two substations. Therefore, two random numbers should be drawn independently to determine the consequent event at each substation.

4) Effects of switching and repair: For the elements whose states have been changed in step 2) or in step 3), draw new random numbers to determine the time of their next transitions. Appropriate transition rates should be used according to situations.
5) Evaluate system state: Perform the network power flow analysis to assess system operation states. Update reliability indices.
6) Repeat steps 2) to 5) until convergence is achieved.

In step 5), the following DC power flow based linear programming model [49]-[51] is used with the objective of minimizing total load curtailment.

Objective: $y = Min \sum_{i=1}^{N_b} C_i$

subject to:

$$\hat{B}\theta + G + C = L \tag{4.10}$$

$$G \leq G^{max}$$

$$C \leq L$$

$$DA\theta \leq F^{max}$$

$$-DA\theta \leq F^{max}$$

$$G, C \geq 0$$

$$\theta_1 = 0$$

$\theta_{2 \ldots N_b}$ unrestricted

where,

N_b	Number of buses
C	$N_b \times 1$ vector of bus load curtailments
C_i	Load curtailment at bus i
$\hat{B}$	$N_b \times N_b$ augmented node susceptance matrix
G	$N_b \times 1$ vector of bus actual generating power
G^{max}	$N_b \times 1$ vector of bus maximum generating availability
L	$N_b \times 1$ vector of bus loads
D	$N_t \times N_t$ diagonal matrix of transmission line susceptances, with N_t the number of transmission lines
A	$N_t \times N_b$ line-bus incidence matrix
θ	$N_b \times 1$ vector of bus voltage angles
F^{max}	$N_t \times 1$ vector of transmission line power flow capacities

In equation (4.10), the variables are vectors θ, G, and C. Thus, the total number of variables is $3N_b$. This problem can be solved by using the *linprog* function provided in MATLAB software.

The convergence is measured by the coefficient of variation of a chosen index, as defined in [47]. A simulation with 200 simulated years is performed and the coefficient of variation for the system EENS drops below 5%.

4.4.3 Results and Discussions

The simulation results of LOLP, LOLE, EENS, and EFLC for each bus and for the overall system are tabulated in Table 35. The simulated transmission line failure rates due to primary faults and protection system malfunctions are tabulated in Table 36. In Table 36, for line 3, the simulated line failure rate due to protection system malfunctions equals 0. This is because line 3 links bus 1 to bus 2 and protection malfunctions are not considered for either of the two buses.

To make a comparison, the situation in which protection systems are assumed perfectly reliable is also simulated with results tabulated in Table 37. The comparison is also displayed in Figure 17.

Table 35 Reliability indices for buses

	LOLP	LOLE (hours/year)	EENS (MWh/year)	EFLC (/year)
Bus 1	0	0	0	0
Bus 2	0.00015926	1.395	2.655	0.260
Bus 3	0.00017063	1.495	8.597	0.300
Bus 4	0.00019288	1.690	10.095	0.315
Bus 5	0.00016786	1.470	3.729	0.275
Bus 6	0.00124176	10.878	116.104	1.305
Overall System	0.00128584	11.264	141.180	1.395

Table 36 Simulated transmission line failure rates

Line No.	Failure rate resulting from primary faults (/year)	Failure rate resulting from protection malfunctions (/year)
1	1.455	0.010
2	4.850	0.005
3	3.870	0
4	1.030	0.075
5	0.925	0.010
6	1.570	0.010
7	5.100	0.005
8	1.080	0.010
9	1.030	0.010

Table 37 EENS comparison

	EENS (MWh/year)		Δ
	If protection systems are perfectly reliable	Considering protection malfunctions	
Bus 1	0	0	N/A
Bus 2	1.862	2.655	42.59%
Bus 3	2.828	8.597	204.00%
Bus 4	1.950	10.095	417.69%
Bus 5	2.145	3.729	73.85%
Bus 6	103.947	116.104	11.70%
Overall System	112.732	141.180	25.24%

For each row, Δ is defined as the percentage increment of the EENS from not considering to considering protection malfunctions.

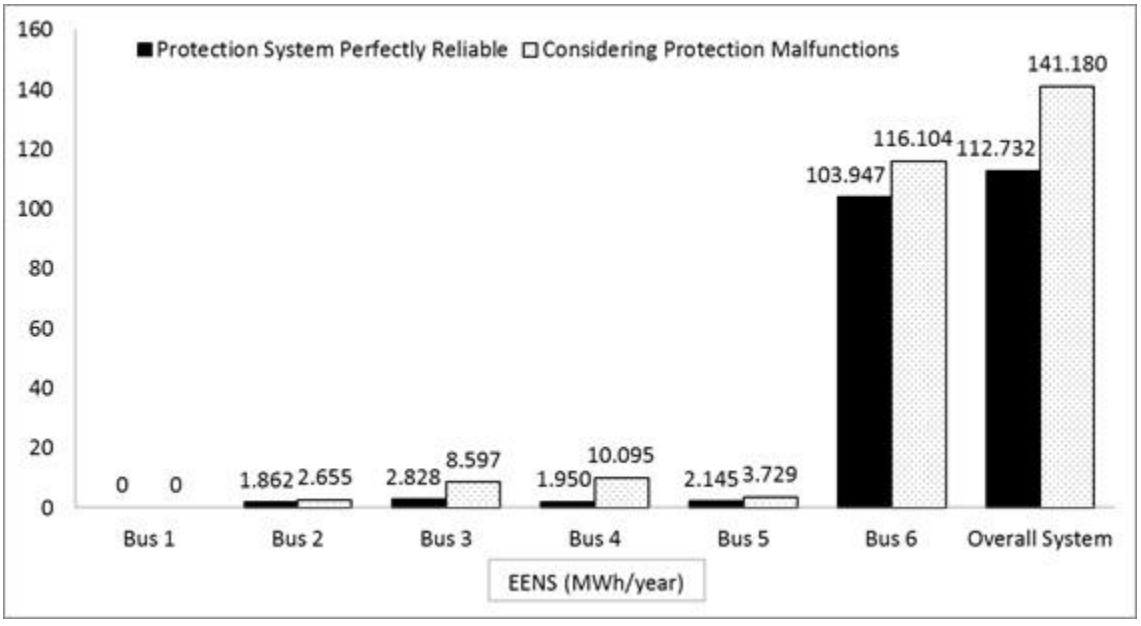

Figure 17. EENS comparison at each bus.

The results in Tables 36 and 37 show that protection system malfunctions have significant impact on energy unavailability even though they do not have much impact on individual line failure rates. Compared with not considering protection malfunctions, the percentage increment of the EENS for individual buses can be quite significant.

The effects of protection system malfunctions on EENS are noticeable for buses 3, 4, and 5, with increments of 204.00%, 417.69%, and 73.85%, respectively. These three buses are also the ones in which we have modeled and considered protection system malfunctions. This further points to the impact of protection malfunctions on energy unavailability.

4.4.4 The Effects of Switching Time

A value of 4.0 hours is assumed as the switching time for all transmission lines and this value has been used in the analysis in Sections 4.4.1 and 4.4.2.

In engineering practice, a switching process may be accelerated with the aid of smart grid technologies, or may be prolonged due to other factors. The quantitative relationship between switching time and system EENS are studied and the results are shown in Table 38. In each case, same value of switching time is assumed for all transmission lines and the system EENS is compared with the case in which the switching time is 4.0 hours. This relationship is also displayed in Figure 18.

Table 38 Effect of switching time on system EENS

Switching Time (hours)	System EENS (MWh/year)	Percentage increment/decrement compared with the value of 141.180 MWh/year in Table 37
0.2	115.089	-18.48%
0.5	120.941	-14.34%
1	126.945	-10.08%
2	132.675	-6.02%
4	141.180	0
10	157.615	+11.64%
24	178.986	+26.78%
48	190.628	+35.02%

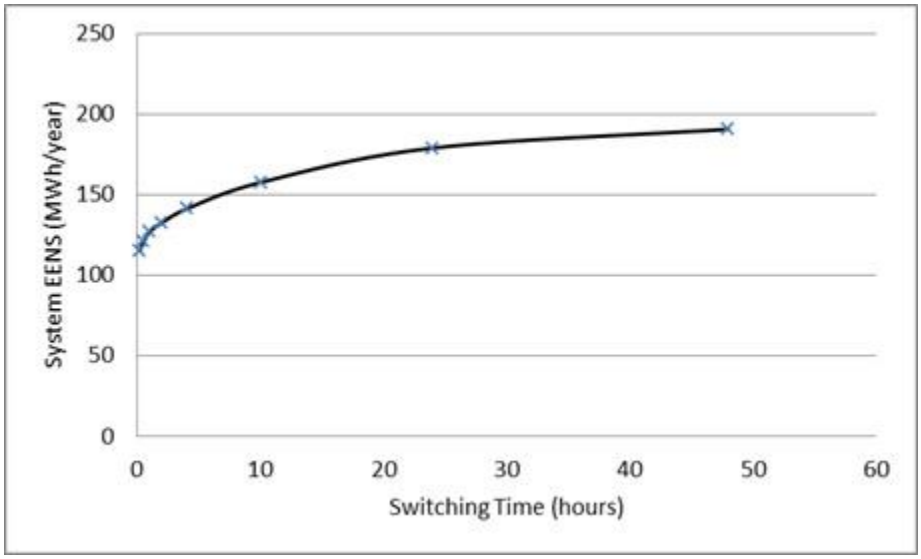

Figure 18. Relationship between switching time and system EENS.

The information in Table 38 and Figure 18 indicate a close relationship between the line switching time and the system EENS. The value of system EENS increases considerably with prolonged switching time. This also signifies the importance of using advanced technologies with which the process of fault location and cyber failure identification would be accelerated so that healthy lines can be switched back to service more promptly.

4.5 The Scalability of the Overall Methodology

As shown in Section 4, the overall methodology consists of two stages:

1) Reliability analysis at the substation level (i.e., the work performed in Section 4.4.1).
2) System-wide reliability evaluation (i.e., the work performed in Section 4.4.2).

In the first stage, the detailed analysis depends on the actual protection architecture of a substation. The analysis may seem to be tedious for a substation with complex architecture. However, the analysis in this stage can be performed locally at each substation and the computations can be performed offline. The increased workload for more complex substations does not change the framework of the overall methodology. It should be noted that although in this stage, the analysis is needed for each individual substation, with more experience in the analysis at substation level, it may be possible to generate classifications into types of substations and thus expedite the process.

Once the CPIMs and CEMs are established in the first stage, they can be permanently stored and can be directly plugged into the reliability evaluation in the second stage. The Monte-Carlo simulation performed in the second stage is generic and applicable for large power systems.

The CPIM decouples the first stage of analysis from the second stage and makes the overall analysis more tractable.

4.6 Considerations in Software Implementation for Large Power Systems

The proposed methodology establishes a framework for power system reliability evaluation considering cyber-malfunctions in substations. Some implementation considerations are important to its application for large power systems. This section discusses two major considerations, the CPU time for Monte Carlo simulation and the storage of matrices.

4.6.1 CPU Time for Monte Carlo Simulation

The convergence in a Monte Carlo simulation is measured by the coefficient of variation of a chosen index. In this section, simulation is performed for 200 years and the coefficient of variation for the system EENS drops below 5%. The simulation is performed in MATLAB running on a computer with a 3.10 GHz processor and the running time for a simulation is approximately 8 minutes. It should be noted that this

software implementation of the simulation is only research grade to illustrate the concept and is therefore not the most efficient as far as the running time is concerned. The running time is largely consumed by the *linprog* function in MATLAB for DC power flow based linear programming to evaluate system operation states. In the development of a commercial grade program, the running time can be drastically reduced by several means as described below.

1) The linear programming incorporating DC power flow can be performed less frequently with the use of heuristic algorithms for screening, thus reducing the CPU time.
2) Simulation can be custom coded in more efficient programming languages. Custom programs are generally more efficient than generic ones coded in MATLAB.
3) Much more efficient methods such as interior point methods can be used for linear programming.
4) Monte Carlo simulation is readily amenable to parallel and distributed processing environments [52], [53] to reduce the CPU time.

It is important to mention that Monte Carlo simulation has already been successfully used for large composite power systems but without considering the cyber-malfunctions. The major contribution of this dissertation is to develop a methodology to include cyber induced dependent failures in such Monte Carlo programs. The cyber induced dependent failures can be included in Monte Carlo simulation by using CPIMs.

This does not significantly alter the number of times linear programming is called for and thus does not alter the CPU time much.

4.6.2 Storage of Matrices

For a given power system, let *m* be the total number of rows in all CPIMs (or CEMs), *n* be the number of columns in a CPIM (or a CEM).

The value of *m* depends on the number of transmission lines. The number of transmission lines in an actual power system is typically 1.2 to 2 times of the number of buses. Each transmission line contributes a row in two CPIMs (or CEMs) corresponding to both of the two buses it connects to. Consider a power system with 1000 buses (substations), which is a typical size of an actual transmission grid, it is reasonable to estimate the number of transmission lines as 2000 and thus the value of *m* is estimated to be 4000.

The value of *n* is determined by the row with maximum number of consequent events, which depends on the transmission line having maximum number of adjacent lines. Assuming a transmission line has maximum 10 adjacent lines, thus the maximum possible value of *n* is 2^{10}, which is 1024. Of course, it is possible that a few transmission lines may have more than 10 adjacent lines. For such lines, only the 1024 most likely consequent events are considered since the remaining consequent events have negligible probabilities. Thus, it is reasonable to estimate *n* as 1024.

Each entry in a CPIM can be stored as a 64-bit double-precision floating-point number. Therefore, the total storage space needed for all CPIMs is $8 \cdot m \cdot n$ Bytes, which equals 31.25 MB (32,768,000 Bytes).

Each entry in a CEM is a binary number corresponding to a consequent event. For a system with 2000 transmission lines, 2000 bits are needed to represent such an event. Thus, each entry uses 250 Bytes (2000 bits) and the total storage space needed for all CEMs is $250 \cdot m \cdot n$ Bytes, which equals 976.5625 MB (1,024,000,000 Bytes).

Therefore, for a power system with 1000 buses, the total space needed to store all CPIMs and CEMs is estimated to be 1007.8125 MB, which is approximately 0.9842 GB. It is feasible to claim such space on hard drive or Random Access Memory (RAM).

4.7 Summary

In this section, a systematic reliability evaluation methodology is enhanced and implemented in a composite power system consisting of current-carrying components and protection systems with modern architecture. The quantitative relationship between switching time and system EENS is also studied. The results clearly indicate the impact of protection failures on system-wide reliability indices and also signify the importance of accelerating line switching process.

The methodology implemented in this section is scalable and provides an option for the reliability evaluation of large cyber-physical power systems. For such systems, in

spite of more efforts needed in detailed analysis, the main procedures remain similar to those performed in this section.

It should be noted that the methodology performed in this section is based on a sequential Monte Carlo simulation. It would be significantly beneficial for its application in large systems if the efficiency is further improved with the use of non-sequential techniques since non-sequential techniques generally require less computational and storage resources compared to sequential ones. Pertinent studies will be performed in the following section.

5. NON-SEQUENTIAL MONTE CARLO SIMULATION FOR CYBER-INDUCED DEPENDENT FAILURES IN COMPOSITE POWER SYSTEM RELIABILITY EVALUATION

5.1 Introduction

Cyber-induced dependent failures affect power system reliability and thus are important to be considered in composite system reliability evaluation. A scalable methodology is proposed in Section 2 [42] of this dissertation with the use of Cyber-Physical Interface Matrix (CPIM) that decouples the analysis of the cyber part from the physical part and provides the means of performing the overall analysis in a tractable fashion. In Section 4 [54], this methodology is further enhanced and implemented on an extended Roy Billinton Test System (RBTS) with the illustration of its applicability for large power systems.

The techniques used in Monte Carlo simulations can be basically classified into two categories known as sequential and non-sequential techniques [55]-[57]. The methodology presented in Section 2 and Section 4 is based on a sequential Monte Carlo technique and establishes the main framework for reliability evaluation of cyber-physical power systems. Non-sequential methods are typically easier to implement and require much less computational and storage resources as compared to sequential methods [3], [23], [24]. Therefore, it would be significantly beneficial for the application of the proposed methodology in large systems if the efficiency is further improved with

the use of non-sequential techniques. However, the failure and repair processes in cyber-induced events are inherently sequential involving dependent failures, making it very difficult to utilize a non-sequential sampling throughout the complete process in the same manner as in independent components by sampling the component states individually.

It has been recognized that the basic idea in sampling is to sample states from a state space proportional to their probabilities [23]. For a large system it is not possible to first find the probabilities of all the states in the state space. Therefore, an approach is proposed in this section with the basic idea of developing a representative state space from which states can be sampled. This is achieved here by the use of sequential Monte Carlo simulation as the computational effort needed for only generating a chronological state sequence is negligible compared to the effort of evaluating the states using DC power flow based linear programming. A similar approach, called *pseudo-sequential simulation*, has been proposed in [24] but for completely different purposes. In [24], the approach is proposed with the purpose of computing duration-related reliability indices. In this section, the purpose is to include the characteristics of cyber-induced dependent failures. Also a method is used in this section such that the state space generated by sequential simulation does not need to be stored. Furthermore, it should be noted that the sequential simulation may not be the only option for state space generation thus there may be alternative solutions. The major difficulties of applying conventional non-sequential sampling methods to generating appropriate state space in the presence of dependent failures are also thoroughly explored in this section with the intention of

enlightening future studies on this subject as composite power system reliability evaluation in the presence of dependent failures has not received sufficient attention.

The remainder of this section is organized as follows. Section 5.2 describes the overall problem. Section 5.3 illustrates the major difficulties of applying conventional non-sequential sampling methods to generating appropriate state space in presence of dependent failures. Section 5.4 introduces the proposed method with the use of sequential technique for state space generation. The implementation of the proposed method is demonstrated in Section 5.5. Section 5.6 is the summary of this section.

5.2 Origination of Dependent Failures

Traditional power system reliability evaluation focuses on the physical part only and assumes perfect reliability for the cyber part, which neglects cyber-induced failures and results in too optimistic evaluation. For realistic evaluation, it is necessary to consider cyber-induced failures as well as their impact on composite systems.

Due to the complexity of cyber-physical interdependencies, it is hard and impractical to explicitly model and analyze the entire system, cyber and physical, in one step. A methodology has been proposed in Section 2 of this dissertation with the use of Cyber-Physical Interface Matrix (CPIM) to decouple the analysis of the cyber part from the physical part so that the overall evaluation is performed in a tractable fashion.

The format of a Cyber-Physical Interface Matrix is shown in Table 39. It can be obtained by examining the failure modes of cyber components and their impact on the physical system.

Table 39 The format of a cyber-physical interface matrix

	Event 1	Event 2	……	Event *n*
Component 1	p_{11}	p_{12}	……	p_{1n}
Component 2	P_{21}	P_{22}	……	P_{2n}
……	……	……	……	……
Component *m*	P_{m1}	p_{m2}	……	P_{mn}

The number of rows in a CPIM, denoted by *m*, corresponds to the number of transmission lines. The number of columns, denoted by *n*, corresponds to the number of consequent events. Consider a transmission line l ($0 < l \leq m$) with k adjacent lines. When a fault occurs at line l, 0–k of its unfaulted adjacent lines can be isolated due to cyber malfunctions with 2^k maximum possible cases. The complete row l in a CPIM summarizes the probabilities of all possible consequent events (cases) given that a fault occurs at transmission line l. These probabilities are obtained by analyzing cyber element failure cases and their impact on transmission line tripping behaviors. It should be noted that these probabilities are a result of cyber failures. If the cyber part is perfectly reliable, there is only one consequent event with probability 1 in each row corresponding to the isolation of the faulty transmission line only.

In applications, another matrix called Consequent Event Matrix (CEM) is used as an auxiliary matrix for CPIM to identify specific components involved in a consequent event. The detailed illustrations of the CPIM and CEM have been presented in Section 4 of this dissertation.

Once the CPIM is obtained, its results can be directly utilized in the composite system reliability evaluation without the necessity of considering cyber element details. The steps of a sequential Monte Carlo simulation can be outlined as follows:

1) Generate a chronological sequence of system state by drawing random numbers for each physical component and applying the load profile;
2) Evaluate each system state and update reliability indices;
3) If a state transition associates with a fault occurs on a transmission line, such as line i, then the i^{th} row of the CPIM is used to determine the consequent event. The probabilities of n possible events (p_{i1}, p_{i2}, …, p_{in}) in the i^{th} row sum up to 1. Draw a random number r ($0 < r < 1$). The value of r determines which consequent event is going to happen. Update all affected component states in the determined consequent event;
4) For the components whose states have been changed in step 2) or step 3), draw new random numbers to determine the time of their next transitions to update the chronological system state sequence;
5) Repeat steps 2) to 4) until the convergence criterion is achieved.

The steps shown above are completely based on sequential techniques. Non-sequential techniques typically require much less CPU time and memory as compared to

sequential techniques and thus are preferable in applications for large systems. In order to seek possible non-sequential techniques that could be applied in the situation described above, it is important to first discuss the difficulties of applying conventional non-sequential sampling methods to generating appropriate state space in presence of cyber-induced dependent failures or other types of dependent failures, as presented in the following section.

5.3 Problem of Applying Non-sequential Sampling for Dependent Failures

It is important to first examine the basic idea of sampling a state in non-sequential simulation in order to appreciate the problem of applying it to systems with dependent failures. Let us say that the state space S is defined by all states $x \in S$ where the state x is represented by the states of components:

$$x = (x_1, x_2, \ldots, x_n)$$

where x_i represents the state of component i.

Now if the probabilities of all the states x of the system (i.e., the joint probability distribution of components) are known, then we can sample states by drawing a random number between 0 and 1 and formulating a process as follows. The interval between 0 and 1 can be divided into segments equal to the number of system states, the length of a particular segment being equal to the probability of the state that the segment represents. Then one has to determine which segment the random number drawn falls in and that determines the state that is sampled. In practice it is more convenient to construct the

probability distribution function of *x* and determine the state. For example let us assume that the system has five states with their probabilities as shown in Figure 19 (a). These can be organized as a distribution function shown in Figure 19 (b). Now a random number between 0 and 1 can be drawn and put on the probability axis and the random variable axis to give the system state sampled. One should remember that the basic idea is that the states should be sampled proportional to their probabilities.

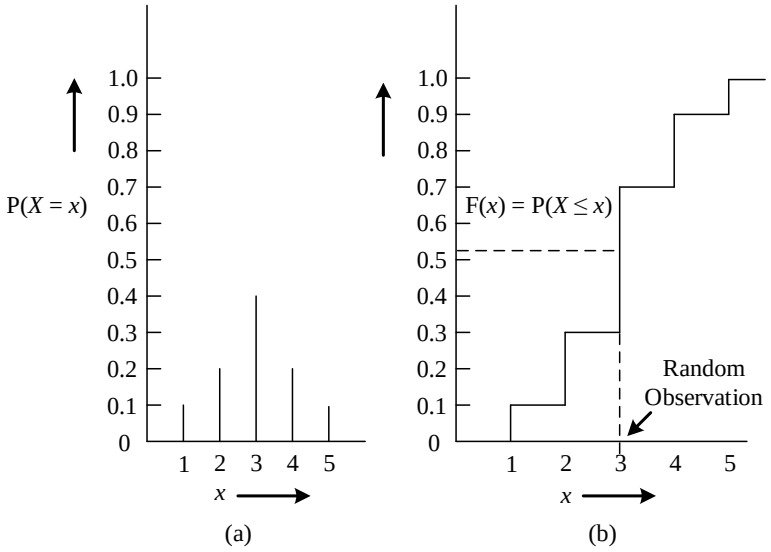

Figure 19. An example of sampling.

The difficulties of applying conventional non-sequential sampling methods to generating appropriate state space in presence of dependent failures are discussed in this section.

A small power system with three components is shown in Figure 20. Each component has two states, Up and Down. The scenarios in which the components are

completely independent, partially independent, and fully dependent are illustrated respectively as follows.

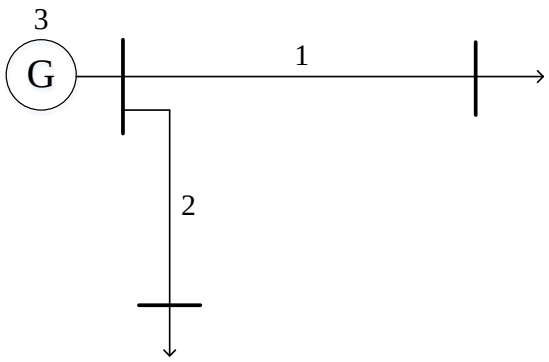

Figure 20. A three-component system.

5.3.1 Completely Independent Scenario

In this scenario, the failure modes of all three components shown in Figure 20 are independent from each other. The corresponding state space transition diagram for the system is shown in Figure 21.

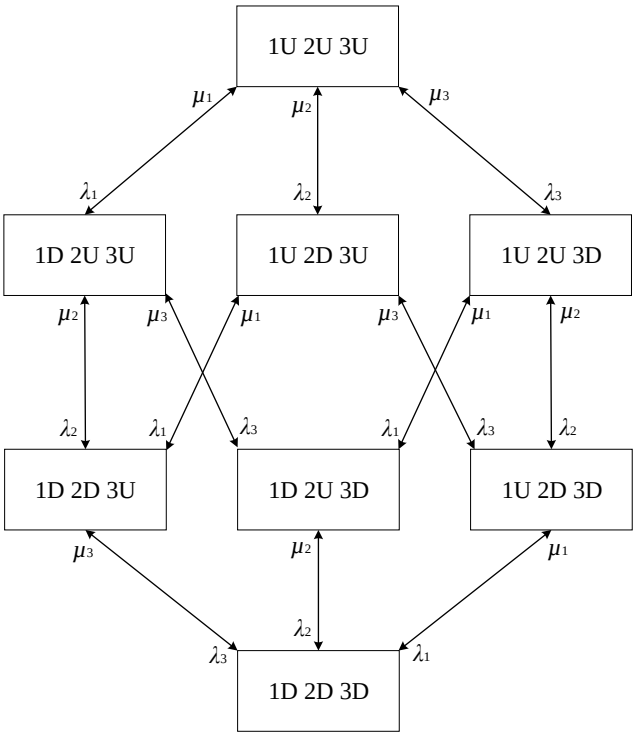

Figure 21. The system state space diagram for completely independent scenario.

The letters "U" and "D" represent Up and Down states, respectively. λ_i $(1 \leq i \leq 3)$ represents the failure rate of component i. μ_i $(1 \leq i \leq 3)$ represents the repair rate of component i.

Because of the independence of individual component failure modes, the system state space can be decoupled into component states, as shown in Figure 22. When performing a non-sequential sampling, the states of individual components can be sampled independently and their combination yields a system state. For example, if the sampled states of individual components are 1U, 2D, and 3D, then the system state is (1U, 2D, 3D). It is actually this ability to sample a system state by a combination of

component states that makes the non-sequential method powerful as the probabilities of all the system states do not need to be known before sampling but only the probabilities of component states need to be known. The components can be two-state or multi-state but so long as they are independent, their states can be sampled at the component level.

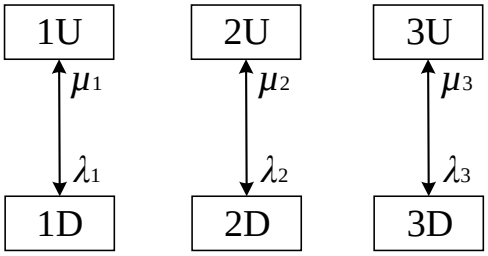

Figure 22. The state transition diagrams for individual components.

The Up and Down probabilities of individual components are readily computable. With the assumption of exponential reliability distribution, the Up and Down probabilities can be computed using equations (5.1) and (5.2), respectively.

$$p_{Up-i} = \frac{\mu_i}{\lambda_i + \mu_i} \tag{5.1}$$

$$p_{Down-i} = \frac{\lambda_i}{\lambda_i + \mu_i} \tag{5.2}$$

5.3.2 Partially Independent Scenario

In this scenario, components 1 and 2 have a common failure mode with failure rate λ_{c12}, as shown in Figure 23.

Component 3 is still independent from components 1 and 2. The corresponding state space transition diagram for the system is shown in Figure 24.

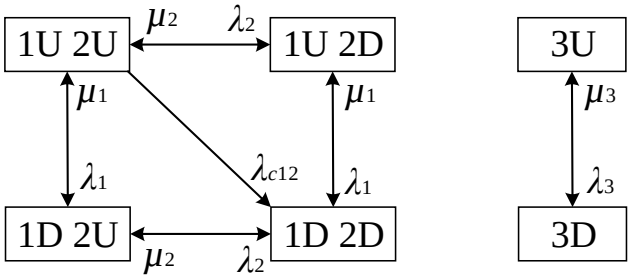

Figure 23. The state transition diagrams for partially independent scenario.

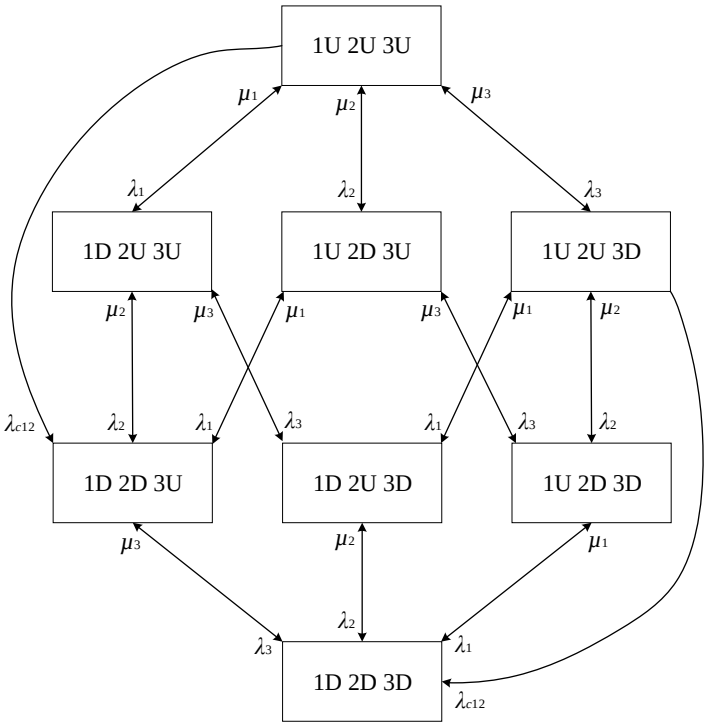

Figure 24. The system state space diagram for partially independent scenario.

In this scenario, the system state space can still be decoupled if components 1 and 2 are treated as a joint unit with four states. However, the probabilities of the four states need to be computed before performing a non-sequential sampling to generate the system state space. The four states, denoted by p_{1U2U}, p_{1U2D}, p_{1D2U}, p_{1D2D}, can be obtained by solving equation (5.3). This requires more effort in analytical analysis compared to the previous scenario.

$$\boldsymbol{BP} = \boldsymbol{C} \tag{5.3}$$

where,

$\boldsymbol{P} = [p_{1U2U} \quad p_{1U2D} \quad p_{1D2U} \quad p_{1D2D}]^T$

$$\boldsymbol{B} = \begin{bmatrix} -(\lambda_2 + \lambda_1 + \lambda_{c12}) & \mu_2 & \mu_1 & 0 \\ 1 & 1 & 1 & 1 \\ \lambda_1 & 0 & -(\mu_1 + \lambda_2) & \mu_2 \\ \lambda_{c12} & \lambda_1 & \lambda_2 & -(\mu_1 + \mu_2) \end{bmatrix}$$

$\boldsymbol{C} = [0 \quad 1 \quad 0 \quad 0]^T$

Once the four state probabilities are obtained, components 1 and 2 can be treated as a joint unit. The Up and Down probabilities of component 3 are readily computable from equations (5.1) and (5.2). A non-sequential sampling can be performed accordingly.

5.3.3 Fully Dependent Scenario

In this scenario, components 1 and 2 have a common failure mode with transition rate λ_{c12} and components 2 and 3 have a common failure mode with transition rate λ_{c23}.

All three components also have a common failure mode with transition rate λ_{c123}. The corresponding state space transition diagram for the system is shown in Figure 25.

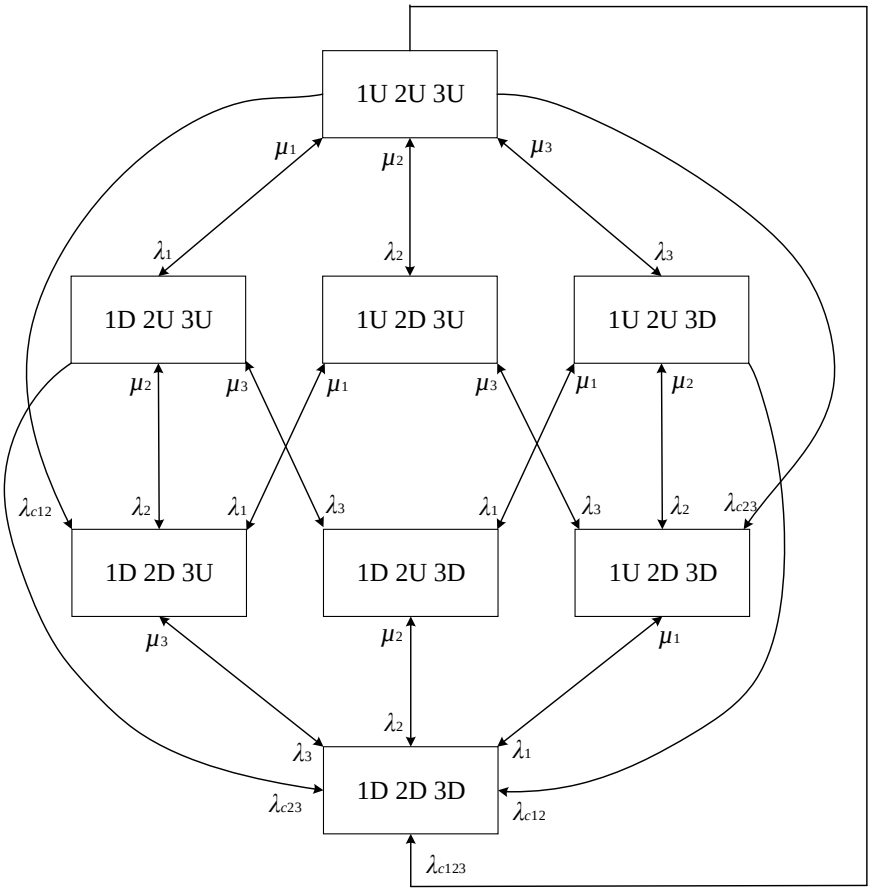

Figure 25. The system state space diagram for fully dependent scenario.

In this scenario, it requires that the probabilities of all the system states be known before sampling can be performed. Due to the dependencies existing among all components, it is very difficult to decouple the system state space into mutually independent disjoint subsets with state probabilities readily available so that a non-

sequential sampling can be conveniently performed. It is possible to analytically compute the system state probabilities for a small system with only a few components. However, for a large system consisting of highly dependent components, it is impractical to analytically compute the probabilities of all the system states before sampling is performed. This is what makes the application of non-sequential methods to systems with dependent failures challenging.

5.4 Proposed Method

The state space for an actually power system may consist of numerous states, as shown in Figure 26. Due to the effects of cyber-induced failures, various transitions exist among these system states. Examples of transitions can be a primary fault, a repair process, a cyber-induced expanded outage, or a switching process.

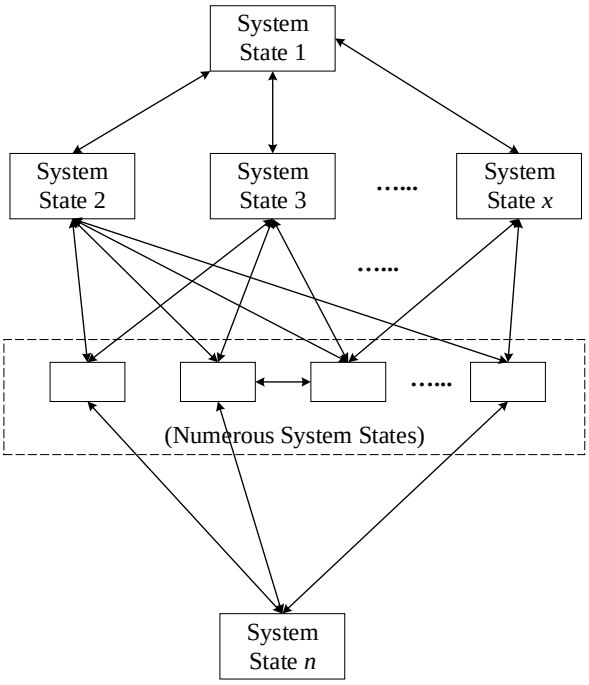

Figure 26. The system state space diagram for an actual power system.

One approach of generating the system state space is to use a completely analytical method to compute the probabilities of all system states. However, the size of a large system as well as the complexity of various transitions may prohibit such an analytical analysis.

Another approach is to decouple the entire system into mutually independent subsets so that system states can be sampled as combinations of subset states, as illustrated in the previous section. Each subset should consist of only a small number of components so that the state space for this subset can be readily developed with state probabilities computed. However, the high dependencies among system states in the presence of cyber-induced failures make such a decoupling very difficult.

It is, therefore, necessary to find some "smart" means of generating a representative system state space that preserves the causal and chronological features without insurmountable analytical computations. It is expected that this state space will not represent the entire state space but will be its representative. With this objective, a novel method is proposed in this section.

The method is proposed based on the fact that in a sequential Monte Carlo simulation, the computational effort for only generating a chronological state sequence is small compared to the effort of evaluating the states using DC power flow based linear programming. Actually the method outlined below is valid irrespective of this observation but the computational advantage over pure sequential simulation is obtained only if the state evaluation process is computationally time consuming.

1) Perform a sequential Monte Carlo simulation for N years to generate a chronological state sequence of system states. One hour is considered as the unit of time advancement so that a system state, which is a combination of all component states and load states, remains unchanged within each hour. Therefore, there are $8760N$ system states when the simulation is finished. These system states, each with probability $1/(8760N)$, establish a representative state space. They are generated sequentially therefore they preserve the chronological, causal, and dependent characteristics. For more precision, smaller time advancement like 0.25 hour can be selected.
2) Randomly generate a list of $8760N_e$ ($1 \leq N_e < N$) integer numbers with each random number having a value between 1 to $8760N$. Pick up the $8760N_e$

states from the state space generated in the previous step and evaluate them. It should be noted that since time unit of each state is the same, all of the states are equally probable.

3) Calculate the reliability indices.

To implement the procedure outlined above, a very large number of system states need to be stored first. This can make the storage and retrieval cumbersome and time consuming. To overcome this difficulty of storing the system states generated by the sequential Monte Carlo simulation, the list of $8760N_e$ random numbers can be generated first. The sequential Monte Carlo simulation is then performed and as it proceeds, it only evaluates the states existing in the list. Other states are discarded and therefore the states do not need to be stored.

An intuitive expression of the proposed method is shown in Figure 27. A mark "**X**" indicates one of the $8760N_e$ hours generated in the list by random sampling. Then the sequential process is started and as the sampled hour (**X**) is encountered, the state is evaluated. Therefore, only the marked states are evaluated as the sequential simulation proceeds. All unmarked states are discarded.

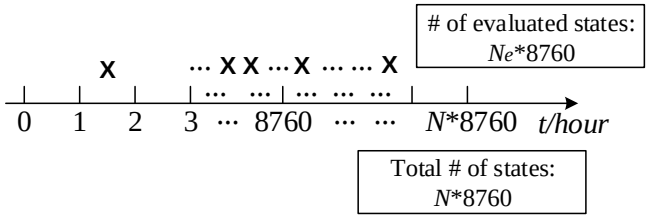

Figure 27. Expression of the proposed method.

5.5 Case Studies

The proposed method is implemented in comparison with a completely sequential methodology, as described in Section 4 of this dissertation. The test system is established based on the Roy Billinton Test System (RBTS) [46] with extensions of cyber part at buses 3, 4, and 5. The placements and connections of cyber elements such as Current/Potential Transformers, Merging Units, and Protection Intelligent Electronic Devices, are defined in the extensions. The reliability data of the extended system are presented in Section 4. The hourly load profile is created based on the data in Tables 1, 2, and 3 from [48].

Currently, the obstacle to performing the case studies in a larger system (such as an extended IEEE Reliability Test System [48]) is the unavailability of such a system with detailed configuration descriptions on the cyber part. The size of the RBTS permits us to perform such extensions, as described in Section 4, while the effort needed to extend the IEEE RTS is very significant and far beyond the scope of this dissertation. The applicability of the completely sequential methodology for large power systems is illustrated in Section 4. Once a large test system with detailed descriptions on the cyber part is available, the method proposed in this section can be implemented as well.

5.5.1 Index Definitions

In the completely sequential methodology, the reliability indices Loss of Load Probability (LOLP), Loss of Load Expectation (LOLE), and Expected Energy Not Supplied (EENS) are defined in Section 4. The coefficient of variation (β) is defined as:

$$\beta = \frac{\sqrt{V(F)/N_y}}{E(F)} \tag{5.4}$$

where $V(F)$ is the variance of the test function, N_y is the number of simulated years, and $E(F)$ is the expected estimate of the test function.

For the method proposed in this section, reliability indices are defined as follows.

$$LOLP = \frac{1}{N_k}\sum_{i=1}^{N_k} H_i \tag{5.5}$$

where N_k is the total number of samples randomly selected from the state space. N_k equals $8760N_e$ with N_e defined in the previous section. H_i equals 1 if load curtailment occurs in the i^{th} sample, otherwise it equals 0.

$$LOLE = LOLP \cdot 8760 \tag{5.6}$$

with unit of hours/year.

$$EENS = \frac{8760}{N_k}\sum_{i=1}^{N_k} C_i \cdot (1\ hour) \tag{5.7}$$

with unit of MWh/year, where N_k is the total number of samples randomly selected from the state space. C_i is the load curtailment in the i^{th} sample, with unit MW.

For the method proposed in this section, the coefficient of variation (β') is defined as:

$$\beta' = \frac{\sqrt{V(F)/N_k}}{E(F)} \tag{5.8}$$

where N_k is the total number of samples randomly selected from the state space. $V(F)$ is the variance of the test function. $E(F)$ is the expected estimate of the test function.

5.5.2 Results and Discussions

The completely sequential methodology is simulated for 300 years. For the method proposed in this section, $8760N$ samples are generated as the representative state space, of which $8760N_e$ samples are randomly selected and evaluated. N = 300 and N_e = 50 are used.

The simulations are performed in MATLAB on a computer with a 3.20 GHz processor. The results are shown in Table 40.

Table 40 Estimated reliability indices

Index	Completely Sequential	Proposed Method with N = 300, N_e = 50
LOLP	0.00131989	0.00134932
LOLE (hours/year)	11.562	11.820
EENS (MWh/year)	144.901	140.440
CPU Time (seconds)	501	212
β/β' of EENS	0.0340	0.0429

The comparison between the proposed method and the completely sequential methodology clearly indicates an efficiency improvement in evaluation. With an acceptable coefficient of variation (<5%), the CPU time of the proposed method is reduced to less than 50% of the time consumed by the completely sequential methodology. It should be noted that the relative CPU times are important but the absolute values of CPU times can be significantly improved in both cases by using more efficient linear programming modules.

The relationship between the selected sample size (N_e) and the estimated system EENS is plotted in Figure 28. Also, the relationship between N_e and the coefficient of variation (β') of EENS is plotted in Figure 29. Both of the two cases are studied with N = 300 to generate the representative state space.

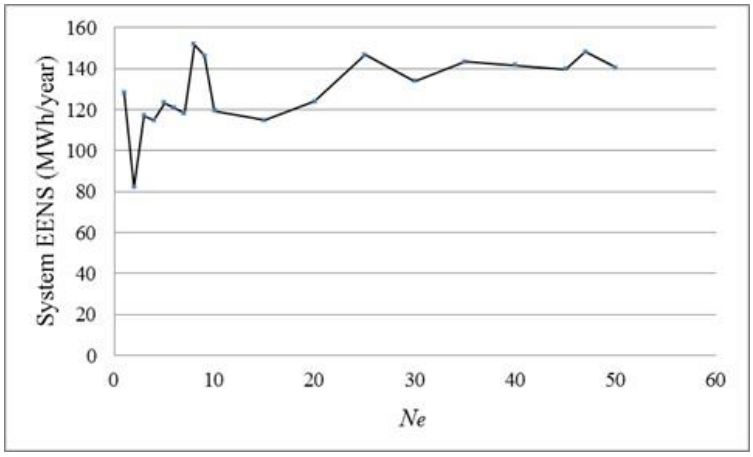

Figure 28. Relationship between EENS and selected sample size (N_e).

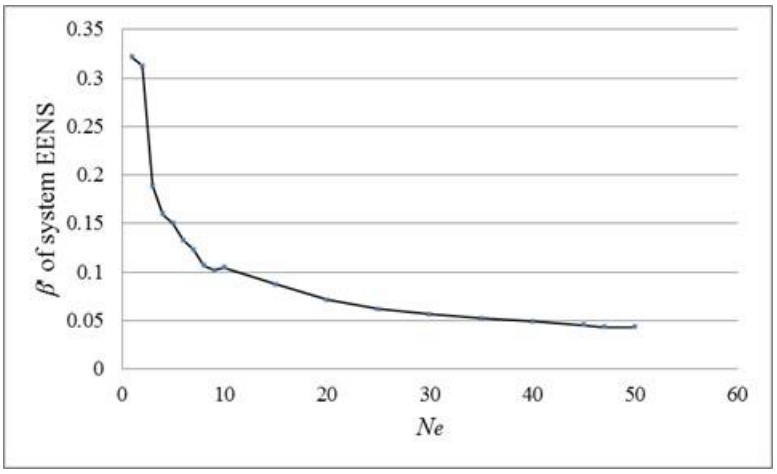

Figure 29. Relationship between coefficient of variation (β') and selected sample size(N_e).

5.6 Summary

In this section, a non-sequential approach is proposed for systems involving dependent failures. A representative state space is generated from which sampling can be performed. The sequential technique is used to generate this representative state space that preserves the chronological and causal characteristics of cyber-induced incidents. The non-sequential technique is used with the major objective of accelerating evaluation process. The results clearly show an efficiency improvement by the proposed method compared to the completely sequential methodology, with an acceptable precision. The efficiency improvement will be even more significant for applications in large cyber-physical power systems.

It should be noted that the sequential simulation may not be the only option to generate the representative state space, which is basically a joint probability distribution of component probability distributions. The major difficulties of applying conventional

non-sequential sampling methods to generating appropriate state space in presence of dependent failures are thoroughly discussed in this section with the intention of enlightening future studies on this subject.

6. CONCLUSIONS AND OUTLOOK

This dissertation extends the scope of bulk power system reliability modeling and analysis with the consideration of cyber elements. The major contributions, research conclusions, and outlook are summarized as follows.

6.1 Contributions and Research Conclusions

In Section 2, a novel methodology for composite cyber-physical power system reliability analysis is proposed. The concept of Cyber-Physical Interface Matrix (CPIM) is introduced. A typical substation protection system with modern features is designed and analyzed as an example to illustrate the construction and utility of CPIM. The CPIM is the critical idea in the proposed methodology. It decouples the analysis of the cyber part from the physical part and provides the means of performing the overall analysis in a tractable fashion.

In Section 3, the consideration of cyber-link failures is included in substation modeling. The results clearly indicate a degradation of system reliability due to cyber-link failures.

In Section 4, the CPIM is realized into a concrete application from an abstract concept. The overall methodology for composite system reliability evaluation with the use of CPIM is enhanced and implemented on an extended Roy Billinton Test System (RBTS). The results clearly indicate the impact of cyber-induced failures on system-

wide reliability indices and also signify the importance of accelerating switching process. With its scalability illustrated, the overall methodology provides a scalable option for reliability evaluation of large cyber-physical power systems.

In Section 5, the difficulties of using non-sequential techniques when there are dependent failures are thoroughly explored. An approach is proposed to overcome the difficulties by generating a representative state space from which states can be sampled. Furthermore, a method is introduced such that the state space generated by the sequential process does not need to be stored. The results clearly show an efficiency improvement of the proposed approach compared to the completely sequential methodology, with an acceptable precision. The efficiency improvement will be even more beneficial for applications in large cyber-physical power systems.

6.2 Outlook

The overall methodology proposed in this dissertation establishes the main framework for reliability evaluation of large cyber-physical power systems. More technical details, such as the internal structure of the Process Bus, can be considered in cyber part modeling without changing the framework of the proposed methodology. Consideration of these details will provide more precise probabilities in the CPIM and thereby yield more realistic reliability indices.

Furthermore, it has been recognized in this dissertation that the unavailability of a large reliability test system with detailed description on the cyber part is an obstacle for

testing developed methodologies. It is worthwhile to develop such a system as this is of crucial significance for future cyber-physical reliability studies. The development of such a test system requires substantial efforts as well as sound judgment from industry.

REFERENCES

[1] R. Billinton, *Power System Reliability Evaluation*. New York, USA: Gordon and Breach, 1970.

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

[3] R. Billinton and W. Li, *Reliability Assessment of Electric Power Systems using Monte Carlo Methods*. New York, USA: Plenum Press, 1994.

[4] B. Falahati, Y. Fu, and L. Wu, "Reliability assessment of smart grid considering direct cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515-1524, Sep. 2012.

[5] B. Falahati and Y. Fu, "Reliability assessment of smart grids considering indirect cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1677-1685, Jul. 2014.

[6] C. Singh and A. Sprintson, "Reliability assurance of cyber-physical power systems," in *Proc. IEEE Power and Energy Society General Meeting*, pp. 1-6, Jul. 2010.

[7] A. G. Phadke and J. S. Thorp, "Expose hidden failures to prevent cascading outages," *IEEE Computer Applications in Power*, vol. 9, no. 3, pp. 20-23, Jul. 1996.

[8] X. Yu and C. Singh, "A practical approach for integrated power system vulnerability analysis with protection failures," *IEEE Trans. Power Systems*, vol. 19, no. 4, pp. 1811-1820, Nov. 2004.

[9] D. C. Elizondo, J. De La Ree, A. G. Phadke, and S. Horowitz, "Hidden failures in protection systems and their impact on wide-area disturbances," in *Proc. IEEE Power Engineering Society Winter Meeting*, vol. 2, pp. 710-714, Jan./Feb. 2001.

[10] F. Yang, A. P. S. Meliopoulos, G. J. Cokkinides, and Q. B. Dam, "Effects of protection system hidden failures on bulk power system reliability," in *Proc. 2006 IEEE 38th North American Power Symp.*, pp. 517-523, Sep. 2006.

[11] S. H. Horowitz and A. G. Phadke, *Power System Relaying*, 3rd ed. Chichester, West Sussex, UK: John Wiley & Sons Ltd, 2008.

[12] J. L. Blackburn and T. J. Domin, *Protective Relaying: Principles and Applications*, 3rd ed. Boca Raton, FL, USA: CRC, 2007.

[13] P. M. Anderson, *Power System Protection – Part VI: Reliability of Protective Systems*. New York, USA: McGraw-Hill/IEEE Press, 1999.

[14] T. Skeie, S. Johannessen, and C. Brunner, "Ethernet in substation automation," *IEEE Control Syst. Mag.*, vol. 22, no. 3, pp. 43-51, Jun. 2002.

[15] B. Kasztenny, J. Whatley, E. A. Udren, J. Burger, D. Finney, and M. Adamiak, "Unanswered questions about IEC 61850 – What needs to happen to realize the vision?," presented at the 32nd Annual Western Protective Relay Conf., Spokane, WA, USA, Oct. 2005.

[16] T. S. Sidhu and P. K. Gangadharan, "Control and automation of power system substation using IEC 61850 communication," in *Proc. 2005 IEEE Conference on Control Applications*, pp. 1331-1336, Aug. 2005.

[17] J. D. McDonald, *Electric Power Substations Engineering*, 3rd ed. Boca Raton, FL, USA: CRC, 2012.

[18] F. Yang, "A comprehensive approach for bulk power system reliability assessment," Ph.D. dissertation, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA, 2007.

[19] R. Billinton and J. Tatla, "Composite generation and transmission system adequacy evaluation including protection system failure modes," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-102, no. 6, pp. 1823-1830, Jun. 1983.

[20] M. C. Bozchalui, M. Sanaye-Pasand, and M. Fotuhi-Firuzabad, "Composite system reliability evaluation incorporating protection system failures," in *Proc. 2005 IEEE Canadian Conference on Electrical and Computer Engineering*, pp. 486-489, May 2005.

[21] K. Jiang and C. Singh, "New models and concepts for power system reliability evaluation including protection system failures," *IEEE Trans. Power Systems*, vol. 26, no. 4, pp. 1845-1855, Nov. 2011.

[22] K. Jiang, "The impact of protection system failures on power system reliability evaluation," Ph.D. dissertation, Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA, 2012.

[23] C. Singh and R. Billinton, *System Reliability Modeling and Evaluation*. London, UK: Hutchinson, 1977.

[24] J. C. O. Mello, M. V. F. Pereira, and A. M. Leite da Silva, "Evaluation of reliability worth in composite systems based on pseudo-sequential Monte Carlo simulation," *IEEE Trans. Power Systems*, vol. 9, no. 3, pp. 1318-1326, Aug. 1994.

[25] I. Ali and M. S. Thomas, "Substation communication networks architecture," in *Proc. Joint International Conf. on Power System Technology (POWERCON) and IEEE Power India Conf.*, pp. 1-8, Oct. 2008.

[26] P. Zhang, L. Portillo, and M. Kezunovic, "Reliability and component importance analysis of all-digital protection systems," in *Proc. IEEE Power Eng. Soc. Power Systems Conf. and Exposition*, pp. 1380-1387, Oct. 2006.

[27] T. S. Sidhu, M. G. Kanabar, and P. P. Parikh, "Implementation issues with IEC 61850 based substation automation systems," in *Proc. 15th National Power Systems Conf.*, Mumbai, India, pp. 473-478, Dec. 2008.

[28] M. G. Kanabar and T. S. Sidhu, "Reliability and availability analysis of IEC 61850 based substation communication architectures," in *Proc. IEEE Power & Energy Society General Meeting*, Calgary, AB, Canada, pp. 1-8, 2009.

[29] Y. Zhang, A. Sprintson, and C. Singh, "An integrative approach to reliability analysis of an IEC 61850 digital substation," in *Proc. IEEE Power & Energy Society General Meeting*, San Diego, CA, USA, pp. 1-8, 2012.

[30] A. F. Sleva, *Protective Relay Principles*. Boca Raton, FL, USA: CRC, 2009, pp. 112-113.

[31] *IEC Standard for Communication network and systems in substations, IEC 61850,* 2003.

[32] K. Jiang and C. Singh, "Reliability modeling of all-digital protection systems including impact of repair," *IEEE Trans. Power Delivery*, vol. 25, no. 2, pp. 579-587, Apr. 2010.

[33] K. P. Brand, V. Lohmann, and W. Wimmer, *Substation Automation Handbook*. Bremgarten, Switzerland: Utility Automation Consulting Lohmann, 2003.

[34] V. Skendzic, I. Ender, and G. Zweigle, "IEC 61850-9-2 process bus and its impact on power system protection and control reliability," Schweitzer Engineering Laboratories, Inc., Pullman, WA, USA, Tech. Rep., 2007.

[35] T. M. Lindquist, L. Bertling, and R. Eriksson, "Circuit breaker failure data and reliability modeling," *IET generation, transmission & distribution*, vol. 2, no. 6, pp. 813-820, Nov. 2008.

[36] P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu, and A. Shami, "Evaluation of communication technologies for IEC 61850 based distribution automation system with distributed energy resources," in *Proc. IEEE Power & Energy Society General Meeting*, Calgary, AB, Canada, pp. 1-8, 2009.

[37] C. Singh and J. Mitra, "Monte Carlo simulation for reliability analysis of emergency and standby power systems," in *Proc. 30th IEEE Industry Applications Society Conf.*, Orlando, FL, USA, pp. 2290-2295, Oct. 1995.

[38] M. G. Kanabar and T. S. Sidhu, "Performance of IEC 61850-9-2 process bus and corrective measure for digital relaying," *IEEE Trans. Power Delivery*, vol. 26, no. 2, pp. 725-735, Apr. 2011.

[39] P. Ferrari, A. Flammini, S. Rinaldi, and G. Prytz, "Mixing real time Ethernet traffic on the IEC 61850 process bus," in *Proc. 9th IEEE International Workshop on Factory Communication Systems (WFCS)*, Lemgo, Germany, pp. 153-156, May 2012.

[40] L. Andersson, K.-P. Brand, C. Brunner, and W. Wimmer, "Reliability investigations for SA communication architectures based on IEC 61850," in *Proc. 2005 IEEE Russia Power Tech*, St. Petersburg, Russia, pp. 1-7, Jun. 2005.

[41] A. Apostolov and B. Vandiver, "IEC 61850 process bus–principles, applications and benefits," in *Proc. 63rd Annual Conf. Protective Relay Engineers*, pp. 1-6, 2010.

[42] H. Lei, C. Singh, and A. Sprintson, "Reliability modeling and analysis of IEC 61850 based substation protection systems," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2194-2202, Sep. 2014.

[43] H. Hajian-Hoseinabadi, "Impacts of automated control systems on substation reliability," *IEEE Trans. Power Delivery*, vol. 26, no. 3, pp. 1681-1691, Jul. 2011.

[44] H. Hajian-Hoseinabadi, M. Hasanianfar, and M. E. H. Golshan, "Quantitative reliability assessment of various automated industrial substations and their impacts on distribution reliability," *IEEE Trans. Power Delivery*, vol. 27, no. 3, pp. 1223-1233, Jul. 2012.

[45] J. J. Grainger and W. D. Stevenson, *Power System Analysis*. New York, USA: McGraw-Hill, 1994, pp. 337-338.

[46] R. Billinton, S. Kumar, N. Chowdhury, K. Chu, K. Debnath, L. Goel, E. Khan, P. Kos, G. Nourbakhsh, and J. Oteng-Adjei, "A reliability test system for educational

purposes-basic data," *IEEE Trans. Power Systems*, vol. 4, no. 3, pp. 1238-1244, Aug. 1989.

[47] A. Sankarakrishnan and R. Billinton, "Sequential Monte Carlo simulation for composite power system reliability analysis with time varying loads," *IEEE Trans. Power Systems*, vol. 10, no. 3, pp. 1540-1545, Aug. 1995.

[48] IEEE Committee Report, "IEEE reliability test system," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-98, no. 6, pp. 2047-2054, Nov./Dec. 1979.

[49] C. Singh and J. Mitra, "Composite system reliability evaluation using state space pruning," *IEEE Trans. Power Systems*, vol. 12, no. 1, pp. 471-479, Feb. 1997.

[50] EPRI, "Composite system reliability evaluation methods," Final Report on Research Project 2473-10, EPRI EL-5178, Jun. 1987.

[51] J. Mitra and C. Singh, "Incorporating the DC load flow model in the decomposition-simulation method of multi-area reliability evaluation," *IEEE Trans. Power Systems*, vol. 11, no. 3, pp. 1245-1254, Aug. 1996.

[52] N. Gubbala and C. Singh, "Models and considerations for parallel implementation of Monte Carlo simulation methods for power system reliability evaluation," *IEEE Trans. Power Systems*, vol. 10, no. 2, pp. 779-787, May 1995.

[53] C. L. T. Borges, D. M. Falcão, J. C. O. Mello, and A. C. G. Melo, "Composite reliability evaluation by sequential Monte Carlo simulation on parallel and distributed processing environments," *IEEE Trans. Power Systems*, vol. 16, no. 2, pp. 203-209, May 2001.

[54] H. Lei and C. Singh, "Power system reliability evaluation considering cyber-malfunctions in substations," *Electric Power Systems Research*, vol. 129, pp. 160-169, 2015.

[55] R. Billinton and W. Li, "A system state transition sampling method for composite system reliability evaluation," *IEEE Trans. Power Systems*, vol. 8, no. 3, pp. 761-770, Aug. 1993.

[56] A. M. Rei and M. T. Schilling, "Reliability assessment of the Brazilian power system using enumeration and Monte Carlo," *IEEE Trans. Power Systems*, vol. 23, no. 3, pp. 1480-1487, Aug. 2008.

[57] Z. Shu and P. Jirutitijaroen, "Non-sequential simulation methods for reliability analysis of power systems with photovoltaic generation," in *Proc. 2010 IEEE 11th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, pp. 703-709, Jun. 2010.